Neukirch
Algebraische Zahlentheorie

Jürgen Neukirch

Algebraische Zahlentheorie

Mit 16 Abbildungen

Springer

Jurgen Neukirch †

Unveranderter Nachdruck der ersten Auflage, die 1992 im Springer-Verlag Berlin Heidelberg unter dem Titel *Algebraische Zahlentheorie*, ISBN 3-540-54273-5, erschien

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie, detaillierte bibliografische Daten sind im Internet über http://dnb d nb de abrufbar

Mathematics Subject Classification (1991) 11-XX, 14-XX

ISBN-10 3-540-37547-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-37547-0 Springer Berlin Heidelberg New York

Umschlaggestaltung WMXDesign GmbH, Heidelberg
Herstellung: LE-TEX Jelonek, Schmidt & Vöckler GbR, Leipzig
Gedruckt auf saurefreiem Papier 175/3100YL 5 4 3 2 1 0

Vorwort

Die Zahlentheorie nimmt unter den mathematischen Disziplinen eine ähnlich idealisierte Stellung ein wie die Mathematik selbst unter den anderen Naturwissenschaften. Frei von der Pflicht, von außen kommenden Gegebenheiten dienlich sein zu müssen, schöpft sie ihre Zielsetzungen weitgehend aus sich selbst heraus und erhält sich dadurch eine ungestörte Harmonie. Die Unmittelbarkeit ihrer Problemstellungen, die eigenartige Klarheit ihrer Aussagen, der Hauch des Geheimnisvollen in ihren entdeckten wie unentdeckten, d.h. nur erahnten Gesetzmäßigkeiten, nicht zuletzt aber auch der Reiz ihrer eigentümlich befriedigenden Schlußweisen haben ihr zu allen Zeiten eine hingebungsvolle Anhängerschaft zugetragen.

In der Zuwendung der Zahlentheoretiker zu ihrer Wissenschaft läßt sich nun ein unterschiedliches Verhalten ausmachen. Während die einen einen theoretischen Aufbau nur so weit treiben wollen, als er für das einzelne, ins Auge gefaßte konkrete Resultat nötig ist, streben die anderen nach einer umfassenderen, konzeptionellen Klarheit, die hinter der Vielfalt der zahlentheoretischen Erscheinungen stets den Vater des Gedankens sucht. Beide Neigungen haben ihre Berechtigung und erhalten eine besondere Wirkung durch den gegenseitigen Einfluß, den sie mit vielen Anregungen aufeinander ausüben. Vom Erfolg der ersten Haltung, die sich stets am konkret gestellten Problem orientiert, gibt manches schöne Lehrbuch überzeugende Auskunft. Unter diesen sei namentlich das überaus lehrreiche und leicht lesbare Werk „Zahlentheorie" von *S. I. Borevicz* und *I. R. Šafarevič* [14] hervorgehoben, dessen Lektüre dem Leser mit besonderer Empfehlung ans Herz gelegt werden soll.

Das vorliegende Buch ist von einer anderen Absicht getragen. Wohl soll es als echtes, zunächst nur die Grundlagen der Algebra voraussetzendes Lehrbuch den Studenten in die Theorie der algebraischen Zahlkörper einführen (es beginnt mit der Gleichung $2 = 1 + 1$). Anders aber als die oben angesprochenen Bücher stellt es im Verlauf die auf moderner Begrifflichkeit fußenden theoretischen Aspekte heraus, wobei es sich allerdings bemüht, die Abstraktion in engen Grenzen zu halten und den Blick auf die konkreten und eigentlichen Zielsetzungen der Zahlentheorie nicht zu verstellen. Das Anliegen, die algebraische Zahlentheorie so weit wie möglich einer theoretischen Einheitlichkeit unterzuordnen, er-

scheint heute als ein Gebot, das sich durch die revolutionäre Entwicklung aufdrängt, die die Zahlentheorie in den letzten Jahrzehnten mit der „arithmetischen algebraischen Geometrie" genommen hat. Die enormen Erfolge, die diese neue geometrische Sicht der Dinge etwa im Bereich der Weil-Vermutungen, der Mordell-Vermutung, in dem Problemkreis um die Birch-Swinnterton-Dyer-Vermutung etc. gezeitigt hat, beruhen ganz wesentlich auf dem Entschluß, der konzeptionellen Denkweise eine unumschränkte Geltung einzuräumen.

Nun können zwar diese beeindruckenden Ergebnisse ihres großen höherdimensionalen Aufwandes wegen in diesem Buch kaum angesprochen werden, das sich ganz bewußt auf die Theorie der algebraischen Zahlkörper allein, also auf den eindimensionalen Fall beschränkt. Jedoch schien mir eine Darstellung der Theorie nötig zu sein, die diesen Fortentwicklungen mit vorwärts gerichtetem Blick Rechnung trägt, die ihre Akzente und Argumente der höheren Einsicht unterwirft und die Theorie der algebraischen Zahlkörper in die höherdimensionale Theorie einzupassen vermag oder sich wenigstens einer solchen Eingliederung nicht entgegenstellt. Aus diesem Grund habe ich mich bemüht, dem funktoriellen Gesichtspunkt und dem weitertragenden Argument nach Möglichkeit den Vorzug über den schnellen Kunstgriff zu geben, und habe besonderen Wert darauf gelegt, die geometrische, sich an der Theorie der algebraischen Kurven orientierende Interpretation der Dinge in den Vordergrund zu rücken.

Auf die weithin geübte Gewohnheit, den Inhalt der einzelnen Kapitel im Vorwort zusammenfassend vorzustellen, will ich verzichten. Ein einfaches Durchblättern derselben liefert die gleiche Information auf unterhaltsamere Weise. Es mögen aber einige prinzipielle Erwägungen hervorgehoben werden, die mich bei der Abfassung des Buches besonders bewegt haben. Das erste Kapitel legt die globalen und das zweite die lokalen Grundlagen der Theorie der algebraischen Zahlkörper. Diese Grundlagen finden einen abrundenden Abschluß in den ersten drei Paragraphen des dritten Kapitels, der von dem Bestreben beherrscht ist, die klassischen Begriffsbildungen und Resultate in eine vollständige Analogie zur Theorie der algebraischen Kurven zu setzen und der Thematik des Riemann-Rochschen Satzes zu unterwerfen. Dabei steht der in jüngerer Zeit so wichtig gewordene „Arakelovsche Standpunkt" im Vordergrund der Betrachtungen, der mit vielen ineinandergreifenden Normierungen wohl zum ersten Mal in einem Lehrbuch eine ausführliche Darstellung findet. Ich habe mich allerdings nicht entschließen können, den inzwischen vielfach benutzten Terminus „Arakelov-Divisor" zu verwenden. Dies hätte den Namen *Arakelov* auf viele weitere Begriffe fortsetzen müssen und zu einer hypertrophen Bezeichnungsweise geführt,

die der elementaren Sachlage nicht angemessen erscheint. Dieser Entschluß schien um so mehr gerechtfertigt, als *ARAKELOV* selbst seine Divisoren nur für arithmetische Flächen eingeführt hat, während der entsprechende Gedanke bei den algebraischen Zahlkörpern schon auf *HASSE* zurückgeht und in dem Lehrbuch [94] von *S. LANG* etwa eine deutliche Herausstellung gefunden hat.

Zur Aufnahme der *Klassenkörpertheorie* in den Kapiteln IV–VI habe ich mich nicht ohne Skrupel entschlossen. Da mein Buch [107] über dieses Gebiet vor noch nicht langer Zeit erschienen ist, mußte eine abermalige Abhandlung dieser Theorie fragwürdig erscheinen. Es gab aber nach langem Bedenken schließlich doch keinen anderen Ausweg. Ein Lehrbuch über die algebraischen Zahlkörper ohne den krönenden Abschluß der Klassenkörpertheorie mit ihrer wichtigen Auswirkung auf die Theorie der L-Reihen mußte wie ein Torso erscheinen und hätte unter einem unvertretbaren Mangel an Vollständigkeit gelitten. Überdies war hier die Gelegenheit zu mehreren Veränderungen und Korrekturen gegeben und die Möglichkeit, den dort etwas karg behandelten Stoff mit manchen illustrativen Ergänzungen, weiterweisenden Anmerkungen und lehrreichen Aufgaben zu versehen.

Eine große Mühe habe ich auf das letzte Kapitel über die Zetafunktionen und L-Reihen gewandt, denen in den letzten Jahrzehnten eine zentrale Bedeutung zugewachsen ist, ohne daß dies in den Lehrbüchern eine ausreichende Berücksichtigung gefunden hat. Ich habe aber darauf verzichtet, bei den Heckeschen L-Reihen den auf der harmonischen Analysis basierenden *TATE*schen Zugang zu wählen, obgleich gerade dieser seines konzeptionellen Charakters wegen dem Anliegen dieses Buches genau entsprochen hätte. Der Grund lag in der kaum zu verbessernden Klarheit der *TATE*schen Darstellung, die ihre Wiederholung in hinreichender Weise anderswo erfahren hat. Statt dessen habe ich es vorgezogen, mich der ursprünglichen *HECKE*schen Vorgehensweise zuzuwenden, die in der originalen Fassung dem direkten Verständnis nur schwer zugänglich ist, aber mit ihren vielen Vorteilen nach einer modernen Darstellung rief. Im Anschluß daran war die Gelegenheit gegeben, den *ARTIN*schen L-Reihen mit ihrer Funktionalgleichung einen ausreichenden Platz einzuräumen, den sie erstaunlicherweise in den bisherigen Lehrbüchern nicht gefunden haben.

Schwer ist mir der Entschluß gefallen, die *Iwasawa-Theorie* auszuschließen, eine vergleichsweise junge Theorie, die ganz und gar den algebraischen Zahlkörpern zugeschrieben ist, also dem eigentlichen Gegenstand dieses Buches. Sie wäre als Abbild eines wichtigen, bei den algebraischen Kurven anzutreffenden geometrischen Sachverhalts eine besonders schöne Bestätigung der ständig herausgekehrten Auffassung

gewesen, daß Zahlentheorie Geometrie sei. Ich glaube aber, daß der geometrische Aspekt in diesem Fall seine wahre Überzeugungskraft erst durch den Einsatz der *Etalkohomologie* gewinnt, die weder vorausgesetzt noch hier in vernünftigen Grenzen entwickelt werden konnte. Möge das Unbehagen über diesen Mangel stark genug sein, den Entschluß hervorzurufen, den vorliegenden Band mit einem zweiten über die Kohomologie der algebraischen Zahlkörper fortzusetzen.

Das Buch hat von Anfang an nicht nur ein modernes Lesebuch über die algebraische Zahlentheorie werden sollen, sondern auch eine handliche Vorlage für eine Kursvorlesung. Diese Absicht wurde im Verlauf durch den überraschend anwachsenden Stoff bedrängt, dessen Aufnahme sich durch eine in der Theorie angelegte innere Notwendigkeit ergab. Gleichwohl hat das Buch, wie ich denke, diesen Charakter nicht verloren und hat eine erste Probe darauf schon bestanden. Mit dem Wintersemester beginnend läßt sich der grundlegende Inhalt der ersten drei Kapitel in zwei Semestern bei kluger Beschränkung (aber womöglich unter Einbeziehung der unendlichen Galoistheorie) in bequemer Weise darbringen, so daß im darauffolgenden Wintersemester die in Kapitel IV–VI ausgeführte Klassenkörpertheorie einen etwas knappen, aber doch hinreichenden Platz finden kann.

Im Kapitel I sind die §§ 11–14 für eine einführende Vorlesung weitgehend entbehrlich. Die Aufnahme des § 12 in das Buch über die *Ordnungen* schien mir dennoch besonders wichtig, obgleich seine Resultate auf den weiteren Gang der Dinge keinen Einfluß nehmen. Mit den Ordnungen treten nämlich nicht nur die für viele diophantische Probleme wesentlichen Multiplikatorenringe ins Blickfeld, sondern vor allem die Analoga zu den *singulären* Kurven. Bei der wachsenden Bedeutung, die die Kohomologietheorie für die algebraischen Zahlkörper erfährt, mehr aber noch die *algebraische K-Theorie*, für deren Aufbau die Einbeziehung der singulären Schemata ganz unerläßlich ist, ist es an der Zeit, den Ordnungen eine angemessene Darstellung einzuräumen.

Im Kapitel II kann die besondere Behandlung der henselschen Körper in § 6 auf die vollständig bewerteten Körper beschränkt und dem § 4 zugeschlagen werden. Der § 10 über die höheren Verzweigungsgruppen darf bei knapper Zeit ganz entfallen.

Vom Kapitel III sollten die ersten drei Paragraphen in den Vorlesungsstoff einbezogen sein, die eine neue Begründung klassischer Ergebnisse der algebraischen Zahlentheorie herausstellen. Die sich daran anschließende Theorie um den Grothendieck-Riemann-Roch ist ein günstiges Thema eher für ein Seminar als für eine einführende Vorlesung.

Bei der Darstellung der Klassenkörpertheorie schließlich ist es sehr zeitsparend, wenn die Hörer mit den pro-endlichen Gruppen und der unendlichen Galoistheorie schon vorher vertraut gemacht worden sind. Vom Kapitel V müssen die §§ 4–7 über die formalen Gruppen, die Lubin-Tate-Theorie und die höhere Verzweigungstheorie nicht unbedingt gebracht werden. Will man es ganz kurz machen, so erhält man selbst durch das Fortlassen von V, § 3 über die Hilbertsymbole und VI, § 7 und § 8 eine abgeschlossene Theorie, die allerdings dann etwas unbefriedigend ist, weil sie zu sehr im Abstrakten haften bleibt und zu den klassischen Problemstellungen nicht mehr zurückführt.

Ein Wort noch zu den Aufgaben am Schluß der einzelnen Paragraphen. Manche von ihnen sind im eigentlichen nicht als Übungsaufgaben gemeint, sondern als zusätzliche Hinweise, die im Text keinen passenden Platz finden konnten. Der Leser ist hier aufgerufen, seine Findigkeit im Aufspüren der einschlägigen Literatur zu beweisen. Auch habe ich nicht alle Aufgaben selbst durchgerechnet, und man muß auf die Möglichkeit gefaßt sein, daß die eine oder andere nicht richtig gestellt ist. Es ist dem Leser damit die zusätzliche Aufgabe gegeben, in solchem Fall die korrekte Formulierung selbst zu finden. Er wird gebeten, ein eventuelles Versehen des Autors unter das Goethesche Wort zu stellen:

„Irrtum verläßt uns nie, doch ziehet ein höher Bedürfnis
Immer den strebenden Geist leise zur Wahrheit hinan."

Für die Fertigstellung des Buches ist mir mannigfache Hilfe zuteil geworden. Ich danke dem Springer-Verlag für das zuvorkommende Eingehen auf meine Wünsche. Meine Schüler *I. Kauzs*, *B. Köck*, *P. Kolcze*, *Th. Moser*, *M. Spiess* haben größere und kleinere Teile einer kritischen Durchsicht unterzogen, was zu zahlreichen Verbesserungen und zur Vermeidung von Fehlern und Unklarheiten geführt hat. Meinen Freunden *W.-D. Geyer*, *G. Tamme* und *K. Wingberg* verdanke ich viele wertvolle Ratschläge, die dem Buche zugute gekommen sind, und *C. Deninger* und *U. Jannsen* die Anregung, der Heckeschen Theorie der Theta-Reihen und L-Reihen eine neue Darstellung angedeihen zu lassen. Ein großes Verdienst hat sich Frau *Eva-Maria Strobel* um das Buch erworben. Sie hat die Bilder hergestellt und hat mich in unermüdlicher, ins letzte Detail hineinreichender Arbeit beim Korrekturlesen und bei der äußeren Gestaltung des Textes unterstützt. Allen Helfern, auch den nicht genannten, sei an dieser Stelle herzlich gedankt. Einen besonders großen Dank bringe ich schließlich Frau *Martina Hertl* entgegen, die das Manuskript in TEX gesetzt hat. Ihrer verständigen Umsicht, ihrer unerschütterlichen und freund-

lichen Bereitschaft, bei der Bewältigung des langen handgeschriebenen Textes, der vielen Veränderungen, Ergänzungen, Korrekturen stets das beste zu leisten, ist das Erscheinen des Buches in wesentlicher Weise zu danken.

Regensburg, Februar 1992 Jürgen Neukirch

Inhaltsverzeichnis

Kapitel I
Ganze algebraische Zahlen

§ 1. Die Gaußschen Zahlen

Die Gleichungen

$$2 = 1+1\,,\quad 5 = 1+4\,,\quad 13 = 4+9\,,\quad 17 = 1+16\,,\quad 29 = 4+25\,,\quad 37 = 1+36$$

zeigen die ersten Primzahlen, die sich als eine Summe von zwei Quadratzahlen darstellen lassen. Von der 2 abgesehen sind sie alle $\equiv 1 \bmod 4$, und für eine ungerade Primzahl der Form $p = a^2+b^2$ gilt ganz allgemein $p \equiv 1 \bmod 4$, weil Quadratzahlen entweder $\equiv 0$ oder $\equiv 1 \bmod 4$ sind. Dies liegt auf der Hand; keineswegs aber die bemerkenswerte Tatsache, daß sich die Aussage umkehren läßt:

(1.1) Satz. *Für die Primzahlen $p \neq 2$ gilt*

$$p = a^2 + b^2 \quad (a, b \in \mathbb{Z}) \quad \Longleftrightarrow \quad p \equiv 1 \bmod 4\,.$$

Diese Gesetzmäßigkeit im Ring $\mathbb{Z}$ der ganzen rationalen Zahlen findet ihre natürliche Erklärung im erweiterten Bereich der **Gaußschen Zahlen**

$$\mathbb{Z}[i\,] = \{a + bi \mid a, b \in \mathbb{Z}\}\,, \qquad i = \sqrt{-1}\,.$$

In diesem Ring verwandelt sich die Gleichung $p = x^2 + y^2$ in die Produktzerlegung

$$p = (x + iy)(x - iy)\,,$$

wodurch sich das Problem stellt, wann und wie eine Primzahl $p \in \mathbb{Z}$ in $\mathbb{Z}[i\,]$ in Faktoren zerfällt. Die Antwort auf diese Frage gründet sich auf den folgenden Satz von der eindeutigen Primzerlegung in $\mathbb{Z}[i\,]$.

(1.2) Satz. *Der Ring $\mathbb{Z}[i\,]$ ist euklidisch, insbesondere also faktoriell.*

Beweis: Wir zeigen, daß $\mathbb{Z}[i\,]$ euklidisch ist bzgl. der Funktion $\mathbb{Z}[i\,] \to \mathbb{N} \cup \{0\}$, $\alpha \mapsto |\alpha|^2$. Sind $\alpha, \beta \in \mathbb{Z}[i\,]$, $\beta \neq 0$, so ist die Existenz von Gaußschen Zahlen γ, ρ nachzuweisen mit

$$\alpha = \gamma\beta + \rho \qquad \text{und} \qquad |\rho|^2 < |\beta|^2\,.$$

Es genügt offenbar, ein $\gamma \in \mathbb{Z}[i]$ zu finden mit $|\frac{\alpha}{\beta} - \gamma| < 1$. Die Gaußschen Zahlen bilden nun ein **Gitter** in der komplexen Zahlenebene $\mathbb{C}$ (Punkte mit ganzzahligen Koordinaten bzgl. der Basis 1, i). Die komplexe Zahl $\frac{\alpha}{\beta}$ liegt in einer Masche des Gitters und hat vom nächsten Gitterpunkt einen Abstand, der nicht größer ist, als die halbe Länge $\frac{\sqrt{2}}{2}$ der Diagonalen der Masche. Daher gibt es ein $\gamma \in \mathbb{Z}[i]$ mit $|\frac{\alpha}{\beta} - \gamma| \leq \frac{\sqrt{2}}{2} < 1$. □

Aufgrund dieses Satzes über den Ring $\mathbb{Z}[i]$ ergibt sich der Satz (1.1) folgendermaßen. Es genügt zu zeigen, daß eine Primzahl $p \equiv 1 \bmod 4$ von $\mathbb{Z}$ im Ring $\mathbb{Z}[i]$ kein Primelement bleibt. In der Tat, ist dies bewiesen, so existiert eine Zerlegung

$$p = \alpha \cdot \beta$$

in zwei Nicht-Einheiten α, β von $\mathbb{Z}[i]$. Die **Norm** von $z = x + iy$ ist durch

$$N(x + iy) = (x + iy)(x - iy) = x^2 + y^2$$

gegeben, also durch $N(z) = |z|^2$. Sie ist multiplikativ, so daß

$$p^2 = N(\alpha) \cdot N(\beta)\,.$$

Da α und β keine Einheiten sind, so ist $N(\alpha)$, $N(\beta) \neq 1$ (Aufgabe 1), d.h. $p = N(\alpha) = a^2 + b^2$, wenn $\alpha = a + bi$ gesetzt ist.

Um nun zu zeigen, daß eine Primzahl der Form $p = 1 + 4n$ kein Primelement in $\mathbb{Z}[i]$ sein kann, bemerken wir, daß die Kongruenz

$$-1 \equiv x^2 \bmod p$$

eine Lösung besitzt, nämlich $x = (2n)!$. In der Tat, wegen $-1 \equiv (p-1)! \bmod p$ (Satz von Wilson) ist

$$\begin{aligned} -1 \equiv (p-1)! &= [\,1 \cdot 2 \cdots (2n)\,][\,(p-1)(p-2)\cdots(p-2n)\,] \\ &\equiv [\,(2n)!\,][\,(-1)^{2n}(2n)!\,] = [\,(2n)!\,]^2 \bmod p\,. \end{aligned}$$

Wir erhalten somit $p \mid x^2 + 1 = (x+i)(x-i)$. Wegen $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$ teilt p jedoch keinen der Faktoren $x+i$, $x-i$ und ist daher kein Primelement im faktoriellen Ring $\mathbb{Z}[i]$.

Das Beispiel der Gleichung $p = x^2 + y^2$ zeigt, daß man schon durch sehr elementare Fragen aus dem Bereich der ganzen rationalen Zahlen

auf die Betrachtung höherer Bereiche von ganzen Zahlen geführt wird. Aber nicht so sehr wegen dieser Gleichung, sondern um der allgemeinen Theorie der ganzen algebraischen Zahlen ein greifbares Beispiel voranzuschicken, haben wir den Ring $\mathbb{Z}[i]$ eingeführt und wollen aus diesem Grund genauer auf ihn eingehen.

Im Vordergrund der Teilbarkeitslehre in einem Ring stehen zwei grundsätzliche Probleme: Die Bestimmung der **Einheiten** des Ringes einerseits und die seiner **Primelemente** andererseits. Die Antwort auf die erste Frage ist im vorliegenden Fall denkbar einfach. Eine Zahl $\alpha = a + bi \in \mathbb{Z}[i]$ ist genau dann eine Einheit, wenn

$$N(\alpha) := (a + ib)(a - ib) = a^2 + b^2 = 1$$

ist (Aufgabe 1), d.h. wenn entweder $a^2 = 1$, $b^2 = 0$ oder $a^2 = 0$, $b^2 = 1$ ist. Wir erhalten daher den

(1.3) Satz. *Die Gruppe der Einheiten des Ringes $\mathbb{Z}[i]$ besteht aus den vierten Einheitswurzeln,*

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$

Um die Frage nach den Primelementen, d.h. irreduziblen Elementen des Ringes $\mathbb{Z}[i]$ zu beantworten, erinnern wir daran, daß zwei Elemente α, β in einem Ring **assoziiert** heißen, in Zeichen $\alpha \sim \beta$, wenn sie sich nur um einen Einheitenfaktor unterscheiden, und daß mit einem irreduziblen Element π auch jedes Assoziierte irreduzibel ist. Mit Hilfe des Satzes (1.1) erhalten wir den folgenden genauen Überblick über die Primzahlen von $\mathbb{Z}[i]$.

(1.4) Satz. *Die Primelemente π von $\mathbb{Z}[i]$ sind bis auf Assoziierte wie folgt gegeben:*

(1) $\pi = 1 + i$,
(2) $\pi = a + bi$ *mit* $a^2 + b^2 = p$, $p \equiv 1 \bmod 4$, $a > |b| > 0$,
(3) $\pi = p$, $p \equiv 3 \bmod 4$.

Dabei bedeutet p eine Primzahl von $\mathbb{Z}$.

Beweis: Die Zahlen unter (1) und (2) sind prim, weil aus einer Zerlegung $\pi = \alpha \cdot \beta$ in $\mathbb{Z}[i]$ die Gleichung

$$p = N(\pi) = N(\alpha) \cdot N(\beta)$$

mit einer Primzahl p folgt, so daß entweder $N(\alpha) = 1$ oder $N(\beta) = 1$, also entweder α oder β eine Einheit ist. Die Zahlen $\pi = p$, $p \equiv 3 \bmod 4$, sind prim in $\mathbb{Z}[i]$, weil eine Zerlegung $p = \alpha \cdot \beta$ in Nicht-Einheiten α, β zur Folge hätte, daß $p^2 = N(\alpha) \cdot N(\beta)$ ist, d.h. $p = N(\alpha) = N(a+bi) = a^2 + b^2$, woraus sich nach (1.1) $p \equiv 1 \bmod 4$ ergäbe.

Nach dieser Feststellung haben wir zu zeigen, daß ein beliebiges Primelement π von $\mathbb{Z}[i]$ assoziiert ist zu einem der Genannten. Zunächst folgt aus

$$N(\pi) = \pi \cdot \overline{\pi} = p_1 \cdot \ldots \cdot p_r ,$$

p_i Primzahl in $\mathbb{Z}$, daß $\pi | p$ für ein $p = p_i$, also $N(\pi) | N(p) = p^2$, d.h. entweder $N(\pi) = p$ oder $N(\pi) = p^2$. Im Falle $N(\pi) = p$ ist $\pi = a + bi$ mit $a^2 + b^2 = p$, d.h. π ist vom Typ (2) oder, wenn $p = 2$ ist, assoziiert zu $1 + i$. Ist aber $N(\pi) = p^2$, so ist π zu p assoziiert, weil p/π wegen $N(p/\pi) = 1$ eine Einheit ist. Es muß überdies $p \equiv 3 \bmod 4$ gelten, weil sonst $p = 2$ oder $p \equiv 1 \bmod 4$ und nach (1.1) $p = a^2 + b^2 = (a+bi)(a-bi)$ nicht prim wäre. Damit ist alles gezeigt. □

Mit diesem Satz ist auch die Frage nach der Zerlegung der Primzahlen $p \in \mathbb{Z}$ in $\mathbb{Z}[i]$ vollständig geklärt. Die Primzahl $2 = (1+i)(1-i)$ ist wegen $1 - i = -i(1+i)$ assoziiert zum Quadrat des Primelements $1 + i$, $2 \sim (1+i)^2$, die Primzahlen $p \equiv 1 \bmod 4$ zerfallen in zwei konjugierte prime Faktoren

$$p = (a + bi)(a - bi) ,$$

und die Primzahlen $p \equiv 3 \bmod 4$ bleiben prim.

Die Gaußschen Zahlen spielen im Körper

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

die gleiche Rolle wie die ganzen rationalen Zahlen im Körper $\mathbb{Q}$, sind also als die „ganzen Zahlen" von $\mathbb{Q}(i)$ anzusehen. Dieser Ganzheitsbegriff bezieht sich auf die Koordinaten zur Basis $1, i$. Wir haben jedoch die folgende, von dieser Basiswahl unabhängige Charakterisierung der Gaußschen Zahlen:

(1.5) Satz. *$\mathbb{Z}[i]$ besteht aus genau denjenigen Zahlen der Körpererweiterung $\mathbb{Q}(i)|\mathbb{Q}$, die einer normierten Gleichung*

$$x^2 + ax + b = 0$$

mit Koeffizienten $a, b \in \mathbb{Z}$ genügen.

Beweis: Ein Element $\alpha = c + id \in \mathbb{Q}(i)$ ist Nullstelle des Polynoms

$$x^2 + ax + b \in \mathbb{Q}[x] \qquad \text{mit} \quad a = -2c,\ b = c^2 + d^2 .$$

Sind c und d ganz, so auch a und b. Sind umgekehrt a und b ganz, so auch $2c$ und $2d$. Wegen $(2c)^2 + (2d)^2 = 4b \equiv 0 \bmod 4$ folgt $(2c)^2 \equiv (2d)^2 \equiv 0 \bmod 4$, weil Quadratzahlen nur $\equiv 0$ oder $\equiv 1$ sein können, und damit die Ganzheit von c und d. □

Der letzte Satz führt uns auf die allgemeine Definition einer ganzen algebraischen Zahl als einer Zahl, die einer normierten algebraischen Gleichung mit ganzrationalen Koeffizienten genügt. Für den Bereich der Gaußschen Zahlen haben wir in diesem Paragraphen eine vollständige Antwort auf die Frage nach den Einheiten, auf die Frage nach den Primelementen und auf die Frage nach der eindeutigen Primzerlegung erhalten.

Mit diesen Fragen sind gleichzeitig die grundlegenden Probleme der allgemeinen Theorie der ganzen algebraischen Zahlen angesprochen. Die im Falle $\mathbb{Z}[i]$ gefundenen Antworten sind jedoch nicht exemplarisch; es treten an ihre Stelle ganz neuartige Entdeckungen.

Aufgabe 1. $\alpha \in \mathbb{Z}[\imath]$ ist genau dann eine Einheit, wenn $N(\alpha) = 1$.

Aufgabe 2. Zeige, daß im Ring $\mathbb{Z}[\imath]$ aus $\alpha\beta = \varepsilon\gamma^n$ mit teilerfremden Zahlen α, β und einer Einheit ε stets $\alpha = \varepsilon'\xi^n$ und $\beta = \varepsilon''\eta^n$ mit Einheiten ε', ε'' folgt.

Aufgabe 3. Zeige, daß die ganzzahligen Lösungen der Gleichung

$$x^2 + y^2 = z^2$$

mit $x, y, z > 0$ und $(x, y, z) = 1$ („Pythagoräische Tripel") durch

$$x = u^2 - v^2 , \qquad y = 2uv , \qquad z = u^2 + v^2$$

gegeben sind, mit $u, v \in \mathbb{Z}$, $u > v > 0$, $(u, v) = 1$, u, v nicht beide ungerade, und durch die Tripel, die man hieraus durch Vertauschung von x und y erhält.

Hinweis: Zeige mit Hilfe von Aufgabe 2, daß $x + \imath y = \varepsilon\alpha^2$ mit einer Einheit ε und einem $\alpha = u + \imath v \in \mathbb{Z}[\imath]$ gelten muß.

Aufgabe 4. Zeige, daß sich der Ring $\mathbb{Z}[\imath]$ nicht anordnen läßt.

Aufgabe 5. Zeige, daß der Ring $\mathbb{Z}[\sqrt{-d}] = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$ für eine ganze Zahl $d > 1$ nur die Einheiten ± 1 besitzt.

Aufgabe 6. Zeige, daß der Ring $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ für quadratfreies $d > 1$ unendlich viele Einheiten hat.

Aufgabe 7. Zeige, daß der Ring $\mathbb{Z}[\sqrt{2}] = \mathbb{Z}+\mathbb{Z}\sqrt{2}$ euklidisch ist. Zeige ferner, daß seine Einheiten durch $\pm(1+\sqrt{2})^n$, $n \in \mathbb{Z}$, gegeben sind, und bestimme seine Primelemente.

§ 2. Ganzheit

Ein **algebraischer Zahlkörper** ist eine endliche Körpererweiterung K von $\mathbb{Q}$. Die Elemente von K heißen **algebraische Zahlen**. Eine algebraische Zahl heißt **ganz**, wenn sie Nullstelle eines normierten Polynoms $f(x) \in \mathbb{Z}[x]$ ist. Dieser Ganzheitsbegriff betrifft aber nicht nur die algebraischen Zahlen. Er tritt in vielen verschiedenen Zusammenhängen auf und muß daher in voller Allgemeinheit behandelt werden.

Wenn im folgenden von Ringen die Rede ist, so sind damit stets kommutative Ringe mit Einselement gemeint.

(2.1) Definition. *Sei $A \subseteq B$ eine Ringerweiterung. Ein Element $b \in B$ heißt* **ganz** *über A, wenn es einer normierten Gleichung*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0\,, \qquad n \geq 1\,,$$

mit Koeffizienten $a_i \in A$ genügt. Der Ring B heißt **ganz** *über A, wenn alle Elemente $b \in B$ ganz über A sind.*

Die wünschenswerte Tatsache, daß mit zwei über A ganzen Elementen von B auch ihre Summe und ihr Produkt ganz sind, fällt seltsamerweise nicht vom Himmel. Sie ergibt sich aber durch die folgende abstrakte Umdeutung des Ganzheitsbegriffs.

(2.2) Satz. *Endlich viele Elemente $b_1, \ldots, b_n \in B$ sind genau dann sämtlich ganz über A, wenn der Ring $A[b_1, \ldots, b_n]$, aufgefaßt als A-Modul, endlich erzeugt ist.*

Zum Beweis benützen wir aus der linearen Algebra den

(2.3) Laplaceschen Entwicklungssatz. *Sei $A = (a_{ij})$ eine $(r \times r)$-Matrix über einem beliebigen Ring und $A^* = (a^*_{ij})$ die adjungierte Matrix, d.h. $a^*_{ij} = (-1)^{i+j} \det(A_{ij})$, wobei die Matrix A_{ij} aus A durch Herausstreichen der i-ten Spalte und j-ten Zeile entsteht. Dann gilt*

$$AA^* = A^*A = \det(A)E\,,$$

wobei E die Einheitsmatrix vom Grade r ist. Für einen Vektor $x = (x_1, \ldots, x_r)$ folgt die Implikation

$$Ax = 0 \quad \Longrightarrow \quad (\det A)x = 0\,.$$

Beweis zu (2.2): Sei $b \in B$ ganz über A und $f(x) \in A[x]$ ein normiertes Polynom vom Grade $n \geq 1$ mit $f(b) = 0$. Für ein beliebiges Polynom $g(x) \in A[x]$ können wir dann

$$g(x) = q(x)f(x) + r(x)$$

schreiben mit $q(x)$, $r(x) \in A[x]$ und $\mathrm{Grad}(r(x)) < n$, so daß

$$g(b) = r(b) = a_0 + a_1 b + \cdots + a_{n-1}b^{n-1}$$

gilt. Daher wird $A[b]$ als A-Modul durch $1, b, \ldots, b^{n-1}$ erzeugt.

Sind allgemeiner $b_1, \ldots, b_n \in B$ ganz über A, so folgt die Endlichkeit von $A[b_1, \ldots, b_n]$ über A mit vollständiger Induktion über n. Da nämlich b_n ganz über $R = A[b_1, \ldots, b_{n-1}]$ ist, so ist nach dem soeben Gezeigten $R[b_n] = A[b_1, \ldots, b_n]$ endlich erzeugt über R, also auch über A, wenn wir induktiv annehmen, daß R ein endlich erzeugter A-Modul ist.

Sei umgekehrt der A-Modul $A[b_1, \ldots, b_n]$ endlich erzeugt und $\omega_1, \ldots, \omega_r$ ein Erzeugendensystem. Für ein beliebiges Element $b \in A[b_1, \ldots, b_n]$ ist dann

$$b\,\omega_i = \sum_{j=1}^{r} a_{ij}\omega_j\,, \quad i = 1, \ldots, r\,, \quad a_{ij} \in A\,.$$

Aus (2.3) folgt $\det(bE - (a_{ij}))\omega_i = 0$, $i = 1, \ldots, r$ (E Einheitsmatrix vom Grade r), und da 1 eine Darstellung $1 = c_1\omega_1 + \cdots + c_r\omega_r$ hat, erhalten wir in $\det(bE - (a_{ij})) = 0$ eine normierte Gleichung für b mit Koeffizienten in A. Sie zeigt, daß b ganz ist über A. □

Nach diesem Satz ist mit $b_1, \ldots, b_n \in B$ *jedes* Element b aus $A[b_1, \ldots, b_n]$ ganz über A, weil $A[b_1, \ldots, b_n, b] = A[b_1, \ldots, b_n]$ ein endlich erzeugter A-Modul ist. Insbesondere ist mit zwei Elementen $b_1, b_2 \in B$ auch $b_1 + b_2$ und $b_1 b_2$ ganz über A. Es folgt überdies der

(2.4) Satz. *Seien $A \subseteq B \subseteq C$ zwei Ringerweiterungen. Ist C ganz über B und B ganz über A, so ist C ganz über A.*

Beweis: Sei $c \in C$ und $c^n + b_1 c^{n-1} + \cdots + b_n = 0$ eine Gleichung mit Koeffizienten in B und sei $R = A[b_1, \ldots, b_n]$. Dann ist $R[c]$ ein endlich

erzeugter R-Modul. Ist B ganz über A, so ist $R[c]$ sogar endlich erzeugt über A, da R endlich erzeugt über A ist. Daher ist c ganz über A. □

Die Gesamtheit der ganzen Elemente

$$\bar{A} = \{b \in B \mid b \quad \text{ganz über } A\}$$

in einer Ringerweiterung $A \subseteq B$ bildet nach dem oben Bewiesenen einen Ring. Dieser heißt der **ganze Abschluß** von A in B. Man nennt A **ganzabgeschlossen** in B, wenn $A = \bar{A}$. Aus (2.4) folgt unmittelbar, daß der ganze Abschluß $\bar{A}$ immer ganzabgeschlossen ist in B. Ist A ein Integritätsbereich mit dem Quotientenkörper K, so nennt man den ganzen Abschluß $\bar{A}$ von A in K die **Normalisierung** von A und sagt, daß A ganzabgeschlossen schlechthin ist, wenn $A = \bar{A}$. Jeder **faktorielle** Ring A ist z.B. ganzabgeschlossen. In der Tat, ist $a/b \in K \quad (a, b \in A)$ ganz über A und ist

$$(a/b)^n + a_1(a/b)^{n-1} + \cdots + a_n = 0\,,$$

$a_i \in A$, so ist

$$a^n + a_1 b a^{n-1} + \cdots + a_n b^n = 0\,.$$

Jedes Primelement π, welches b teilt, teilt hiernach auch a. Denken wir uns a/b gekürzt, so folgt $a/b \in A$.

Wir wenden uns jetzt einer spezielleren Situation zu. Sei A ein ganzabgeschlossener Integritätsbereich, K sein Quotientenkörper, $L|K$ eine endliche Körpererweiterung und B der ganze Abschluß von A in L. Nach (2.4) ist automatisch auch B ganzabgeschlossen. Jedes Element $\beta \in L$ hat dann die Gestalt

$$\beta = \frac{b}{a}\,, \quad b \in B\,, \quad a \in A\,,$$

denn wenn

$$a_n\beta^n + \cdots + a_1\beta + a_0 = 0\,, \quad a_i \in A\,, \quad a_n \neq 0\,,$$

so ist $b = a_n\beta$ ganz über A, weil die Multiplikation der Gleichung mit a_n^{n-1} eine Gleichung

$$(a_n\beta)^n + \cdots + a_1'(a_n\beta) + a_0' = 0\,, \quad a_i' \in A\,,$$

ergibt. Die Ganzabgeschlossenheit von A bewirkt ferner, daß ein Element $\beta \in L$ genau dann ganz ist über A, wenn sein **Minimalpolynom** $p(x)$ Koeffizienten in A hat. In der Tat, sei β Nullstelle des normierten Polynoms $g(x) \in A[x]$. Dann ist $p(x)$ ein Teiler von $g(x)$ in $K[x]$, so

daß alle Nullstellen $\beta_1, \ldots, \beta_n$ von $p(x)$ ganz sind über A, also auch alle Koeffizienten, d.h. $p(x) \in A[x]$.

Ein wichtiges Instrument für das Studium der ganzen Elemente in L ist durch die Spur und die Norm der Erweiterung $L|K$ gegeben. Wir erinnern an ihre

(2.5) Definition. Spur *und* **Norm** *eines Elementes $x \in L$ sind als die Spur und die Determinante der Transformation*

$$T_x : L \to L\,, \quad T_x(\alpha) = x\alpha\,,$$

des K-Vektorraums L definiert:

$$Tr_{L|K}(x) = Tr(T_x)\,, \quad N_{L|K}(x) = \det(T_x)\,.$$

In dem charakteristischen Polynom

$$f_x(t) = \det(tId - T_x) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in K[t]$$

von T_x, $n = [L : K]$, finden wir Spur und Norm durch

$$a_1 = Tr_{L|K}(x) \qquad \text{und} \qquad a_n = N_{L|K}(x)$$

wieder. Wegen $T_{x+y} = T_x + T_y$ und $T_{xy} = T_x \circ T_y$ erhalten wir Homomorphismen

$$Tr_{L|K} : L \to K \qquad \text{und} \qquad N_{L|K} : L^* \to K^*\,.$$

Im Fall, daß die Erweiterung $L|K$ separabel ist, erhält man die folgende galoistheoretische Interpretation der Spur und der Norm.

(2.6) Satz. *Ist $L|K$ separabel und durchläuft $\sigma : L \to \overline{K}$ die verschiedenen K-Einbettungen von L in einen algebraischen Abschluß $\overline{K}$, so gilt*

(i) $$f_x(t) = \prod_\sigma (t - \sigma x),$$

(ii) $$Tr_{L|K}(x) = \sum_\sigma \sigma x,$$

(iii) $$N_{L|K}(x) = \prod_\sigma \sigma x.$$

Beweis: Das charakteristische Polynom $f_x(t)$ ist eine Potenz

$$f_x(t) = p_x(t)^d\,, \quad d = [L : K(x)]\,,$$

des Minimalpolynoms

$$p_x(t) = t^m + c_1 t^{m-1} + \cdots + c_m\,, \quad m = [\,K(x) : K\,]\,,$$

von x. In der Tat, $1, x, \ldots, x^{m-1}$ ist eine Basis von $K(x)|K$, und wenn $\alpha_1, \ldots, \alpha_d$ eine Basis von $L|K(x)$ ist, so ist

$$\alpha_1, \alpha_1 x, \ldots, \alpha_1 x^{m-1}; \ldots; \alpha_d, \alpha_d x, \ldots, \alpha_d x^{m-1}$$

eine Basis von $L|K$. Die Matrix der linearen Transformation $T_x : y \mapsto xy$ in dieser Basis ist offensichtlich kästchenweise eine Diagonalmatrix, wobei alle Kästchen gleich der Matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \cdots & -c_1 \end{pmatrix}$$

sind. Das zugehörige charakteristische Polynom ist, wie man leicht nachrechnet,

$$t^m + c_1 t^{m-1} + \cdots + c_m = p_x(t)\,,$$

so daß insgesamt $f_x(t) = p_x(t)^d$.

Die Menge $\mathrm{Hom}_K(L, \overline{K})$ der K-Einbettungen von L zerfällt nun unter der Relation

$$\sigma \sim \tau \iff \sigma x = \tau x$$

in m Äquivalenzklassen der Mächtigkeit d, und wenn $\sigma_1, \ldots, \sigma_m$ ein Repräsentantensystem ist, so ist

$$p_x(t) = \prod_{i=1}^{m} (t - \sigma_i x)$$

und $f_x(t) = \prod_{i=1}^m (t - \sigma_i x)^d = \prod_{i=1}^m \prod_{\sigma \sim \sigma_i} (t - \sigma x) = \prod_\sigma (t - \sigma x)$. Damit ist (i), und nach dem Vietaschen Wurzelsatz gleichzeitig (ii) und (iii) bewiesen. □

(2.7) Korollar. *Für einen Turm $K \subseteq L \subseteq M$ endlicher Erweiterungen gilt*

$$Tr_{L|K} \circ Tr_{M|L} = Tr_{M|K}\,,\ N_{L|K} \circ N_{M|L} = N_{M|K}\,.$$

Beweis: Wir nehmen an, daß $M|K$ separabel ist. Die Menge $\mathrm{Hom}_K(M, \overline{K})$ der K-Einbettungen von M zerfällt unter der Relation

$$\sigma \sim \tau \iff \sigma|_L = \tau|_L$$

in $m = [L : K]$ Äquivalenzklassen. Ist $\sigma_1, \ldots, \sigma_m$ ein Repräsentantensystem, so ist $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i|_L \mid i = 1, \ldots, m\}$ und

$$\begin{aligned} Tr_{M|K}(x) &= \sum_{i=1}^{m} \sum_{\sigma \sim \sigma_i} \sigma x = \sum_{i=1}^{m} Tr_{\sigma_i M|\sigma_i L}(\sigma_i x) = \sum_{i=1}^{m} \sigma_i Tr_{M|L}(x) \\ &= Tr_{L|K}(Tr_{M|L}(x)), \end{aligned}$$

und gleichermaßen für die Norm.

Den inseparablen Fall werden wir nicht zu betrachten haben. Er folgt aber leicht aus dem oben Bewiesenen durch Übergang zur maximalen separablen Teilerweiterung $M^s|K$. Für den Inseparabilitätsgrad $[M : K]_i = [M : M^s]$ hat man nämlich $[M : K]_i = [M : L]_i[L : K]_i$ und

$$Tr_{M|K}(x) = [M : K]_i Tr_{M^s|K}(x), \; N_{M|K}(x) = N_{M^s|K}(x)^{[M:K]_i}$$

(vgl. [143], vol I, Ch. II, § 10). □

Die **Diskriminante** einer Basis $\alpha_1, \ldots, \alpha_n$ der separablen Erweiterung $L|K$ ist durch

$$d(\alpha_1, ..., \alpha_n) = \det((\sigma_i \alpha_j))^2$$

gegeben, wobei σ_i, $i = 1, \ldots, n$, die K-Einbettungen $L \to \overline{K}$ durchläuft. Da die Matrix $(Tr_{L|K}(\alpha_i \alpha_j))$ wegen

$$Tr_{L|K}(\alpha_i \alpha_j) = \sum_k (\sigma_k \alpha_i)(\sigma_k \alpha_j)$$

das Produkt der Matrizen $(\sigma_k \alpha_i)^t$ und $(\sigma_k \alpha_j)$ ist, so kann man auch

$$d(\alpha_1, \ldots, \alpha_n) = \det(Tr_{L|K}(\alpha_i \alpha_j))$$

schreiben. In dem besonderen Fall einer Basis der Form $1, \theta, \ldots, \theta^{n-1}$ ist

$$d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2,$$

wobei $\theta_i = \sigma_i \theta$. Man sieht dies, indem man in der **Vandermondeschen Matrix**

$$\begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \cdots & \theta_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{pmatrix}$$

jede der $(n-1)$ ersten Spalten mit θ_1 multipliziert und von der folgenden subtrahiert und so fortfährt.

(2.8) Satz. *Ist $L|K$ separabel und $\alpha_1, \ldots, \alpha_n$ eine Basis, so ist die Diskriminante*

$$d(\alpha_1, \ldots, \alpha_n) \neq 0\,,$$

und es ist

$$(x, y) = Tr_{L|K}(xy)$$

eine nicht-ausgeartete Bilinearform auf dem K-Vektorraum L.

Beweis: Wir zeigen zunächst, daß die Bilinearform $(x, y) = Tr(xy)$ nicht-ausgeartet ist. Sei θ ein primitives Element für $L|K$, d.h. $L = K(\theta)$. Dann ist $1, \theta, \ldots, \theta^{n-1}$ eine Basis, bezüglich der die Form (x, y) durch die Matrix $M = (Tr_{L|K}(\theta^{i-1}\theta^{j-1}))_{i,j=1,\ldots,n}$ gegeben ist. Diese ist nicht-ausgeartet. denn wenn $\theta_i = \sigma_i\theta$ ist, so haben wir

$$\det(M) = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0\,.$$

Ist $\alpha_1, \ldots, \alpha_n$ eine beliebige Basis von $L|K$, so ist die Bilinearform (x, y) bzgl. dieser Basis durch die Matrix $M = (Tr_{L|K}(\alpha_i\alpha_j))$ gegeben. Nach dem Obigen ist somit $d(\alpha_1, \ldots, \alpha_n) = \det(M) \neq 0$. □

Nach diesem Rückblick auf die Körpertheorie kehren wir zurück zum ganzabgeschlossenen Integritätsbereich A mit dem Quotientenkörper K und seinem ganzen Abschluß B in der endlichen separablen Erweiterung $L|K$. Wenn $x \in B$ ein ganzes Element von L ist, so sind offenbar auch alle Konjugierten σx ganz. Beachtet man, daß A ganzabgeschlossen ist, d.h. $A = B \cap K$, so folgt aus (2.6)

$$Tr_{L|K}(x),\ N_{L|K}(x) \in A\,.$$

Überdies erhalten wir für die Einheitengruppe von B über A

$$x \in B^* \iff N_{L|K}(x) \in A^*\,.$$

Denn wenn $aN_{L|K}(x) = 1$ ist, $a \in A$, so ist $1 = a\prod_\sigma \sigma x = yx$ mit einem $y \in B$. Die Diskriminante findet eine häufige Anwendung durch das

(2.9) Lemma. *Sei $\alpha_1, \ldots, \alpha_n$ eine in B gelegene Basis von $L|K$ mit der Diskriminante $d = d(\alpha_1, \ldots, \alpha_n)$. Dann gilt*

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n\,.$$

Beweis: Ist $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \in B$, $a_j \in K$, so bilden die a_j eine Lösung des linearen Gleichungssystems

$$Tr_{L|K}(\alpha_i\alpha) = \sum_j Tr_{L|K}(\alpha_i\alpha_j)a_j$$

und sind deshalb wegen $Tr_{L|K}(\alpha_i\alpha) \in A$ als Quotient eines in A gelegenen Zählers und der Determinante $\det(Tr_{L|K}(\alpha_i\alpha_j)) = d$ gegeben. Daher ist $da_j \in A$, also

$$d\alpha \in A\alpha_1 + \cdots + A\alpha_n\,. \qquad \square$$

Unter einer **Ganzheitsbasis** von B über A (oder auch A-Basis von B) versteht man ein System von Elementen $\omega_1, \ldots, \omega_n \in B$, derart daß sich jedes $b \in B$ in eindeutiger Weise als Linearkombination

$$b = a_1\omega_1 + \cdots + a_n\omega_n$$

mit Koeffizienten $a_i \in A$ darstellen läßt. Da eine solche Ganzheitsbasis stets auch eine Basis von $L|K$ ist, so ist ihre Länge n immer gleich dem Körpergrad $[L : K]$. Die Existenz einer Ganzheitsbasis bedeutet also, daß B ein **freier A-Modul** vom Rang $n = [L : K]$ ist. Im allgemeinen gibt es aber keine Ganzheitsbasis. Ist jedoch A ein Hauptidealring, so hat man den weitergehenden

(2.10) Satz. *Ist $L|K$ separabel und A ein Hauptidealring, so ist jeder endlich erzeugte B-Untermodul $M \neq 0$ von L ein freier A-Modul vom Rang $[L : K]$. Insbesondere besitzt B eine Ganzheitsbasis über A.*

Beweis: Sei $M \neq 0$ ein endlich erzeugter B-Untermodul von L und $\alpha_1, \ldots, \alpha_n$ eine Basis von $L|K$. Durch Multiplikation mit einem Element aus A können wir erreichen, daß sie in B liegt. Nach (2.9) ist dann $dB \subseteq A\alpha_1 + \cdots + A\alpha_n$. Sei $\mu_1, \ldots, \mu_r \in M$ ein Erzeugendensystem des B-Moduls M. Es gibt ein $a \in A$ mit $a\mu_i \in B$, $i = 1, \ldots, r$, also $aM \subseteq B$. Damit ist

$$adM \subseteq dB \subseteq A\alpha_1 + \cdots + A\alpha_n = M_0\,.$$

Nach dem Hauptsatz für die Moduln über Hauptidealringen ist mit M_0 auch adM, also auch M ein freier A-Modul. Wegen

$$\mathrm{Rang}(M) = \mathrm{Rang}(dM) \leq \mathrm{Rang}(M_0) \leq \mathrm{Rang}(M)$$

ist $\mathrm{Rang}(M) = \mathrm{Rang}(M_0) = [L : K]$. $\square$

Ganzheitsbasen nachzuweisen ist i.a. ein schwieriges, aber in konkreten Situationen auch wichtiges Problem. Aus diesem Grund verdient der folgende Satz ein Interesse. Anstatt von Ganzheitsbasen des ganzen Abschlusses B von A in L sprechen wir dabei kurz von Ganzheitsbasen der Erweiterung $L|K$.

(2.11) Satz. *Seien $L|K$ und $L'|K$ zwei galoissche Erweiterungen von den Graden n bzw. n' mit $L \cap L' = K$. Sei $\omega_1, \ldots, \omega_n$ bzw. $\omega'_1, \ldots, \omega'_{n'}$ eine Ganzheitsbasis von $L|K$ bzw. $L'|K$ mit der Diskriminante d bzw. d'. Sind dann d und d' teilerfremd im Sinne von $xd + x'd' = 1$ für passende $x, x' \in A$, so ist $\omega_i\omega'_j$ eine Ganzheitsbasis von LL' mit der Diskriminante $d^{n'}d'^{n}$.*

Beweis: Wegen $L \cap L' = K$ ist $[LL' : K] = nn'$, so daß die nn' Produkte $\omega_i\omega'_j$ eine Basis von $LL'|K$ bilden. Sei nun α ein ganzes Element von LL' und

$$\alpha = \sum_{i,j} a_{ij}\omega_i\omega'_j\,, \quad a_{ij} \in K\,.$$

Wir haben zu zeigen, daß $a_{ij} \in A$. Sei dazu $\beta_j = \sum_i a_{ij}\omega_i$. Sei $G(LL'|L') = \{\sigma_1, \ldots, \sigma_n\}$ und $G(LL'|L) = \{\sigma'_1, \ldots, \sigma'_{n'}\}$, so daß

$$G(LL'|K) = \{\sigma_k\sigma'_l \mid k = 1, \ldots, n,\, l = 1, \ldots, n'\}\,.$$

Setzen wir

$$T = (\sigma'_l\omega'_j)\,, \quad a = (\sigma'_1\alpha, \ldots, \sigma'_{n'}\alpha)^t\,, \quad b = (\beta_1, \ldots, \beta_{n'})^t,$$

so ist $\det(T)^2 = d'$ und

$$a = Tb\,.$$

Sei T^* die zu T adjungierte Matrix. Dann folgt aus dem Laplaceschen Entwicklungssatz (2.3)

$$\det(T)b = T^*a\,.$$

Da T^* und a aus ganzen Elementen von LL' bestehen, so besteht $d'b$ aus ganzen Elementen $d'\beta_j = \sum_i d'a_{ij}\omega_i$ von L, so daß $d'a_{ij} \in A$. Indem man die Rolle von (ω_i) und (ω'_j) vertauscht, sieht man auf die gleiche Weise $da_{ij} \in A$, so daß

$$a_{ij} = xda_{ij} + x'd'a_{ij} \in A\,.$$

Daher ist $\omega_i\omega'_j$ in der Tat eine Ganzheitsbasis von $LL'|K$. Wir berechnen die Diskriminante Δ dieser Ganzheitsbasis . Wegen $G(LL'|K) = \{\sigma_k\sigma'_l \mid$

$k = 1, \ldots, n,\ l = 1, \ldots, n'\}$ ist sie das Quadrat der Determinante der $(nn' \times nn')$-Matrix

$$M = (\sigma_k \sigma'_l \omega_i \omega'_j) = (\sigma_k \omega_i \sigma'_l \omega'_j)\,.$$

Diese Matrix ist wiederum eine $(n' \times n')$-Matrix von $(n \times n)$-Matrizen, an deren (l, j)-Stelle die Matrix $Q\sigma'_l\omega'_j$ mit $Q = (\sigma_k\omega_i)$ steht. Daher ist

$$M = \begin{pmatrix} Q & & O \\ & \ddots & \\ O & & Q \end{pmatrix} \begin{pmatrix} E\sigma'_1\omega'_1 & \cdots & E\sigma'_{n'}\omega'_1 \\ \vdots & & \vdots \\ E\sigma'_1\omega'_{n'} & \cdots & E\sigma'_{n'}\omega'_{n'} \end{pmatrix}$$

wobei E die $(n \times n)$-Einheitsmatrix ist. Man bringt die zweite Matrix durch Umindizierung in die Form der ersten und erhält

$$\Delta = \det(M)^2 = \det(Q)^{2n'} \det((\sigma'_l\omega'_j))^{2n} = d^{n'} d'^{n}\,. \qquad \square$$

Bemerkung. Man kann dem Beweis entnehmen, daß der Satz für beliebige separable Erweiterungen (also nicht notwendig galoissche) gilt, wenn man anstelle von $L \cap L' = K$ die lineare Disjunktheit fordert.

Die wichtigste Anwendung unserer Betrachtungen über die Ganzheit bezieht sich auf den ganzen Abschluß $\mathcal{O}_K \subseteq K$ von $\mathbb{Z} \subseteq \mathbb{Q}$ in einem algebraischen Zahlkörper K. Nach dem Satz (2.10) besitzt jeder endlich erzeugte $\mathcal{O}_K$-Untermodul $\mathfrak{a}$ von K eine $\mathbb{Z}$-Basis $\alpha_1, \ldots, \alpha_n$,

$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n\,.$$

Die Diskriminante

$$d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i\alpha_j))^2$$

hängt nicht von der Wahl der $\mathbb{Z}$-Basis ab. Ist nämlich $\alpha'_1, \ldots, \alpha'_n$ eine andere Basis, so ist die Übergangsmatrix $T = (a_{ij})$, $\alpha'_i = \sum_j a_{ij}\alpha_j$, mit ihrer Inversen ganzzahlig, hat also die Determinante ± 1, so daß in der Tat

$$d(\alpha'_1, \ldots, \alpha'_n) = \det(T)^2 d(\alpha_1, \ldots, \alpha_n) = d(\alpha_1, \ldots, \alpha_n)\,.$$

Wir dürfen daher

$$d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n)$$

setzen. Im besonderen Fall einer Ganzheitsbasis $\omega_1, \ldots, \omega_n$ von $\mathcal{O}_K$ erhalten wir die **Diskriminante des Zahlkörpers** K,

$$d_K = d(\mathcal{O}_K) = d(\omega_1, \ldots, \omega_n)\,.$$

Man hat allgemein den

(2.12) Satz. *Sind $\mathfrak{a} \subseteq \mathfrak{a}'$ zwei von Null verschiedene, endlich erzeugte $\mathcal{O}_K$-Untermoduln von K, so ist der Index $(\mathfrak{a}' : \mathfrak{a})$ endlich, und es gilt*

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}') .$$

Man hat nur zu zeigen, daß der Index $(\mathfrak{a}' : \mathfrak{a})$ gleich dem Betrag der Determinante der Übergangsmatrix von einer $\mathbb{Z}$-Basis von $\mathfrak{a}$ zu einer $\mathbb{Z}$-Basis von $\mathfrak{a}'$ ist. Der Beweis gehört der wohlbekannten Theorie der endlich erzeugten $\mathbb{Z}$-Moduln an.

Aufgabe 1. Ist $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$ eine ganze algebraische Zahl?

Aufgabe 2. Zeige: Ist der Integritätsbereich A ganzabgeschlossen, so auch der Polynomring $A[t]$.

Aufgabe 3. Im Polynomring $A = \mathbb{Q}[X, Y]$ betrachte man das Hauptideal $\mathfrak{p} = (X^2 - Y^3)$. Man zeige, daß $\mathfrak{p}$ ein Primideal, $A/\mathfrak{p}$ aber nicht ganzabgeschlossen ist.

Aufgabe 4. Sei D eine quadratfreie ganze Zahl $\neq 0, 1$ und d die Diskriminante des quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{D})$. Zeige, daß

$$d = D \quad , \text{ wenn } D \equiv 1 \bmod 4 ,$$
$$d = 4D \quad , \text{ wenn } D \equiv 2 \text{ oder } 3 \bmod 4 ,$$

und daß $\{1, \sqrt{D}\}$ im zweiten Fall und $\{1, \frac{1}{2}(1 + \sqrt{D})\}$ im ersten eine Ganzheitsbasis ist, und $\{1, \frac{1}{2}(d + \sqrt{d})\}$ in jedem Fall.

Aufgabe 5. Zeige, daß $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ eine Ganzheitsbasis von $\mathbb{Q}(\sqrt[3]{2})$ ist.

Aufgabe 6. Zeige, daß $1, \theta, \frac{1}{2}(\theta + \theta^2)$ eine Ganzheitsbasis von $\mathbb{Q}(\theta)$, $\theta^3 - \theta - 4 = 0$, ist.

Aufgabe 7. Die Diskriminante d_K eines Zahlkörpers K ist stets $\equiv 0 \bmod 4$ oder $\equiv 1 \bmod 4$. (*Stickelbergerscher Diskriminantensatz*).

Hinweis: Die Determinante $\det(\sigma_i \omega_j)$ einer Ganzheitsbasis ω_j ist eine Summe von Termen, die mit einem Plus- oder Minuszeichen versehen sind. Ist P bzw. N die Summe der Terme mit Plus- bzw. Minuszeichen , so gilt $d_K = (P - N)^2 = (P + N)^2 - 4PN$.

§ 3. Ideale

Der Ring $\mathcal{O}_K$ der ganzen Zahlen eines algebraischen Zahlkörpers K ist als Verallgemeinerung des Ringes $\mathbb{Z} \subseteq \mathbb{Q}$ der Hauptgegenstand aller unserer Betrachtungen. Wie in $\mathbb{Z}$, so läßt sich auch in $\mathcal{O}_K$ jede Nicht-Einheit $\alpha \neq 0$ in ein Produkt von irreduziblen Elementen zerlegen. Denn wenn α nicht selbst irreduzibel ist, so zerfällt es in ein Produkt $\alpha = \beta\gamma$ von zwei Nicht-Einheiten, so daß nach § 2

$$1 < |N_{K|\mathbb{Q}}(\beta)| < |N_{K|\mathbb{Q}}(\alpha)|\,, \quad 1 < |N_{K|\mathbb{Q}}(\gamma)| < |N_{K|\mathbb{Q}}(\alpha)|$$

gilt und die Primzerlegung von α mit vollständiger Induktion aus der von β und γ folgt. Anders jedoch als in den Ringen $\mathbb{Z}$ und $\mathbb{Z}[i]$ findet die Eindeutigkeit der Primzerlegung im allgemeinen nicht statt.

Beispiel: Im Körper $K = \mathbb{Q}(\sqrt{-5})$ ist nach § 2, Aufgabe 4, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ der Ring der ganzen Zahlen. In ihm läßt sich die Zahl 21 auf zwei Weisen zerlegen ,

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})\,.$$

Alle Faktoren sind irreduzibel in $\mathcal{O}_K$. Wäre nämlich etwa $3 = \alpha\beta$, α, β Nicht-Einheiten, so würde aus $9 = N_{K|\mathbb{Q}}(\alpha)N_{K|\mathbb{Q}}(\beta)$ folgen, daß $N_{K|\mathbb{Q}}(\alpha) = \pm 3$ ist. Die Gleichung

$$N_{K|\mathbb{Q}}(x + y\sqrt{-5}) = x^2 + 5y^2 = \pm 3$$

ist aber in $\mathbb{Z}$ unlösbar. Ebenso zeigt man, daß 7, $1 + 2\sqrt{-5}$, $1 - 2\sqrt{-5}$ irreduzibel sind. Da die Brüche

$$\frac{1 \pm 2\sqrt{-5}}{3}\,, \quad \frac{1 \pm 2\sqrt{-5}}{7}$$

nicht in $\mathcal{O}_K$ liegen, sind die Zahlen 3 und 7 nicht assoziiert zu $1 + 2\sqrt{-5}$ oder $1 - 2\sqrt{-5}$. Es liegen also zwei verschiedene Primzerlegungen der Zahl 21 vor.

Die Betrachtung der Mehrdeutigkeit der Primzerlegung hat zu einem der großartigsten Ereignisse in der Geschichte der Zahlentheorie geführt, zur Entdeckung der Idealtheorie durch *Eduard Kummer*. Von der Erfindung der komplexen Zahlen geleitet, bestand die Kummersche Idee darin, daß es für die ganzen Zahlen in K einen erweiterten Bereich neuer „idealer Zahlen“ geben müsse, in dem sie sich **eindeutig** als Produkt „idealer Primzahlen“ darstellen würden. In dem Beispiel

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

etwa würden sich demnach die rechten Faktoren aus „idealen Primzahlen“ $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ zusammensetzen nach der Regel

$$3 = \mathfrak{p}_1\mathfrak{p}_2\,, \quad 7 = \mathfrak{p}_3\mathfrak{p}_4\,, \quad 1 + 2\sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3\,, \quad 1 - 2\sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4\,,$$

wodurch sich die obige Mehrdeutigkeit in die fabelhafte Eindeutigkeit

$$21 = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4)$$

auflösen würde.

Aus den von Kummer konzipierten „idealen Zahlen“ sind später die **Ideale** des Ringes $\mathcal{O}_K$ geworden. Der Grund hierfür ist leicht einzusehen. Wie immer eine ideale Zahl $\mathfrak{a}$ definiert ist, sie soll mit den Zahlen $a \in \mathcal{O}_K$ in einer Teilbarkeitsrelation $\mathfrak{a} \mid a$ stehen, die für $a, b, \lambda \in \mathcal{O}_K$ die Regeln

$$\mathfrak{a}|a \text{ und } \mathfrak{a}|b \;\Rightarrow\; \mathfrak{a}|a \pm b\,; \quad \mathfrak{a}|a \;\Rightarrow\; \mathfrak{a}|\lambda a$$

erfüllt, und sie soll durch die Gesamtheit

$$\underline{\mathfrak{a}} = \{a \in \mathcal{O}_K \mid \mathfrak{a}|a\}$$

aller Zahlen $a \in \mathcal{O}_K$, die sie teilt, eindeutig bestimmt sein. Diese Gesamtheit ist aber wegen der angegebenen Teilbarkeitsregeln ein Ideal von $\mathcal{O}_K$. Aus diesem Grund sind die Kummerschen „idealen Zahlen“ von *Richard Dedekind* als die Ideale von $\mathcal{O}_K$ eingeführt worden. Die Teilbarkeit $\mathfrak{a}|a$ kann dann einfach durch die Inklusion $a \in \mathfrak{a}$ definiert werden und allgemeiner die Teilbarkeit $\mathfrak{a}|\mathfrak{b}$ zwischen zwei Idealen durch $\mathfrak{b} \subseteq \mathfrak{a}$. Im folgenden wollen wir diesen Teilbarkeitsbegriff genauer studieren. Grundlegend dafür ist das

(3.1) Theorem. *Der Ring $\mathcal{O}_K$ ist noethersch, ganzabgeschlossen, und jedes Primideal $\mathfrak{p} \neq 0$ ist ein maximales Ideal.*

Beweis: $\mathcal{O}_K$ ist noethersch, weil jedes Ideal $\mathfrak{a}$ nach (2.10) ein endlich erzeugter $\mathbb{Z}$-Modul, erst recht also ein endlich erzeugter $\mathcal{O}_K$-Modul ist. Als ganzer Abschluß von $\mathbb{Z}$ ist $\mathcal{O}_K$ nach § 2 auch ganzabgeschlossen. Bleibt zu zeigen, daß jedes Primideal $\mathfrak{p} \neq 0$ maximal ist. Nun ist $\mathfrak{p} \cap \mathbb{Z}$ ein von Null verschiedenes Primideal (p) in $\mathbb{Z}$. Die Primidealeigenschaft ist klar, und wenn $y \in \mathfrak{p}$, $y \neq 0$, ist und

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0$$

eine Gleichung für y mit $a_i \in \mathbb{Z}$, $a_n \neq 0$, so ist $a_n \in \mathfrak{p} \cap \mathbb{Z}$. Der Integritätsbereich $\overline{\mathcal{O}} = \mathcal{O}_K/\mathfrak{p}$ entsteht aus $\kappa = \mathbb{Z}/p\mathbb{Z}$ durch Adjunktion

algebraischer Elemente und ist somit ein Körper (man erinnere sich an $\kappa[\alpha] = \kappa(\alpha)$, wenn α algebraisch ist). Daher ist $\mathfrak{p}$ ein maximales Ideal.□

Auf die drei soeben bewiesenen Eigenschaften des Ringes o_K gründet sich die ganze Teilbarkeitslehre seiner Ideale. Sie wurde von Dedekind entwickelt, der damit Anlaß gab zur folgenden

(3.2) Definition. *Ein noetherscher, ganzabgeschlossener Integritätsbereich, in dem jedes von Null verschiedene Primideal ein maximales Ideal ist, heißt* **Dedekindring**.

So wie die Ringe o_K als Verallgemeinerung des Ringes $\mathbb{Z}$ anzusehen sind, so kann man die Dedekindringe als Verallgemeinerung der Hauptidealringe ansehen. Ist nämlich A ein Hauptidealring mit dem Quotientenkörper K und $L|K$ eine endliche Körpererweiterung, so ist der ganze Abschluß B von A in L i.a. zwar kein Hauptidealring mehr, aber, wie wir noch zeigen werden, stets ein Dedekindring.

Anstelle des Ringes o_K betrachten wir im folgenden einen beliebigen Dedekindring o und bezeichnen mit K den Quotientenkörper von o. Für zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ von o (allgemeiner eines beliebigen Ringes) wird die Teilbarkeitsrelation $\mathfrak{a}|\mathfrak{b}$ durch $\mathfrak{b} \subseteq \mathfrak{a}$ definiert und ihre Summe durch

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\}.$$

Sie ist das kleinste $\mathfrak{a}$ und $\mathfrak{b}$ umfassende Ideal, also der $\mathrm{ggT}(\mathfrak{a}, \mathfrak{b})$ (größte gemeinsame Teiler) von $\mathfrak{a}$ und $\mathfrak{b}$. Entsprechend ist der Durchschnitt $\mathfrak{a} \cap \mathfrak{b}$ das kgV (kleinste gemeinsame Vielfache) von $\mathfrak{a}$ und $\mathfrak{b}$. Wir definieren das **Produkt** von $\mathfrak{a}$ und $\mathfrak{b}$ durch

$$\mathfrak{a}\mathfrak{b} = \{\sum_i a_i b_i \mid a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}\}.$$

Hinsichtlich dieser Multiplikation erhalten wir für die Ideale von o, was uns von den Elementen allein versagt wird, nämlich die **eindeutige Primzerlegung**.

(3.3) Theorem. *Jedes von (0) und (1) verschiedene Ideal $\mathfrak{a}$ von o besitzt eine bis auf die Reihenfolge eindeutige Zerlegung*

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

in Primideale $\mathfrak{p}_i$ von o.

Dieses Theorem liegt natürlich ganz im Sinne des Erfinders der „idealen Zahlen". Seine Gültigkeit ist aber dennoch erstaunlich, weil sein Beweis alles andere als offenkundig ist und eine tieferliegende Gesetzmäßigkeit zwischen den Zahlen in $\mathcal{O}$ aufdeckt. Wir schicken dem Beweis zwei Lemmata voraus.

(3.4) Lemma. *Zu jedem Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}$ gibt es von Null verschiedene Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ mit*

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r .$$

Beweis: Nehmen wir an, die Menge $\mathfrak{M}$ der sich dieser Bedingung widersetzenden Ideale wäre nicht leer. Da $\mathcal{O}$ noethersch ist, so bricht jede aufsteigende Idealkette ab. $\mathfrak{M}$ ist daher hinsichtlich der Inklusion induktiv geordnet und besitzt somit nach dem Zornschen Lemma ein maximales Element $\mathfrak{a}$. Dieses kann kein Primideal sein, d.h. es gibt Elemente $b_1, b_2 \in \mathcal{O}$ mit $b_1 b_2 \in \mathfrak{a}$, aber $b_1, b_2 \notin \mathfrak{a}$. Setzen wir $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$, $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$, so ist $\mathfrak{a} \underset{\neq}{\subset} \mathfrak{a}_1$, $\mathfrak{a} \underset{\neq}{\subset} \mathfrak{a}_2$ und $\mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a}$. Wegen der Maximalität enthalten $\mathfrak{a}_1$ und $\mathfrak{a}_2$ Primidealprodukte, deren Produkt in $\mathfrak{a}$ liegt, Widerspruch. □

(3.5) Lemma. *Ist $\mathfrak{p}$ ein Primideal von $\mathcal{O}$ und*

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}\},$$

so ist $\mathfrak{a}\mathfrak{p}^{-1} := \{\sum_i a_i x_i \mid a_i \in \mathfrak{a},\ x_i \in \mathfrak{p}^{-1}\} \neq \mathfrak{a}$ für jedes Ideal $\mathfrak{a} \neq 0$.

Beweis: Sei $a \in \mathfrak{p}$, $a \neq 0$, und $\mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$ mit minimalem r. Dann ist eines der $\mathfrak{p}_i$, etwa $\mathfrak{p}_1$, in $\mathfrak{p}$ enthalten, also $\mathfrak{p}_1 = \mathfrak{p}$ wegen der Maximalität von $\mathfrak{p}_1$. Denn sonst gäbe es für jedes i ein $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ mit $a_1 \ldots a_r \in \mathfrak{p}$. Wegen $\mathfrak{p}_2 \ldots \mathfrak{p}_r \not\subseteq (a)$ gibt es ein $b \in \mathfrak{p}_2 \ldots \mathfrak{p}_r$ mit $b \notin a\mathcal{O}$, also $a^{-1}b \notin \mathcal{O}$. Andererseits ist aber $b\mathfrak{p} \subseteq (a)$, also $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$, und somit $a^{-1}b \in \mathfrak{p}^{-1}$. Damit ist $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Sei nun $\mathfrak{a} \neq 0$ ein Ideal von $\mathcal{O}$ und $\alpha_1, \ldots, \alpha_n$ ein Erzeugendensystem. Nehmen wir an, daß $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Dann ist für jedes $x \in \mathfrak{p}^{-1}$

$$x\alpha_i = \sum_j a_{ij}\alpha_j , \quad a_{ij} \in \mathcal{O} .$$

Ist A die Matrix $(x\delta_{ij} - a_{ij})$, so ist also $A(\alpha_1, \ldots, \alpha_n)^t = 0$. Für die Determinante $d = \det(A)$ folgt nach (2.3) $d\alpha_1 = \cdots = d\alpha_n = 0$ und

somit $d = 0$. Daher ist x als Nullstelle des normierten Polynoms $f(X) = \det(X\delta_{ij} - a_{ij}) \in \mathfrak{o}[X]$ ganz über $\mathfrak{o}$, d.h. $x \in \mathfrak{o}$. Es ergibt sich somit $\mathfrak{p}^{-1} = \mathfrak{o}$, Widerspruch. □

Beweis von (3.3). I. **Existenz** der Primzerlegung. Sei $\mathfrak{M}$ die Menge aller von (0) und (1) verschiedenen Ideale, die keine Primzerlegung besitzen. Ist $\mathfrak{M}$ nicht leer, so schließen wir wie bei (3.4), daß es ein maximales Element $\mathfrak{a}$ in $\mathfrak{M}$ gibt. Es liegt in einem maximalen Ideal $\mathfrak{p}$, und wir erhalten wegen $\mathfrak{o} \subsetneq \mathfrak{p}^{-1}$

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{o}\,.$$

Nach (3.5) ist $\mathfrak{a} \underset{\neq}{\subset} \mathfrak{a}\mathfrak{p}^{-1}$ und $\mathfrak{p} \underset{\neq}{\subset} \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{o}$. Da $\mathfrak{p}$ ein maximales Ideal ist, so folgt $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$. Wegen der Maximalität von $\mathfrak{a}$ in $\mathfrak{M}$ und wegen $\mathfrak{a} \neq \mathfrak{p}$, also $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{o}$, besitzt $\mathfrak{a}\mathfrak{p}^{-1}$ eine Primzerlegung $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$, also auch $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \dots \mathfrak{p}_r\mathfrak{p}$, Widerspruch.
II. **Eindeutigkeit** der Primzerlegung. Für ein Primideal $\mathfrak{p}$ gilt: $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ $\Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$, d.h. $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a}$ oder $\mathfrak{p} \mid \mathfrak{b}$. Seien nun

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s$$

zwei Primzerlegungen von $\mathfrak{a}$. Dann teilt $\mathfrak{p}_1$ einen Faktor $\mathfrak{q}_i$, etwa $\mathfrak{q}_1$, und ist wegen der Maximalität $= \mathfrak{q}_1$. Wir multiplizieren mit $\mathfrak{p}_1^{-1}$ und erhalten wegen $\mathfrak{p}_1 \neq \mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathfrak{o}$

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s\,.$$

So fortfahrend erhalten wir $r = s$ und nach eventueller Umordnung $\mathfrak{p}_i = \mathfrak{q}_i\,, i = 1, \dots, r$. □

Faßt man in der Primzerlegung eines Ideals $\mathfrak{a} \neq 0$ von $\mathfrak{o}$ die gleichen Primideale zusammen, so erhält man eine Produktdarstellung

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r}\,, \quad \nu_i > 0\,.$$

Im folgenden soll jede solche Gleichung automatisch so verstanden sein, daß die $\mathfrak{p}_i$ paarweise verschieden sind. Ist insbesondere $\mathfrak{a}$ ein Hauptideal (a), so schreibt man, der Tradition folgend, die den Idealen den Charakter „idealer Zahlen“ beimißt, häufig etwas ungenau

$$a = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r}\,.$$

Auch verwendet man oft die Bezeichnung $\mathfrak{a}|a$ anstelle von $\mathfrak{a}|(a)$ und schreibt $(\mathfrak{a}, \mathfrak{b}) = 1$ bei zwei teilerfremden Idealen anstelle von $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b} = \mathfrak{o}$. Für ein Produkt $\mathfrak{a} = \mathfrak{a}_1 \dots \mathfrak{a}_n$ von teilerfremden Idealen

$\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ hat man ein Analogon des „chinesischen Restsatzes", wie er uns aus dem Bereich der ganzen Zahlen bekannt ist. Wir können diesen Satz für einen beliebigen Ring formulieren, wenn wir beachten, daß

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

ist. In der Tat, wegen $\mathfrak{a}_i | \mathfrak{a}$, $i = 1, \ldots, n$, ist nämlich einerseits $\mathfrak{a} \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$, und wenn $a \in \bigcap_i \mathfrak{a}_i$, so gilt $\mathfrak{a}_i | a$, und damit, wegen der Teilerfremdheit, $\mathfrak{a} = \mathfrak{a}_1 \ldots \mathfrak{a}_n | a$, d.h. $a \in \mathfrak{a}$.

(3.6) Chinesischer Restsatz. *Seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ Ideale in einem Ring $\mathcal{O}$ mit $\mathfrak{a}_i + \mathfrak{a}_j = \mathcal{O}$ für $i \neq j$. Ist dann $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}_i$, so ist*

$$\mathcal{O}/\mathfrak{a} \cong \bigoplus_{i=1}^{n} \mathcal{O}/\mathfrak{a}_i .$$

Beweis: Der kanonische Homomorphismus

$$\mathcal{O} \to \bigoplus_{i=1}^{n} \mathcal{O}/\mathfrak{a}_i , \quad a \mapsto \bigoplus_{i=1}^{n} a \bmod \mathfrak{a}_i ,$$

besitzt den Kern $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$, so daß es genügt, die Surjektivität zu zeigen. Sei dazu $x_i \bmod \mathfrak{a}_i \in \mathcal{O}/\mathfrak{a}_i$, $i = 1, \ldots, n$, gegeben. Ist $n = 2$, so können wir $1 = a_1 + a_2$ schreiben, $a_i \in \mathfrak{a}_i$, und wenn wir $x = x_1 a_1 + x_2 a_2$ setzen, so ist $x \equiv x_i \bmod \mathfrak{a}_i$, $i = 1, 2$.

Ist $n > 2$, so finden wir hiernach ein Element $y_1 \in \mathcal{O}$ mit

$$y_1 \equiv 1 \bmod \mathfrak{a}_1 , \quad y_1 \equiv 0 \bmod \bigcap_{i=2}^{n} \mathfrak{a}_i ,$$

und analog Elemente $y_2, \ldots, y_n$, so daß

$$y_i \equiv 1 \bmod \mathfrak{a}_i , \quad y_i \equiv 0 \bmod \mathfrak{a}_j \quad \text{für } i \neq j.$$

Setzen wir $x = x_1 y_1 + \cdots + x_n y_n$, so ist $x \equiv x_i \bmod \mathfrak{a}_i$, $i = 1, \ldots, n$. Damit ist die Surjektivität bewiesen. □

Sei jetzt wieder $\mathcal{O}$ ein Dedekindring. Für die von Null verschiedenen Ideale von $\mathcal{O}$ erhalten wir wie bei den Zahlen multiplikative **Inverse**, wenn wir den Begriff der gebrochenen Ideale im Quotientenkörper K einführen.

(3.7) Definition. *Ein* **gebrochenes Ideal** *von K ist ein endlich erzeugter $\mathcal{O}$-Untermodul $\mathfrak{a} \neq 0$ von K.*

Für ein Element $a \in K^*$ ist z.B. $(a) = a\mathcal{O}$ ein gebrochenes „Hauptideal". Da $\mathcal{O}$ noethersch ist, so ist ein $\mathcal{O}$-Untermodul $\mathfrak{a} \neq 0$ von K offenbar genau dann ein gebrochenes Ideal, wenn es ein $c \in \mathcal{O}$, $c \neq 0$, gibt mit $c\mathfrak{a} \subseteq \mathcal{O}$. Die gebrochenen Ideale werden genauso multipliziert wie die Ideale von $\mathcal{O}$. Letztere bezeichnen wir von nun an auch als die **ganzen Ideale** von K.

(3.8) Satz. *Die gebrochenen Ideale bilden eine abelsche Gruppe, die* **Idealgruppe** J_K *von* K. *Das Einselement ist* $(1) = \mathcal{O}$, *und das Inverse zu* $\mathfrak{a}$ *ist*

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}.$$

Beweis: Assoziativität, Kommutativität und $\mathfrak{a}(1) = \mathfrak{a}$ sind klar. Für ein Primideal $\mathfrak{p}$ ist nach (3.5) $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$, also $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ wegen der Maximalität von $\mathfrak{p}$. Ist $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ ein ganzes Ideal, so ist hiernach $\mathfrak{b} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1}$ ein Inverses. Wegen $\mathfrak{b}\mathfrak{a} = \mathcal{O}$ ist $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Ist umgekehrt $x\mathfrak{a} \subseteq \mathcal{O}$, so ist $x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, also $x \in \mathfrak{b}$ wegen $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Daher ist $\mathfrak{b} = \mathfrak{a}^{-1}$. Ist $\mathfrak{a}$ ein gebrochenes Ideal und $c \in \mathcal{O}$, $c \neq 0$, mit $c\mathfrak{a} \subseteq \mathcal{O}$, so ist $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ das Inverse von $c\mathfrak{a}$, also $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. □

(3.9) Korollar. *Jedes gebrochene Ideal* $\mathfrak{a}$ *besitzt eine eindeutige Produktdarstellung*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}$$

mit $\nu_\mathfrak{p} \in \mathbb{Z}$ *und* $\nu_\mathfrak{p} = 0$ *für fast alle* $\mathfrak{p}$. *Mit anderen Worten:* J_K *ist die durch die Primideale* $\mathfrak{p} \neq 0$ *erzeugte freie abelsche Gruppe.*

Beweis: Jedes gebrochene Ideal $\mathfrak{a}$ ist Quotient $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$ zweier ganzer Ideale $\mathfrak{b}$ und $\mathfrak{c}$, die nach (3.3) eine Primzerlegung besitzen. Daher besitzt $\mathfrak{a}$ eine Primzerlegung im Sinne des Korollars. Sie ist nach (3.3) eindeutig, wenn $\mathfrak{a}$ ganz ist, und damit evidenterweise auch im allgemeinen Fall. □

Die gebrochenen Hauptideale $(a) = a\mathcal{O}$, $a \in K^*$, bilden eine Untergruppe der Idealgruppe J_K. Sie wird mit P_K bezeichnet. Die Faktorgruppe

$$Cl_K = J_K/P_K$$

heißt die **Idealklassengruppe**, oder auch kurz **Klassengruppe** von K. Sie steht zusammen mit der Einheitengruppe $\mathcal{O}^*$ von $\mathcal{O}$ in der exakten Sequenz

$$1 \to \mathcal{O}^* \to K^* \to J_K \to Cl_K \to 1\,,$$

wobei der mittlere Pfeil durch $a \mapsto (a)$ gegeben ist. Die Klassengruppe Cl_K beschreibt also die Größe der Ausdehnung und die Einheitengruppe $\mathcal{O}^*$ die des Verlustes, die der Bereich der Zahlen beim Übergang zu den Idealen erfahren hat. Es ist uns damit die unmittelbare Aufgabe gestellt, die Gruppen $\mathcal{O}^*$ und Cl_K genauer zu erfassen. Bei allgemeinen Dedekindringen können sie ganz beliebig ausfallen. Beim Ring $\mathcal{O}_K$ der ganzen Zahlen eines Zahlkörpers K erhält man jedoch wichtige Endlichkeitsaussagen, die für die weitere Entwicklung der Zahlentheorie von grundlegender Bedeutung sind. Diese Ergebnisse fallen einem aber nicht leicht zu. Sie werden erhalten durch eine geometrische Betrachtung der Zahlen als Gitterpunkte im Raum, für die wir jetzt die nötigen, ganz der linearen Algebra angehörenden Begriffsbildungen bereitstellen wollen.

Aufgabe 1. Zerlege $33 + 11\sqrt{-7}$ in irreduzible ganze Elemente von $\mathbb{Q}(\sqrt{-7})$.

Aufgabe 2. Zeige, daß

$$54 = 2 \cdot 3^3 = \frac{13 + \sqrt{-47}}{2} \cdot \frac{13 - \sqrt{-47}}{2}$$

zwei verschiedene Zerlegungen in irreduzible ganze Elemente in $\mathbb{Q}(\sqrt{-47})$ sind.

Aufgabe 3. Sei d quadratfrei und p eine zu $2d$ teilerfremde Primzahl. Sei $\mathcal{O}$ der Ring der ganzen Zahlen von $\mathbb{Q}(\sqrt{d})$. Zeige, daß $(p) = p\mathcal{O}$ genau dann ein Primideal in $\mathcal{O}$ ist, wenn die Kongruenz $x^2 \equiv d \bmod p$ unlösbar ist.

Aufgabe 4. Ein Dedekindring mit nur endlich vielen Primidealen ist ein Hauptidealring.

Hinweis: Ist $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r} \neq 0$ ein Ideal, so wähle Elemente $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$ und wende den chinesischen Restsatz auf die Restklassen $\pi_i^{\nu_i} \bmod \mathfrak{p}_i^{\nu_i+1}$ an.

Aufgabe 5. Der Restklassenring $\mathcal{O}/\mathfrak{a}$ eines Dedekindringes nach einem Ideal $\mathfrak{a} \neq 0$ ist ein Hauptidealring.

Hinweis: Für $\mathfrak{a} = \mathfrak{p}^n$ sind $\mathfrak{p}/\mathfrak{p}^n, \dots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$ die einzigen echten Ideale von $\mathcal{O}/\mathfrak{a}$. Wähle $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ und zeige $\mathfrak{p}^\nu = \mathcal{O}\pi^\nu + \mathfrak{p}^n$.

Aufgabe 6. Jedes Ideal eines Dedekindringes läßt sich durch zwei Elemente erzeugen.

Hinweis: Verwende Aufgabe 5.

Aufgabe 7. In einem noetherschen Ring R, in dem jedes Primideal maximal ist, wird jede absteigende Idealkette $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \dots$ stationär.

Hinweis: Zeige wie in (3.4), daß (0) ein Produkt $\mathfrak{p}_1 \dots \mathfrak{p}_r$ von Primidealen ist und daß sich die Kette $R \supseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_1\mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r = (0)$ zu einer Kompositionsreihe verfeinern läßt.

Aufgabe 8. Sei $\mathfrak{m}$ ein ganzes Ideal $\neq 0$ des Dedekindringes $\mathfrak{o}$. Zeige, daß in jeder Idealklasse von Cl_K ein ganzes, zu $\mathfrak{m}$ teilerfremdes Ideal liegt.

Aufgabe 9. Sei $\mathfrak{o}$ ein Ring, dessen von Null verschiedene Ideale eindeutige Primidealzerlegungen besitzen. Zeige, daß $\mathfrak{o}$ ein Dedekindring ist.

Aufgabe 10. Die gebrochenen Ideale $\mathfrak{a}$ eines Dedekindringes $\mathfrak{o}$ sind projektive $\mathfrak{o}$-Moduln, d.h. zu jedem surjektiven Homomorphismus $M \xrightarrow{f} N$ von $\mathfrak{o}$-Moduln läßt sich jeder Homomorphismus $\mathfrak{a} \xrightarrow{g} N$ zu einem Homomorphismus $h : \mathfrak{a} \to M$ mit $f \circ h = g$ hochheben.

§ 4. Gitter

In § 1 haben wir bei der Lösung der Grundprobleme über die Gaußschen Zahlen an wesentlicher Stelle die Inklusion

$$\mathbb{Z}[i] \subseteq \mathbb{C}$$

benützt und haben die ganzen Zahlen von $\mathbb{Q}(i)$ als Gitterpunkte in der komplexen Ebene angesehen. Diese Betrachtungsweise ist von *Hermann Minkowski* (1864–1909) auf beliebige Zahlkörper ausgedehnt worden und hat zu Resultaten geführt, auf die sich die algebraische Zahlentheorie in entscheidender Weise gründet. Um die Minkowskische Theorie zu entwickeln, müssen wir zunächst den allgemeinen Begriff des Gitters einführen und einige seiner grundsätzlichen Eigenschaften studieren.

(4.1) Definition. *Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum. Ein* **Gitter** *in V ist eine Untergruppe der Form*

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

mit linear unabhängigen Vektoren $v_1, \dots, v_m$ von V. Das m-Tupel $(v_1, \dots, v_m)$ heißt eine **Basis** *und die Menge*

$$\Phi = \{x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R}, \quad 0 \leq x_i < 1\}$$

eine **Grundmasche** *des Gitters. Das Gitter heißt* **vollständig** *oder eine* **$\mathbb{Z}$-Struktur** *von V, wenn $m = n$ ist.*

Die Vollständigkeit des Gitters ist offenbar gleichbedeutend damit, daß die sämtlichen Verschiebungen $\Phi + \gamma$, $\gamma \in \Gamma$, der Grundmasche den ganzen Raum V überdecken.

Die obige Definition bezieht sich auf die Wahl linear unabhängiger Vektoren. Wir benötigen aber eine von solcher Wahl unabhängige Charakterisierung der Gitter. Ein Gitter ist zunächst einmal eine endlich erzeugte Untergruppe von V. Aber nicht jede endlich erzeugte Untergruppe ist auch ein Gitter, z.B. $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subseteq \mathbb{R}$ nicht. Jedes Gitter $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ hat jedoch die besondere Eigenschaft, eine **diskrete** Untergruppe von V zu sein. Das soll heißen, daß jeder Punkt $\gamma \in \Gamma$ ein isolierter Punkt ist, also eine Umgebung besitzt, die keinen weiteren Punkt von Γ enthält. Ist nämlich

$$\gamma = a_1 v_1 + \cdots + a_m v_m \in \Gamma$$

und ergänzen wir $v_1, \ldots, v_m$ zu einer Basis $v_1, \ldots, v_n$ von V, so ist offenbar

$$\{x_1 v_1 + \cdots + x_n v_n \mid x_i \in \mathbb{R}, \quad |a_i - x_i| < 1 \quad \text{für } i = 1, \ldots, m\}$$

eine solche Umgebung. Diese Eigenschaft ist ausschlaggebend.

(4.2) Satz. *Eine Untergruppe $\Gamma \subseteq V$ ist genau dann ein Gitter, wenn sie diskret ist.*

Beweis: Sei Γ eine diskrete Untergruppe von V. Sei V_0 der lineare Unterraum von V, der durch die Menge Γ aufgespannt wird, und m seine Dimension. Dann können wir eine in Γ gelegene Basis $u_1, \ldots, u_m$ von V_0 wählen und bilden damit das vollständige Gitter

$$\Gamma_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subseteq \Gamma$$

von V_0. Wir behaupten, daß der Index $(\Gamma : \Gamma_0)$ endlich ist. Zum Beweis durchlaufe $\gamma_i \in \Gamma$ ein Repräsentantensystem für die Nebenklassen in Γ/Γ_0. Da Γ_0 vollständig ist in V_0, so überdecken die Verschiebungen $\Phi_0 + \gamma$, $\gamma \in \Gamma_0$, der Grundmasche

$$\Phi_0 = \{x_1 u_1 + \cdots + x_m u_m \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1\}$$

den ganzen Raum V_0. Daher können wir

$$\gamma_i = \mu_i + \gamma_{0i}, \quad \mu_i \in \Phi_0, \quad \gamma_{0i} \in \Gamma_0 \subseteq V_0,$$

schreiben. Da die $\mu_i = \gamma_i - \gamma_{0i} \in \Gamma$ diskret in der beschränkten Menge Φ_0 liegen, so muß ihre Anzahl endlich sein.

Setzen wir nun $q = (\Gamma : \Gamma_0)$, so ist $q\Gamma \subseteq \Gamma_0$, also

$$\Gamma \subseteq \frac{1}{q}\Gamma_0 = \mathbb{Z}\Big(\frac{1}{q}u_1\Big) + \cdots + \mathbb{Z}\Big(\frac{1}{q}u_m\Big).$$

Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen besitzt Γ daher eine $\mathbb{Z}$-Basis $v_1, \ldots, v_r$, $r \leq m$, d.h. $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r$. Die Vektoren $v_1, \ldots, v_r$ sind überdies $\mathbb{R}$-linear unabhängig, da sie den m-dimensionalen Raum V_0 aufspannen. Daher ist Γ ein Gitter. □

Wir beweisen als nächstes ein Kriterium, das uns sagt, wann ein Gitter im Raum V, gegeben etwa als eine diskrete Untergruppe $\Gamma \subseteq V$, vollständig ist.

(4.3) Lemma. *Ein Gitter Γ in V ist genau dann vollständig, wenn es eine beschränkte Teilmenge $M \subseteq V$ gibt, deren sämtliche Verschiebungen $M + \gamma$, $\gamma \in \Gamma$, den ganzen Raum V überdecken.*

Beweis: Ist $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ vollständig, so kann man für M die Grundmasche $\Phi = \{x_1v_1 + \cdots + x_nv_n \mid 0 \leq x_i < 1\}$ wählen.

Sei andererseits M eine beschränkte Teilmenge von V, deren Verschiebungen $M + \gamma$, $\gamma \in \Gamma$, den Raum V überdecken. Sei V_0 der durch Γ aufgespannte Unterraum. Wir müssen zeigen, daß $V = V_0$ ist. Sei dazu $v \in V$. Wegen $V = \bigcup_{\gamma \in \Gamma}(M + \gamma)$ können wir für jedes $\nu \in \mathbb{N}$ schreiben

$$\nu v = a_\nu + \gamma_\nu\,, \quad a_\nu \in M\,, \quad \gamma_\nu \in \Gamma \subseteq V_0\,.$$

Da M beschränkt ist, ist $\frac{1}{\nu}a_\nu$ eine Nullfolge, und es folgt wegen der Abgeschlossenheit von V_0,

$$v = \lim_{\nu\to\infty} \frac{1}{\nu}a_\nu + \lim_{\nu\to\infty} \frac{1}{\nu}\gamma_\nu = \lim_{\nu\to\infty} \frac{1}{\nu}\gamma_\nu \in V_0\,. \qquad \square$$

Sei jetzt V ein *euklidischer* Vektorraum, also ein $\mathbb{R}$-Vektorraum endlicher Dimension n mit einer symmetrischen, positiv definiten Bilinearform

$$\langle\ ,\ \rangle : V \times V \to \mathbb{R}\,.$$

Auf V haben wir dann einen Volumenbegriff – genauer ein Haarsches Maß. Der von einer Orthonormalbasis $e_1, \ldots, e_n$ aufgespannte Würfel erhält den Inhalt 1, und allgemeiner das von n linear unabhängigen Vektoren $v_1, \ldots, v_n$ aufgespannte Parallelepiped

$$\Phi = \{x_1v_1 + \cdots + x_nv_n \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1\}$$

den Inhalt

$$\mathrm{vol}(\Phi) = |\det A|\,,$$

wenn $A = (a_{ik})$ die Übergangsmatrix der Basis $e_1, \ldots, e_n$ zu $v_1, \ldots, v_n$ ist, d.h. $v_i = \sum_k a_{ik} e_k$. Wegen

$$(\langle v_i, v_j \rangle) = (\sum_{k,l} a_{ik} a_{jl} \langle e_k, e_l \rangle) = (\sum_k a_{ik} a_{jk}) = AA^t$$

kann man auch in invarianter Weise

$$\mathrm{vol}(\Phi) = |\det(\langle v_i, v_j \rangle)|^{1/2}$$

schreiben.

Sei Γ das von $v_1, \ldots, v_n$ aufgespannte Gitter. Φ ist dann eine Grundmasche von Γ, und wir setzen kurz

$$\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi)\,.$$

Dies hängt nicht von der Wahl der Gitterbasis $v_1, \ldots, v_n$ ab, weil die Übergangsmatrix zu einer anderen mit ihrer Inversen ganzzahlige Koeffizienten hat, also eine Determinante ± 1, so daß sie die Menge Φ in eine Menge gleichen Inhalts transformiert.

Wir kommen nun zum wichtigsten Satz über die Gitter. Eine Teilmenge X von V heißt *zentralsymmetrisch*, wenn sie mit jedem Punkt x auch den Punkt $-x$ enthält, und *konvex*, wenn sie mit je zwei Punkten x, y auch die Strecke $\{ty + (1-t)x \mid 0 \leq t \leq 1\}$ von x nach y enthält. Mit diesen Definitionen gilt jetzt der

(4.4) Minkowskische Gitterpunktsatz. *Sei Γ ein vollständiges Gitter im euklidischen Vektorraum V und X eine zentralsymmetrische und konvexe Teilmenge von V. Ist dann*

$$\mathrm{vol}(X) > 2^n \,\mathrm{vol}(\Gamma)\,,$$

so enthält X mindestens einen von Null verschiedenen Gitterpunkt $\gamma \in \Gamma$.

Beweis: Es genügt zu zeigen, daß es zwei verschiedene Gitterpunkte $\gamma_1, \gamma_2 \in \Gamma$ gibt mit

$$\left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \emptyset\,.$$

Wählen wir nämlich dann einen Punkt aus diesem Durchschnitt aus,

$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2\,, \quad x_1, x_2 \in X\,,$$

so ist

$$\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1$$

der Mittelpunkt der Strecke von x_2 nach $-x_1$, liegt also in $X \cap \Gamma$.

Wären nun die Mengen $\frac{1}{2}X + \gamma$, $\gamma \in \Gamma$, paarweise disjunkt, so träfe dies auch auf ihre Durchschnitte $\Phi \cap (\frac{1}{2}X + \gamma)$ mit einer Grundmasche Φ von Γ zu, d.h. es wäre

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}\Big(\Phi \cap \Big(\frac{1}{2}X + \gamma\Big)\Big)\,.$$

Da durch die Translation mit $-\gamma$ aus $\Phi \cap (\frac{1}{2}X + \gamma)$ die Menge $(\Phi - \gamma) \cap \frac{1}{2}X$ von gleichem Volumen entsteht, und da die $\Phi - \gamma$, $\gamma \in \Gamma$, den ganzen Raum V, also auch die Menge $\frac{1}{2}X$ überdecken, so würden wir

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}\Big((\Phi - \gamma) \cap \frac{1}{2}X\Big) = \mathrm{vol}\Big(\frac{1}{2}X\Big) = \frac{1}{2^n}\,\mathrm{vol}(X)$$

erhalten, im Gegensatz zur Voraussetzung. □

Aufgabe 1. Zeige, daß ein Gitter Γ im $\mathbb{R}^n$ genau dann vollständig ist, wenn die Faktorgruppe $\mathbb{R}^n/\Gamma$ kompakt ist.

Aufgabe 2. Man zeige, daß der Minkowskische Gitterpunktsatz nicht verbessert werden kann, indem man eine konvexe, zentralsymmetrische Menge $X \subseteq V$ mit $\mathrm{vol}(X) = 2^n \mathrm{vol}(\Gamma)$ angibt, die keinen von Null verschiedenen Punkt von Γ enthält. Ist aber X kompakt, so ist in (4.4) auch das Gleichheitszeichen zulässig.

Aufgabe 3. (Minkowskischer Linearformensatz). Seien

$$L_i(x_1, \ldots, x_n) = \sum_{j=1}^{n} a_{ij}x_j\,, \quad i = 1, \ldots, n,$$

reelle Linearformen mit $\det(a_{ij}) \neq 0$ und $c_1, \ldots, c_n$ positive reelle Zahlen mit $c_1 \ldots c_n > |\det(a_{ij})|$. Zeige, daß es ganze Zahlen $m_1, \ldots, m_n \in \mathbb{Z}$ gibt mit

$$|L_i(m_1, \ldots, m_n)| < c_i\,, \quad i = 1, \ldots, n.$$

Hinweis: Wende den Minkowskischen Gitterpunktsatz an.

§ 5. Minkowski-Theorie

Der Hauptgedanke der Minkowskischen Betrachtungsweise eines algebraischen Zahlkörpers $K|\mathbb{Q}$ vom Grade n besteht in der Interpretation seiner Zahlen als Punkte im n-dimensionalen Raum. Aus diesem Grund ist diese Theorie als „Geometrie der Zahlen" bezeichnet worden. Es ist aber angebracht, der heutigen Tendenz zu folgen und sie „Minkowski-Theorie" zu nennen, weil man inzwischen zu einer geometrischen Auffassung der Zahlentheorie in einem ganz anderen und viel umfassenderen Sinne gelangt ist. Diese werden wir in § 13 erläutern. Hier betrachten wir die kanonische Abbildung

$$j : K \to K_{\mathbb{C}} := \prod_{\tau} \mathbb{C}\,, \quad a \mapsto ja = (\tau a)\,,$$

die sich durch die n komplexen Einbettungen $\tau : K \to \mathbb{C}$ ergibt. Der $\mathbb{C}$-Vektorraum $K_{\mathbb{C}}$ ist mit dem *hermiteschen Skalarprodukt*

$$(*) \qquad \langle x, y\rangle = \sum_{\tau} x_\tau \bar{y}_\tau$$

ausgestattet, wobei daran erinnert sei, daß ein hermitesches Skalarprodukt durch eine im ersten Argument lineare Form $H(x,y)$ gegeben ist, derart daß $\overline{H(x,y)} = H(y,x)$ und $H(x,x) > 0$ für $x \neq 0$. Wir sehen im folgenden $K_{\mathbb{C}}$ stets als den mit der „Standardmetrik" $(*)$ versehenen hermiteschen Raum an.

Die Galoisgruppe $G(\mathbb{C}\,|\,\mathbb{R})$ wird durch die komplexe Konjugation

$$F : z \mapsto \bar{z}$$

erzeugt. Die Bezeichnung F wird ihre Erklärung erst später finden (vgl. Kap. III, § 4). F operiert einerseits auf den Faktoren des Produktes $\prod_\tau \mathbb{C}$, andererseits aber auch auf der Menge der τ, durch die sie indiziert sind; jeder Einbettung $\tau : K \to \mathbb{C}$ ist die komplex konjugierte $\bar{\tau} : K \to \mathbb{C}$ zugeordnet. Insgesamt ergibt sich hieraus eine Involution

$$F : K_{\mathbb{C}} \to K_{\mathbb{C}}\,,$$

die auf den Punkten $z = (z_\tau) \in K_{\mathbb{C}}$ durch

$$(Fz)_\tau = \bar{z}_{\bar{\tau}}$$

gegeben ist. Das Skalarprodukt $\langle\ ,\ \rangle$ ist unter F invariant, d.h.

$$\langle Fx, Fy\rangle = F\langle x, y\rangle\,.$$

Auf dem $\mathbb{C}$-Vektorraum $K_{\mathbb{C}} = \prod_\tau \mathbb{C}$ haben wir schließlich noch die lineare Abbildung

$$Tr : K_{\mathbb{C}} \to \mathbb{C}\,,$$

die durch die Summe der Koordinaten gegeben ist; auch sie ist F-invariant. Das Kompositum

$$K \xrightarrow{j} K_{\mathbb{C}} \xrightarrow{Tr} \mathbb{C}$$

ergibt die übliche Spur von $K|\mathbb{Q}$ (vgl. (2.6), ii),

$$Tr_{K|\mathbb{Q}}(a) = Tr\,(ja)\,.$$

Unser Augenmerk gilt jetzt dem $\mathbb{R}$-Vektorraum

$$K_{\mathbb{R}} = K_{\mathbb{C}}^{+} = [\prod_{\tau} \mathbb{C}\,]^{+}$$

der unter $G(\mathbb{C}\,|\,\mathbb{R})$, d.h. unter F invarianten Punkte von $K_{\mathbb{C}}$, also der Punkte (z_τ) mit $z_{\bar\tau} = \bar z_\tau$. Wegen $\bar\tau a = \overline{\tau a}$ für $a \in K$ ist $F(ja) = ja$, so daß wir eine Abbildung

$$j : K \to K_{\mathbb{R}}$$

erhalten. Die Einschränkung des hermiteschen Skalarprodukts $\langle\ ,\ \rangle$ von $K_{\mathbb{C}}$ auf $K_{\mathbb{R}}$ wird ein Skalarprodukt

$$\langle\ ,\ \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$$

auf dem $\mathbb{R}$-Vektorraum $K_{\mathbb{R}}$, denn für $x, y \in K_{\mathbb{R}}$ gilt $\langle x, y\rangle \in \mathbb{R}$ wegen $F\langle x, y\rangle = \langle Fx, Fy\rangle = \langle x, y\rangle$, ferner $\langle x, y\rangle = \overline{\langle x, y\rangle} = \langle y, x\rangle$ und $\langle x, x\rangle > 0$ für $x \neq 0$ ohnehin.

Wir nennen den *euklidischen* Vektorraum

$$K_{\mathbb{R}} = [\prod_{\tau} \mathbb{C}\,]^{+}$$

den **Minkowski-Raum**, sein Skalarprodukt $\langle\ ,\ \rangle$ die **kanonische Metrik** und das zugehörige Haarsche Maß (vgl. § 4, S. 27) das **kanonische Maß**. Wegen $Tr \circ F = F \circ Tr$ haben wir auf $K_{\mathbb{R}}$ die $\mathbb{R}$-lineare Abbildung

$$Tr : K_{\mathbb{R}} \to \mathbb{R}\,,$$

und es ist das Kompositum derselben mit $j : K \to K_{\mathbb{R}}$ wieder die übliche Spur von $K|\mathbb{Q}$,

$$Tr_{K|\mathbb{Q}}(a) = Tr(ja)\,.$$

Bemerkung: Ohne im weiteren Bezug darauf zu nehmen, erwähnen wir, daß die Abbildung $j : K \to K_{\mathbb{R}}$ den Vektorraum $K_{\mathbb{R}}$ mit dem Tensorprodukt $K \otimes_{\mathbb{Q}} \mathbb{R}$ identifiziert,

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} K_{\mathbb{R}}\,,\ a \otimes x \mapsto (ja)x\,,$$

und ebenso $K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} K_{\mathbb{C}}$. Der Inklusion $K_{\mathbb{R}} \subseteq K_{\mathbb{C}}$ entspricht bei dieser Interpretation die kanonische Abbildung $K \otimes_{\mathbb{Q}} \mathbb{R} \to K \otimes_{\mathbb{Q}} \mathbb{C}$, die durch die Inklusion $\mathbb{R} \hookrightarrow \mathbb{C}$ induziert wird, und es geht F über in $F(a \otimes z) = a \otimes \bar{z}$.

Explizit läßt sich der Minkowski-Raum $K_{\mathbb{R}}$ wie folgt beschreiben. Von den Einbettungen $\tau : K \to \mathbb{C}$ sind manche reell, d.h. sie fallen schon in $\mathbb{R}$ hinein, und manche komplex, d.h. nicht-reell. Seien

$$\rho_1, \ldots, \rho_r : K \to \mathbb{R}$$

die reellen. Die komplexen gruppieren sich zu Paaren

$$\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s : K \to \mathbb{C}$$

komplex konjugierter Einbettungen, so daß $n = r + 2s$. Aus jedem Paar wählen wir eine feste komplexe Einbettung aus und lassen ρ die Familie der reellen und σ die Familie der ausgewählten komplexen Einbettungen durchlaufen. Da F die ρ invariant läßt, die $\sigma, \bar{\sigma}$ aber vertauscht, so ist

$$K_{\mathbb{R}} = \{(z_\tau) \in \prod_\tau \mathbb{C} \mid z_\rho \in \mathbb{R},\ z_{\bar{\sigma}} = \bar{z}_\sigma\},$$

und es ergibt sich der

(5.1) Satz. *Wir erhalten einen Isomorphismus*

$$f : K_{\mathbb{R}} \to \prod_\tau \mathbb{R} = \mathbb{R}^{r+2s}$$

durch die Zuordnung $(z_\tau) \mapsto (x_\tau)$ *mit*

$$x_\rho = z_\rho\,, \quad x_\sigma = \mathrm{Re}(z_\sigma)\,, \quad x_{\bar{\sigma}} = \mathrm{Im}(z_\sigma)\,.$$

Dieser überführt die kanonische Metrik $\langle\ ,\ \rangle$ *in das Skalarprodukt*

$$(x, y) = \sum_\tau \alpha_\tau x_\tau y_\tau\,,$$

wobei $\alpha_\tau = 1$ *bzw.* $\alpha_\tau = 2$ *ist, je nachdem* τ *reell oder komplex ist.*

Beweis: Die Isomorphie ist klar. Sind $z = (z_\tau) = (x_\tau + iy_\tau)$, $z' = (z'_\tau) = (x'_\tau + iy'_\tau) \in K_{\mathbb{R}}$, so ist $z_\rho \bar{z}'_\rho = x_\rho x'_\rho$ und unter Beachtung von $y_\sigma = x_{\bar{\sigma}}$ und $y'_\sigma = x'_{\bar{\sigma}}$,

$$z_\sigma \bar{z}'_\sigma + z_{\bar{\sigma}} \bar{z}'_{\bar{\sigma}} = z_\sigma \bar{z}'_\sigma + \bar{z}_\sigma z'_\sigma = 2\ \mathrm{Re}(z_\sigma \bar{z}'_\sigma) = 2(x_\sigma x'_\sigma + x_{\bar{\sigma}} x'_{\bar{\sigma}})\,.$$

Hieraus folgt die Behauptung über die Skalarprodukte. □

Durch das Skalarprodukt $(x,y) = \sum_\tau \alpha_\tau x_\tau y_\tau$ wird das kanonische Maß von $K_{\mathbb{R}}$ auf $\mathbb{R}^{r+2s}$ übertragen. Es unterscheidet sich offenbar vom üblichen Lebesgue-Maß durch

$$\mathrm{vol}_{\text{kanonisch}}(X) = 2^s \,\mathrm{vol}_{\text{Lebesgue}}(f(X)).$$

Minkowski selbst hat mit dem Lebesgue-Maß auf $\mathbb{R}^{r+2s}$ gearbeitet, und so halten es auch die meisten Lehrbücher. Ihm entspricht auf $K_{\mathbb{R}}$ das Maß, das durch das Skalarprodukt

$$(x,y) = \sum_\tau \frac{1}{\alpha_\tau} x_\tau \bar{y}_\tau$$

festgelegt wird. Dieses Skalarprodukt möge daher die **Minkowski-Metrik** auf $K_{\mathbb{R}}$ genannt werden. Wir arbeiten jedoch immer mit der kanonischen Metrik und meinen mit vol das zugehörige kanonische Maß.

Durch die Abbildung $j : K \to K_{\mathbb{R}}$ entstehen die folgenden Gitter im Minkowski-Raum $K_{\mathbb{R}}$.

(5.2) Satz. *Ist $\mathfrak{a} \neq 0$ ein Ideal von $\mathcal{O}_K$, so ist $\Gamma = j\mathfrak{a}$ ein vollständiges Gitter in $K_{\mathbb{R}}$ mit dem Grundmaschenvolumen*

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}).$$

Beweis: Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$, so daß $\Gamma = \mathbb{Z}j\alpha_1 + \cdots + \mathbb{Z}j\alpha_n$. Wir numerieren die Einbettungen $\tau : K \to \mathbb{C}$, $\tau_1, \ldots, \tau_n$, und bilden die Matrix $A = (\tau_l \alpha_i)$. Dann ist einerseits nach (2.12)

$$d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n) = (\det A)^2 = (\mathcal{O}_K : \mathfrak{a})^2 d(\mathcal{O}_K) = (\mathcal{O}_K : \mathfrak{a})^2 d_K$$

und andererseits

$$(\langle j\alpha_i, j\alpha_k \rangle) = (\sum_{l=1}^{n} \tau_l \alpha_i \bar{\tau}_l \alpha_k) = A\bar{A}^t.$$

Es ergibt sich hieraus in der Tat

$$\mathrm{vol}(\Gamma) = |\det(\langle j\alpha_i, j\alpha_k \rangle)|^{1/2} = |\det A| = \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}). \qquad \square$$

Mit diesem Resultat liefert nun der Minkowskische Gitterpunktsatz das folgende Ergebnis, auf das es uns für die Anwendung auf die Zahlentheorie vornehmlich ankommen wird.

(5.3) Theorem. *Sei $\mathfrak{a} \neq 0$ ein ganzes Ideal von K, und seien $c_\tau > 0$ ($\tau \in \mathrm{Hom}(K, \mathbb{C})$) reelle Zahlen mit $c_\tau = c_{\bar\tau}$ und*

$$\prod_\tau c_\tau > A(\mathcal{O}_K : \mathfrak{a}),$$

wobei $A = (\frac{2}{\pi})^s \sqrt{|d_K|}$. Dann gibt es ein $a \in \mathfrak{a}$, $a \neq 0$, mit

$$|\tau a| < c_\tau \quad \text{für alle} \quad \tau \in \mathrm{Hom}(K, \mathbb{C}).$$

Beweis: Die Menge $X = \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau\}$ ist zentralsymmetrisch und konvex. Ihr Volumen $\mathrm{vol}(X)$ ergibt sich über die Abbildung (5.1)

$$f : K_{\mathbb{R}} \xrightarrow{\sim} \prod_\tau \mathbb{R}, \quad (z_\tau) \mapsto (x_\tau),$$

mit $x_\rho = z_\rho$, $x_\sigma = \mathrm{Re}(z_\sigma)$, $x_{\bar\sigma} = \mathrm{Im}(z_\sigma)$, als das 2^s-fache des Lebesgue-Inhalts des Bildes

$$f(X) = \{(x_\tau) \in \prod_\tau \mathbb{R} \mid |x_\rho| < c_\rho,\ x_\sigma^2 + x_{\bar\sigma}^2 < c_\sigma^2\}.$$

Es ist also

$$\mathrm{vol}(X) = 2^s \,\mathrm{vol}_{\mathrm{Lebesgue}}(f(X)) = 2^s \prod_\rho (2c_\rho) \prod_\sigma (\pi c_\sigma^2) = 2^{r+s}\pi^s \prod_\tau c_\tau.$$

Setzen wir (5.2) ein, so erhalten wir

$$\mathrm{vol}(X) > 2^{r+s}\pi^s \Big(\frac{2}{\pi}\Big)^s \sqrt{|d_K|}(\mathcal{O}_K : \mathfrak{a}) = 2^n \,\mathrm{vol}(\Gamma).$$

Hiermit ist die Voraussetzung für den Minkowskischen Gitterpunktsatz erfüllt. Es gibt daher in der Tat einen Gitterpunkt $ja \in X$, $a \neq 0$, $a \in \mathfrak{a}$, d.h. $|\tau a| < c_\tau$. □

Die Minkowski-Theorie besitzt auch eine **multiplikative Version**. Sie gründet sich auf den Homomorphismus

$$j : K^* \to K_{\mathbb{C}}^* = \prod_\tau \mathbb{C}^*.$$

Die multiplikative Gruppe $K_{\mathbb{C}}^*$ ist mit dem Homomorphismus

$$N : K_{\mathbb{C}}^* \to \mathbb{C}^*$$

versehen, der sich durch das Produkt der Koordinaten ergibt. Das Kompositum

$$K^* \xrightarrow{j} K_{\mathbb{C}}^* \xrightarrow{N} \mathbb{C}^*$$

ist die übliche Norm von $K|\mathbb{Q}$,

$$N_{K|\mathbb{Q}}(a) = N(ja)\,.$$

Um nun auch im multiplikativen Fall die Gitter ins Spiel zu bringen, gehen wir von den multiplikativen Gruppen zu additiven Gruppen über, indem wir den Logarithmus

$$l : \mathbb{C}^* \to \mathbb{R}\,, \quad z \mapsto \log|z|\,,$$

anwenden. Er induziert einen surjektiven Homomorphismus

$$l : K_{\mathbb{C}}^* \to \prod_\tau \mathbb{R}\,,$$

und wir erhalten das kommutative Diagramm

$$\begin{array}{ccccc} K^* & \xrightarrow{\jmath} & K_{\mathbb{C}}^* & \xrightarrow{l} & \prod_\tau \mathbb{R} \\ {\scriptstyle N_{K|\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{C}^* & \xrightarrow{l} & \mathbb{R}\,. \end{array}$$

Auf allen Gruppen dieses Diagramms operiert die Involution $F \in G(\mathbb{C}|\mathbb{R})$, auf K^* trivial, auf $K_{\mathbb{C}}^*$ wie zuvor und auf den Punkten $x = (x_\tau) \in \prod_\tau \mathbb{R}$ durch $(Fx)_\tau = x_{\bar\tau}$. Es gilt offenbar

$$F \circ j = j\,, \quad F \circ l = l \circ F\,, \quad N \circ F = F \circ N\,, \quad Tr \circ F = Tr\,,$$

d.h. die Homomorphismen des Diagramms sind $G(\mathbb{C}|\mathbb{R})$-Homomorphismen. Wir gehen jetzt überall wieder zu den Fixmoduln unter der $G(\mathbb{C}|\mathbb{R})$-Operation über und erhalten das Diagramm

$$\begin{array}{ccccc} K^* & \xrightarrow{\jmath} & K_{\mathbb{R}}^* & \xrightarrow{l} & [\prod_\tau \mathbb{R}]^+ \\ {\scriptstyle N_{K|\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{l} & \mathbb{R}\,. \end{array}$$

Der $\mathbb{R}$-Vektorraum $[\prod_\tau \mathbb{R}]^+$ ist explizit wie folgt gegeben. Wir teilen die Einbettungen $\tau : K \to \mathbb{C}$ wieder in die reellen $\rho_1, \ldots, \rho_r$ und die Paare $\sigma_1, \bar\sigma_1, \ldots, \sigma_s, \bar\sigma_s$ komplex konjugierter ein und erhalten wie zuvor bei $[\prod_\tau \mathbb{C}]^+$ eine Zerlegung

$$[\prod_\tau \mathbb{R}]^+ = \prod_\rho \mathbb{R} \times \prod_\sigma [\mathbb{R} \times \mathbb{R}]^+\,.$$

Der Faktor $[\mathbb{R} \times \mathbb{R}]^+$ besteht jetzt aus den Punkten (x, x), und wir identifizieren ihn mit $\mathbb{R}$ durch die Zuordnung $(x, x) \mapsto 2x$. Auf diese Weise erhalten wir einen Isomorphismus

$$[\prod_\tau \mathbb{R}]^+ \cong \mathbb{R}^{r+s}\,,$$

bei dem die Abbildung $Tr : [\prod_\tau \mathbb{R}]^+ \to \mathbb{R}$ wieder in die Abbildung

$$Tr : \mathbb{R}^{r+s} \to \mathbb{R}$$

übergeht, die durch die Summe der Koordinaten gegeben ist. Nach der Identifizierung $[\prod_\tau \mathbb{R}]^+ = \mathbb{R}^{r+s}$ wird der Homomorphismus

$$l : K_{\mathbb{R}}^* \to \mathbb{R}^{r+s}$$

durch

$$l(x) = (\log|x_{\rho_1}|, \ldots, \log|x_{\rho_r}|,\ \log|x_{\sigma_1}|^2, \ldots, \log|x_{\sigma_s}|^2)$$

gegeben, wenn $x \in K_{\mathbb{R}}^* \subseteq \prod_\tau \mathbb{C}^*$ in der Form $x = (x_\tau)$ geschrieben wird.

Aufgabe 1. Man gebe eine nur von K abhängige Konstante A an, so daß jedes ganze Ideal $\mathfrak{a} \neq 0$ von K ein Element $a \neq 0$ enthält mit

$$|\tau a| < A(\mathcal{O}_K : \mathfrak{a})^{1/n} \quad \text{für alle } \tau \in \mathrm{Hom}(K, \mathbb{C}),\ n = [K : \mathbb{Q}]\,.$$

Aufgabe 2. Zeige, daß die konvexe und zentralsymmetrische Menge

$$X = \{(z_\tau) \in K_{\mathbb{R}} \mid \sum_\tau |z_\tau| < t\}$$

das Volumen $\mathrm{vol}(X) = 2^r \pi^s \frac{t^n}{n!}$ hat (vgl. III, (2.14)).

Aufgabe 3. Zeige, daß es in jedem Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}_K$ ein $a \neq 0$ gibt mit

$$|N_{K|\mathbb{Q}}(a)| \leq M(\mathcal{O}_K : \mathfrak{a})\,,$$

wobei $M = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$ (die **Minkowski-Schranke**).

Hinweis: Man gehe mit Hilfe von Aufgabe 2 wie bei (5.3) vor und verwende die Ungleichung zwischen arithmetischem und geometrischem Mittel,

$$\frac{1}{n}\sum_\tau |z_\tau| \geq (\prod_\tau |z_\tau|)^{1/n}\,.$$

§ 6. Die Klassenzahl

Als erste Anwendung der Minkowski-Theorie wollen wir zeigen, daß die Idealklassengruppe $Cl_K = J_K/P_K$ eines algebraischen Zahlkörpers K endlich ist. Um die Ideale $\mathfrak{a} \neq 0$ des Ringes $\mathcal{O}_K$ zählen zu können, betrachten wir ihre **Absolutnorm**

$$\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})\,.$$

(Der Fall des Nullideals $\mathfrak{a} = 0$ ist in dem ganzen Buch häufig stillschweigend ausgeschlossen, wenn er augenfälligerweise keinen Sinn ergibt.) Der

Index ist nach (2.12) endlich, und der Name rechtfertigt sich durch den Sonderfall eines Hauptideals (α) von $\mathcal{O}_K$, für den die Gleichung

$$\mathfrak{N}((\alpha)) = |N_{K|\mathbb{Q}}(\alpha)|$$

gilt. In der Tat, ist $\omega_1, \ldots, \omega_n$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$, so ist $\alpha\omega_1, \ldots, \alpha\omega_n$ eine $\mathbb{Z}$-Basis von $(\alpha) = \alpha\mathcal{O}_K$, und wenn $A = (a_{ij})$ die Übergangsmatrix ist, $\alpha\omega_i = \sum a_{ij}\omega_j$, so ist, wie schon in § 2 bemerkt, einerseits $|\det(A)| = (\mathcal{O}_K : (\alpha))$ und andererseits $\det(A) = N_{K|\mathbb{Q}}(\alpha)$ nach Definition.

(6.1) Satz. *Ist* $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ *die Primzerlegung eines Ideals* $\mathfrak{a} \neq 0$, *so gilt*

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \ldots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}.$$

Beweis: Nach dem chinesischen Restsatz (3.6) ist

$$\mathcal{O}_K/\mathfrak{a} = \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{\nu_r},$$

so daß wir weiterhin $\mathfrak{a}$ als eine Primidealpotenz $\mathfrak{p}^\nu$ annehmen dürfen. In der Kette

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^\nu$$

ist $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ wegen der eindeutigen Primzerlegung, und jeder Quotient $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ ist ein $\mathcal{O}_K/\mathfrak{p}$-Vektorraum der Dimension 1. In der Tat, ist $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ und $\mathfrak{b} = (a) + \mathfrak{p}^{i+1}$, so ist $\mathfrak{p}^i \supseteq \mathfrak{b} \supsetneq \mathfrak{p}^{i+1}$ und folglich $\mathfrak{p}^i = \mathfrak{b}$, weil sonst $\mathfrak{b}' = \mathfrak{b}\mathfrak{p}^{-i}$ ein echter Teiler von $\mathfrak{p} = \mathfrak{p}^{i+1}\mathfrak{p}^{-i}$ wäre. Daher bildet $\bar{a} = a \bmod \mathfrak{p}^{i+1}$ eine Basis des $\mathcal{O}_K/\mathfrak{p}$-Vektorraums $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. Wir haben also $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}_K/\mathfrak{p}$ und somit

$$\mathfrak{N}(\mathfrak{p}^\nu) = (\mathcal{O}_K : \mathfrak{p}^\nu) = (\mathcal{O}_K : \mathfrak{p})(\mathfrak{p} : \mathfrak{p}^2) \ldots (\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu) = \mathfrak{N}(\mathfrak{p})^\nu. \qquad \square$$

Aus dem Satz folgt unmittelbar die Multiplikativität

$$\mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$$

der Absolutnorm. Sie setzt sich daher zu einem Homomorphismus

$$\mathfrak{N} : J_K \to \mathbb{R}_+^*$$

auf alle gebrochenen Ideale $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$, $\nu_\mathfrak{p} \in \mathbb{Z}$, fort. Das folgende, sich aus (5.3) ergebende Lemma ist für die Endlichkeit der Idealklassengruppe entscheidend.

(6.2) Lemma. *In jedem Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}_K$ gibt es ein $a \in \mathfrak{a}$, $a \neq 0$, mit*

$$|N_{K|\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) .$$

Beweis: Zu vorgegebenem $\varepsilon > 0$ wählen wir positive reelle Zahlen c_τ, $\tau \in \mathrm{Hom}(K, \mathbb{C})$, mit $c_\tau = c_{\bar{\tau}}$ und

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \varepsilon$$

und finden nach (5.3) ein Element $a \in \mathfrak{a}$, $a \neq 0$, mit $|\tau a| < c_\tau$, also

$$|N_{K|\mathbb{Q}}(a)| = \prod_\tau |\tau a| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \varepsilon .$$

Da dies für alle $\varepsilon > 0$ gilt und da $|N_{K|\mathbb{Q}}(a)|$ stets eine natürliche Zahl ist, so muß es auch ein $a \in \mathfrak{a}$, $a \neq 0$, geben mit

$$|N_{K|\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) . \qquad \square$$

(6.3) Theorem. *Die Idealklassengruppe $Cl_K = J_K/P_K$ ist endlich. Ihre Ordnung*

$$h_K = (J_K : P_K)$$

heißt die **Klassenzahl** *von K.*

Beweis: Ist $\mathfrak{p} \neq 0$ ein Primideal von $\mathcal{O}_K$ und $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, so ist $\mathcal{O}_K/\mathfrak{p}$ eine endliche Erweiterung von $\mathbb{Z}/p\mathbb{Z}$ von einem Grad $f \geq 1$, und es ist

$$\mathfrak{N}(\mathfrak{p}) = p^f .$$

Bei festem p gibt es nur endlich viele Primideale $\mathfrak{p}$ mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ wegen $\mathfrak{p}|(p)$. Daher gibt es nur endlich viele Primideale $\mathfrak{p}$ mit beschränkter Absolutnorm. Da jedes ganze Ideal eine Darstellung $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \ldots \mathfrak{p}_r^{\nu_r}$ mit $\nu_i > 0$ und

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \ldots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}$$

besitzt, gibt es überhaupt nur endlich viele Ideale $\mathfrak{a}$ von $\mathcal{O}_K$ mit beschränkter Absolutnorm $\mathfrak{N}(\mathfrak{a}) \leq M$.

Es genügt hiernach zu zeigen, daß jede Klasse $[\mathfrak{a}] \in Cl_K$ ein ganzes Ideal $\mathfrak{a}_1$ enthält mit

$$\mathfrak{N}(\mathfrak{a}_1) \leq M = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|} .$$

Wir wählen dazu einen beliebigen Repräsentanten $\mathfrak{a}$ der Klasse und ein $\gamma \in \mathcal{O}_K$, $\gamma \neq 0$, mit $\mathfrak{b} = \gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. Nach (6.2) gibt es dann ein $\alpha \in \mathfrak{b}$, $\alpha \neq 0$, mit

$$|N_{K|\mathbb{Q}}(\alpha)| \cdot \mathfrak{N}(\mathfrak{b})^{-1} = \mathfrak{N}((\alpha)\mathfrak{b}^{-1}) = \mathfrak{N}(\alpha\mathfrak{b}^{-1}) \leq M\,.$$

Das Ideal $\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}]$ hat demnach die gewünschte Eigenschaft. □

Der Satz von der Endlichkeit der Klassenzahl h_K bringt zum Ausdruck, daß uns der Übergang von den Zahlen zu den Idealen nicht ins Uferlose geführt hat. Der günstigste Fall liegt natürlich vor, wenn $h_K = 1$ ist. Dies ist gleichbedeutend damit, daß $\mathcal{O}_K$ ein Hauptidealring ist, d.h. daß der Satz von der eindeutigen Primzerlegung im klassischen Sinne gilt. In aller Regel ist jedoch $h_K > 1$. Es ist z.B. inzwischen bekannt, daß die imaginär-quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$, d quadratfrei und < 0, nur für die neun Werte

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

die Klassenzahl 1 haben. Die reell-quadratischen Zahlkörper neigen eher zur Klassenzahl 1. Im Bereich $2 \leq d < 100$ sind sie durch die Werte

$$\begin{aligned} d = {} & 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, \\ & 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, \\ & 83, 86, 89, 93, 94, 97 \end{aligned}$$

gegeben. Es wird vermutet, daß es unendlich viele reell-quadratische Zahlkörper mit der Klassenzahl 1 gibt, jedoch weiß man bis heute nicht einmal, ob es unendlich viele unter schlechthin allen Zahlkörpern gibt. Durch zahllose Untersuchungen ist immer wieder bestätigt worden, daß die Idealklassengruppen Cl_K nach Größe und Struktur ganz beliebig und ganz regellos ausfallen. Eine Ausnahme von dieser Regellosigkeit bildet eine Entdeckung von *Kenkichi Iwasawa*, wonach die Klassenzahl des Körpers der p^n-ten Einheitswurzeln hinsichtlich der p-Teilbarkeit bei laufendem n einem strengen Gesetz gehorcht (vgl. [136], Th. 13.13).

Im Falle des Körpers der p-ten Einheitswurzeln hat die Frage nach der Teilbarkeit seiner Klassenzahl durch p eine hervorragende Sonderrolle gespielt. Sie ist nämlich aufs engste mit der berühmten **Fermatschen Vermutung** verknüpft, nach der die Gleichung

$$x^p + y^p = z^p$$

für $p \geq 3$ in ganzen Zahlen $\neq 0$ unlösbar ist. Ähnlich wie die Quadratsummen $x^2 + y^2 = (x + iy)(x - iy)$ auf das Studium der Gaußschen

Zahlen geführt haben, so führt die Zerlegung von $x^p + y^p$ mit Hilfe einer p-ten Einheitswurzel $\zeta \neq 1$ auf ein Problem im Ring $\mathbb{Z}[\zeta]$ der ganzen Zahlen von $\mathbb{Q}(\zeta)$. Die Gleichung $y^p = z^p - x^p$ verwandelt sich dort in die Gleichheit

$$y \cdot y \cdot \ldots \cdot y = (z - x)(z - \zeta x) \cdot \ldots \cdot (z - \zeta^{p-1} x),$$

d.h. man erhält unter der Annahme der Lösbarkeit zwei multiplikative Zerlegungen ein und derselben Zahl in $\mathbb{Z}[\zeta]$. Man kann nun zeigen, daß dies der eindeutigen Primzerlegung widerspricht, vorausgesetzt, daß sie im Ring $\mathbb{Z}[\zeta]$ gilt. Unter der irrigen Annahme, daß dies im allgemeinen der Fall ist, daß also die Klassenzahl h_p des Körpers $\mathbb{Q}(\zeta)$ gleich 1 ist, hat man in der Tat geglaubt, die Fermatsche Vermutung auf diese Weise bewiesen zu haben. Nicht jedoch *Kummer*, wie lange Zeit behauptet wurde. Er bewies vielmehr, daß sich die oben angedeutete Schlußweise retten läßt, wenn man anstelle von $h_p = 1$ nur $p \nmid h_p$ voraussetzt. Die Primzahl p nannte er in diesem Fall **regulär**, sonst **irregulär**. Er zeigte sogar, daß p genau dann regulär ist, wenn die Zähler der **Bernoullischen Zahlen** $B_2, B_4, \ldots, B_{p-3}$ nicht durch p teilbar sind. Unter den ersten 25 Primzahlen < 100 sind nur drei irregulär, 37, 59, 67. Man weiß aber bis heute nicht, ob es unendlich viele reguläre Primzahlen gibt. Dagegen haben kürzlich die Mathematiker *L.M. Adleman*, *D.R. Heath-Brown* und *E. Fouvry* die Fermatsche Vermutung für unendlich viele p im „ersten Fall" bewiesen (vgl. [1]), d.h. unter der Voraussetzung $p \nmid xyz$. Aufgrund von Computerberechnungen kennt man ihre Gültigkeit für alle Primzahlen < 125000.

Für eine genauere Erörterung der angedeuteten Beziehung der Klassengruppen zur Fermatschen Vermutung verweisen wir auf [14].

Aufgabe 1. Wie viele ganze Ideale $\mathfrak{a}$ gibt es mit gegebener Norm $\mathfrak{N}(\mathfrak{a}) = n$?

Aufgabe 2. Zeige, daß die quadratischen Zahlkörper mit der Diskriminante $5, 8, 11, -3, -4, -7, -8, -11$ die Klassenzahl 1 haben.

Aufgabe 3. Zeige, daß es in jeder Idealklasse eines Zahlkörpers K vom Grade n ein ganzes Ideal $\mathfrak{a}$ gibt mit

$$\mathfrak{N}(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$

Hinweis: Unter Benutzung von Aufgabe 3, § 5, verfahre man wie im Beweis zu (6.3).

Aufgabe 4. Zeige, daß der Diskriminantenbetrag $|d_K| > 1$ ist für jeden algebraischen Zahlkörper $K \neq \mathbb{Q}$ (Minkowskischer Diskriminantensatz, vgl. Kap. III, (2.17)).

Aufgabe 5. Zeige, daß der Diskriminantenbetrag $|d_K|$ mit dem Körpergrad n gegen ∞ geht.

Aufgabe 6. Sei $\mathfrak{a}$ ein ganzes Ideal von K und $\mathfrak{a}^m = (a)$. Zeige, daß $\mathfrak{a}$ im Körper $L = K(\sqrt[m]{a})$ ein Hauptideal wird, d.h. $\mathfrak{a}\,\mathcal{O}_L = (\alpha)$.

Aufgabe 7. Zeige, daß es zu jedem Zahlkörper K eine endliche Erweiterung L gibt, in der jedes Ideal von K ein Hauptideal wird.

§ 7. Der Dirichletsche Einheitensatz

Nach der Idealklassengruppe Cl_K wenden wir uns nun der zweiten Hauptaufgabe zu, die uns der Ring $\mathcal{O}_K$ der ganzen Zahlen eines algebraischen Zahlkörpers K stellt, der Einheitengruppe $\mathcal{O}_K^*$. Sie enthält die endliche Gruppe $\mu(K)$ der in K gelegenen Einheitswurzeln, ist aber im allgemeinen nicht selbst endlich. Ihre Größe richtet sich vielmehr nach der Anzahl r der reellen Einbettungen $\rho : K \to \mathbb{R}$ und der Anzahl s der Paare $\sigma, \bar{\sigma} : K \to \mathbb{C}$ komplex konjugierter Einbettungen. Zu ihrer Beschreibung ziehen wir das in § 5 bereitgestellte Diagramm

$$\begin{array}{ccccc} K^* & \xrightarrow{\ j\ } & K_{\mathbb{R}}^* & \xrightarrow{\ l\ } & [\prod_\tau \mathbb{R}]^+ \\ {\scriptstyle N_{K|\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle Tr} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{\log|\ |} & \mathbb{R} \end{array}$$

heran. Im oberen Teil dieses Diagramms betrachten wir die Untergruppen

$$\begin{aligned} \mathcal{O}_K^* &= \{\varepsilon \in \mathcal{O}_K \mid N_{K|\mathbb{Q}}(\varepsilon) = \pm 1\}, && \text{die Einheitengruppe,} \\ S &= \{y \in K_{\mathbb{R}}^* \mid N(y) = \pm 1\}, && \text{die „Norm-Eins-Fläche“,} \\ H &= \{x \in [\prod_\tau \mathbb{R}]^+ \mid Tr(x) = 0\}, && \text{die „Spur-Null-Hyperebene“.} \end{aligned}$$

Wir erhalten die Homomorphismen

$$\mathcal{O}_K^* \xrightarrow{j} S \xrightarrow{l} H$$

und das Kompositum $\lambda := l \circ j : \mathcal{O}_K^* \to H$. Wir bezeichnen das Bild mit

$$\Gamma = \lambda(\mathcal{O}_K^*) \subseteq H$$

und erhalten den

(7.1) Satz. *Die Sequenz*

$$1 \to \mu(K) \to \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \to 0$$

ist exakt.

Beweis: Zu zeigen ist, daß $\mu(K)$ der Kern von λ ist. Ist nun $\zeta \in \mu(K)$ und $\tau : K \to \mathbb{C}$ eine Einbettung, so ist $\log|\tau\zeta| = \log 1 = 0$, also jedenfalls $\mu(K) \subseteq \mathrm{Ker}(\lambda)$. Sei umgekehrt $\varepsilon \in \mathcal{O}_K^*$ ein Element im Kern, $\lambda(\varepsilon) = l(j\varepsilon) = 0$. Dies bedeutet, daß $|\tau\varepsilon| = 1$ ist für jede Einbettung $\tau : K \to \mathbb{C}$, d.h. daß $j\varepsilon = (\tau\varepsilon)$ in einem beschränkten Bereich des $\mathbb{R}$-Vektorraums $K_{\mathbb{R}}$ liegt. Andererseits aber ist $j\varepsilon$ ein Punkt des Gitters $j\mathcal{O}_K$ von $K_{\mathbb{R}}$ (vgl. (5.2)). Daher kann der Kern von λ nur endlich viele Elemente enthalten, besteht also als endliche Untergruppe von K^* aus lauter Einheitswurzeln. □

Hiernach kommt alles auf die Bestimmung der Gruppe Γ an. Wir benötigen dazu das folgende

(7.2) Lemma. *Bis auf Assoziierte gibt es nur endlich viele Elemente $\alpha \in \mathcal{O}_K$ mit gegebener Norm $N_{K|\mathbb{Q}}(\alpha) = a$.*

Beweis: Sei $a \in \mathbb{Z}$, $a > 1$. In jeder der endlich vielen Nebenklassen von $\mathcal{O}_K/a\mathcal{O}_K$ gibt es bis auf Assoziierte höchstens ein Element α mit $|N(\alpha)| = |N_{K|\mathbb{Q}}(\alpha)| = a$. Ist nämlich $\beta = \alpha + a\gamma$, $\gamma \in \mathcal{O}_K$, ein zweites, so ist

$$\frac{\alpha}{\beta} = 1 \pm \frac{N(\beta)}{\beta}\gamma \in \mathcal{O}_K$$

wegen $N(\beta)/\beta \in \mathcal{O}_K$, und entsprechend $\dfrac{\beta}{\alpha} = 1 \pm \dfrac{N(\alpha)}{\alpha}\gamma \in \mathcal{O}_K$, d.h. β ist zu α assoziiert. Daher gibt es bis auf Assoziierte höchstens $(\mathcal{O}_K : a\mathcal{O}_K)$ Elemente mit der Norm $\pm a$. □

(7.3) Satz. *Die Gruppe Γ ist ein vollständiges Gitter im $(r+s-1)$-dimensionalen Vektorraum H, ist also isomorph zu $\mathbb{Z}^{r+s-1}$.*

Beweis: Wir zeigen zuerst, daß $\Gamma = \lambda(\mathcal{O}_K^*)$ ein Gitter in H, d.h. eine diskrete Untergruppe ist. Die Abbildung $\lambda : \mathcal{O}_K^* \to H$ entsteht durch Einschränkung der Abbildung

$$K^* \xrightarrow{j} \prod_\tau \mathbb{C}^* \xrightarrow{l} \prod_\tau \mathbb{R},$$

und es genügt zu zeigen, daß der beschränkte Bereich $\{(x_\tau) \in \prod_\tau \mathbb{R} \mid |x_\tau| \leq c\}$ für jedes $c > 0$ nur endlich viele Punkte von $\Gamma = l(j\mathcal{O}_K^*)$

enthält. Das Urbild dieses Bereiches unter l ist der beschränkte Bereich

$$\{(z_\tau) \in \prod_\tau \mathbb{C}^* \mid e^{-c} \leq |z_\tau| \leq e^c\}$$

wegen $l((z_\tau)) = (\log|z_\tau|)$. Dieser enthält aber nur endlich viele Elemente der Menge $j\mathcal{O}_K^*$, weil sie Teilmenge des Gitters $j\mathcal{O}_K$ in $[\prod_\tau \mathbb{C}]^+$ ist (vgl. (5.2)). Daher ist Γ ein Gitter.

Wir beweisen nun, daß Γ ein vollständiges Gitter in H ist. Hierin besteht die Hauptaussage des Satzes. Wir ziehen dazu das Kriterium (4.3) heran, wonach wir eine beschränkte Menge $M \subseteq H$ finden müssen, derart daß

$$H = \bigcup_{\gamma \in \Gamma} (M + \gamma).$$

Wir konstruieren die Menge, indem wir ihr Urbild unter dem surjektiven Homomorphismus

$$l : S \to H$$

angeben, genauer konstruieren wir eine beschränkte Menge T in der Norm-Eins-Fläche S, deren *multiplikative* Verschiebungen $Tj\varepsilon$, $\varepsilon \in \mathcal{O}_K^*$, ganz S überdecken:

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} Tj\varepsilon.$$

Für $x = (x_\tau) \in T$ sind dann die Beträge $|x_\tau|$ wegen $\prod_\tau |x_\tau| = 1$ sowohl nach oben als auch nach unten gegen Null beschränkt, so daß auch $M = l(T)$ beschränkt ist. Wir wählen reelle Zahlen $c_\tau > 0$, $\tau \in \mathrm{Hom}(K, \mathbb{C})$, mit $c_\tau = c_{\bar\tau}$ und

$$C = \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$$

und betrachten die Menge

$$X = \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau\}.$$

Für einen beliebigen Punkt $y = (y_\tau) \in S$ ist dann

$$Xy = \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c'_\tau\}$$

mit $c'_\tau = c_\tau |y_\tau|$, und es gilt $c'_\tau = c'_{\bar\tau}$ und $\prod_\tau c'_\tau = \prod_\tau c_\tau = C$ wegen $\prod_\tau |y_\tau| = |N(y)| = 1$. Nach (5.3) gibt es daher einen Punkt

$$ja = (\tau a) \in Xy, \quad a \in \mathcal{O}_K, \quad a \neq 0.$$

Wir können nun nach Lemma (7.2) ein System $\alpha_1, \ldots, \alpha_N \in \mathcal{O}_K$, $\alpha_i \neq 0$, fixieren mit der Eigenschaft, daß jedes $a \in \mathcal{O}_K$, $a \neq 0$, mit $|N_{K|\mathbb{Q}}(a)| \leq C$ zu einer dieser Zahlen assoziiert ist. Die Menge

$$T = S \cap \bigcup_{i=1}^{N} X(j\alpha_i)^{-1}$$

hat dann die gewünschte Eigenschaft: Da X beschränkt ist, ist auch $X(j\alpha_i)^{-1}$ und damit T beschränkt, und es gilt

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^*} Tj\varepsilon\,.$$

In der Tat, ist $y \in S$, so finden wir nach dem Obigen ein $a \in \mathcal{O}_K$, $a \neq 0$, mit $ja \in Xy^{-1}$, also $ja = xy^{-1}$, $x \in X$. Wegen

$$|N_{K|\mathbb{Q}}(a)| = |N(xy^{-1})| = |N(x)| < \prod_\tau c_\tau = C$$

ist a zu einem α_i assoziiert, $\alpha_i = \varepsilon a$, $\varepsilon \in \mathcal{O}_K^*$. Es folgt

$$y = xja^{-1} = xj(\alpha_i^{-1}\varepsilon)\,.$$

Wegen $y, j\varepsilon \in S$ ist $xj\alpha_i^{-1} \in S \cap Xj\alpha_i^{-1} \subseteq T$, also $y \in Tj\varepsilon$. □

Aus den Sätzen (7.1) und (7.3) ergibt sich unmittelbar der **Dirichletsche Einheitensatz** in seiner klassischen Form.

(7.4) Theorem. *Die Einheitengruppe $\mathcal{O}_K^*$ von $\mathcal{O}_K$ ist das direkte Produkt der endlichen zyklischen Gruppe $\mu(K)$ und einer freien abelschen Gruppe vom Rang $r + s - 1$.*

Mit anderen Worten: Es gibt Einheiten $\varepsilon_1, \ldots, \varepsilon_t$, $t = r + s - 1$, **Grundeinheiten** genannt, derart daß sich jede weitere Einheit ε eindeutig als ein Produkt

$$\varepsilon = \zeta \varepsilon_1^{\nu_1} \ldots \varepsilon_t^{\nu_t}$$

mit einer Einheitswurzel ζ und ganzen Zahlen ν_i ausdrücken läßt.

Beweis: In der exakten Sequenz

$$1 \to \mu(K) \to \mathcal{O}_K^* \xrightarrow{\lambda} \Gamma \to 0$$

ist Γ nach (7.3) eine freie abelsche Gruppe vom Rang $t = r + s - 1$. Ist $v_1, \ldots, v_t$ eine $\mathbb{Z}$-Basis von Γ, und sind $\varepsilon_1, \ldots, \varepsilon_t \in \mathcal{O}_K^*$ Urbilder der v_i und $A \subseteq \mathcal{O}_K^*$ die durch die ε_i erzeugte Untergruppe, so wird A durch λ isomorph auf Γ abgebildet, d.h. es ist $\mu(K) \cap A = \{1\}$ und also $\mathcal{O}_K^* = \mu(K) \times A$. □

Nach der Identifizierung $[\prod_\tau \mathbb{R}]^+ = \mathbb{R}^{r+s}$ (vgl. § 5, S. 35) wird H ein Unterraum des euklidischen Raumes $\mathbb{R}^{r+s}$ und ist somit selbst

ein euklidischer Raum. Wir können daher vom Grundmaschеninhalt $\mathrm{vol}(\lambda(\mathcal{O}_K^*))$ des Einheitengitters $\Gamma = \lambda(\mathcal{O}_K^*) \subseteq H$ sprechen und wollen diesen berechnen. Sei $\varepsilon_1, \ldots, \varepsilon_t$, $t = r+s-1$, ein System von Grundeinheiten und Φ die von den Vektoren $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t) \in H$ aufgespannte Grundmasche des Einheitengitters $\lambda(\mathcal{O}_K^*)$. Der Vektor

$$\lambda_0 = \frac{1}{\sqrt{r+s}}(1, \ldots, 1) \in \mathbb{R}^{r+s}$$

ist offensichtlich orthogonal zu H und hat die Länge 1. Daher ist der t-dimensionale Inhalt von Φ gleich dem $(t+1)$-dimensionalen Inhalt des von $\lambda_0, \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)$ aufgespannten Parallelepipeds in $\mathbb{R}^{t+1}$. Dieses aber hat den Inhalt

$$\pm \det \begin{pmatrix} \lambda_{01} & \lambda_1(\varepsilon_1) & \cdots & \lambda_1(\varepsilon_t) \\ \vdots & \vdots & & \vdots \\ \lambda_{0t+1} & \lambda_{t+1}(\varepsilon_1) & \cdots & \lambda_{t+1}(\varepsilon_t) \end{pmatrix}.$$

Addieren wir alle Zeilen zu einer festgewählten, etwa der i-ten, so stellen sich in dieser lauter Nullen ein bis auf die erste Komponente, welche gleich $r+s$ ist. Daher ergibt sich der

(7.5) Satz. *Der Grundmaschеninhalt des Einheitengitters $\lambda(\mathcal{O}_K^*)$ in H ist*

$$\mathrm{vol}(\lambda(\mathcal{O}_K^*)) = \sqrt{r+s}\, R,$$

wobei R der Determinantenbetrag eines beliebigen Minors vom Rang $t = r+s-1$ der Matrix

$$\begin{pmatrix} \lambda_1(\varepsilon_1) & \cdots & \lambda_1(\varepsilon_t) \\ \vdots & & \vdots \\ \lambda_{t+1}(\varepsilon_1) & \cdots & \lambda_{t+1}(\varepsilon_t) \end{pmatrix}$$

ist. Dieser Determinantenbetrag R heißt der **Regulator** *des Körpers K.*

Der Regulator wird erst später seine Wichtigkeit zeigen (vgl. Kap. VII, § 5).

Aufgabe 1. Sei $D > 1$ eine quadratfreie ganze Zahl und d die Diskriminante des reell-quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{D})$ (vgl. § 2, Aufgabe 4). Sei x_1, y_1 diejenige eindeutig bestimmte ganzrationale Lösung der Gleichung

$$x^2 - dy^2 = -4,$$

bzw. – falls diese Gleichung ganzrational unlösbar ist – der Gleichung

$$x^2 - dy^2 = 4,$$

für die $x_1, y_1 > 0$ möglichst klein sind. Dann ist

$$\varepsilon_1 = \frac{x_1 + y_1\sqrt{d}}{2}$$

eine Grundeinheit von K. (Die Doppelgleichung $x^2 - dy^2 = \pm 4$ wird die **Pellsche Gleichung** genannt.)

Aufgabe 2. Verifiziere die folgende Tabelle für die Grundeinheit ε_1 in $\mathbb{Q}(\sqrt{D})$:

D	2	3	5	6	7	10
ε_1	$1+\sqrt{2}$	$2+\sqrt{3}$	$(1+\sqrt{5})/2$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{10}$

Hinweis: Man prüfe der Reihe nach mit $y = 1, 2, 3, \ldots$, ob eine der beiden Zahlen $dy^2 \mp 4$ ein Quadrat x^2 ist. Nach dem Einheitensatz muß dies – mit dem Pluszeichen – sicher einmal auftreten. Man gebe aber für jedes einzelne y dem Minuszeichen den Vorrang. Der in dieser Rangordnung erste Fall mit $dy_1^2 \mp 4 = x_1^2$ liefert die Grundeinheit $\varepsilon_1 = (x_1 + y_1\sqrt{d})/2$.

Aufgabe 3. Die Schlacht von Hastings (14.10.1066).
Harolds Mannen standen nach alter Gewohnheit dichtgedrängt in 13 gleichgroßen Quadraten aufgestellt, und wehe dem Normannen, der es wagte, in eine solche Phalanx einbrechen zu wollen. ... Als aber Harold selbst auf dem Schlachtfeld erschien, formten die Sachsen ein einziges gewaltiges Quadrat mit ihrem König an der Spitze und stürmten mit den Schlachtrufen „Ut!", „Olicrosse!", „Godemite!" vorwärts. ... (vgl. *„Carmen de Hastingae Proelio"* von Guy, Bischof von Amiens).

Frage: Wie groß soll die Armee Harolds II. gewesen sein?

Mitgeteilt von *W.-D. Geyer*.

Aufgabe 4. Sei ζ eine primitive p-te Einheitswurzel, p eine ungerade Primzahl. Zeige, daß $\mathbb{Z}[\zeta]^* = (\zeta)\mathbb{Z}[\zeta + \zeta^{-1}]^*$.

Zeige, daß $\mathbb{Z}[\zeta]^* = \{\pm\zeta^k(1+\zeta)^n \mid 0 \le k < 5,\ n \in \mathbb{Z}\}$, wenn $p = 5$.

Aufgabe 5. Sei ζ eine primitive m-te Einheitswurzel, $m \ge 3$. Zeige, daß die Zahlen $\dfrac{1-\zeta^k}{1-\zeta}$ für $(k, m) = 1$ Einheiten im Ring der ganzen Zahlen des Körpers $\mathbb{Q}(\zeta)$ sind. Die durch sie erzeugte Untergruppe der Einheitengruppe heißt die Gruppe der **Kreiseinheiten**.

Aufgabe 6. Sei K ein total reeller Zahlkörper, d.h. $X = \mathrm{Hom}(K, \mathbb{C}) = \mathrm{Hom}(K, \mathbb{R})$, und T eine echte, nicht-leere Teilmenge von X. Dann gibt es eine Einheit ε mit $0 < \tau\varepsilon < 1$ für $\tau \in T$ und $\tau\varepsilon > 1$ für $\tau \notin T$.

Hinweis: Wende den Minkowskischen Gitterpunktsatz auf das Einheitengitter im Spur-Null-Raum an.

§ 8. Erweiterungen von Dedekindringen

Nach der Betrachtung der Klassengruppe und der Einheitengruppe des Ringes o_K der ganzen Zahlen eines Zahlkörpers K soll uns jetzt daran gelegen sein, einen ersten Überblick über die Menge der Primideale von o_K zu gewinnen. Sie werden häufig als die Primideale von K angesprochen, eine ungenaue, aber unmißverständliche Bezeichnungsweise.

Jedes Primideal $\mathfrak{p} \neq 0$ von o_K enthält eine Primzahl p (vgl. § 3, S. 18) und ist daher ein Teiler des Ideals po_K. Es stellt sich somit die Frage, auf welche Weise eine Primzahl p im Ring o_K in Primideale zerfällt. Wir behandeln dieses Problem allgemeiner, indem wir anstelle von $\mathbb{Z}$ einen beliebigen Dedekindring o zugrunde legen und anstelle von o_K den ganzen Abschluß $\mathcal{O}$ von o in einer endlichen Erweiterung seines Quotientenkörpers betrachten.

(8.1) Satz. *Sei o ein Dedekindring mit dem Quotientenkörper K, $L|K$ eine endliche Erweiterung von K und $\mathcal{O}$ der ganze Abschluß von o in L. Dann ist auch $\mathcal{O}$ ein Dedekindring.*

Beweis: Als ganzer Abschluß von o ist $\mathcal{O}$ ganzabgeschlossen. Die Maximalität der von Null verschiedenen Primideale $\mathfrak{P}$ von $\mathcal{O}$ beweist man ähnlich wie im Fall $o = \mathbb{Z}$ (vgl. (3.1)): $\mathfrak{p} = \mathfrak{P} \cap o$ ist ein von Null verschiedenes Primideal von o, so daß der Integritätsbereich $\mathcal{O}/\mathfrak{P}$ eine Erweiterung des Körpers $o/\mathfrak{p}$ ist und daher selbst ein Körper sein muß, weil er sonst ein von Null verschiedenes Primideal besäße, dessen Durchschnitt mit $o/\mathfrak{p}$ wiederum ein von Null verschiedenes Primideal von $o/\mathfrak{p}$ wäre. Bleibt zu zeigen, daß $\mathcal{O}$ noethersch ist. In dem uns hauptsächlich interessierenden Fall, daß $L|K$ separabel ist, ist der Beweis sehr leicht. Ist $\alpha_1, \ldots, \alpha_n$ eine in $\mathcal{O}$ gelegene Basis von $L|K$ mit der Diskriminante $d = d(\alpha_1, \ldots, \alpha_n)$, so ist $d \neq 0$ nach (2.8), und nach (2.9) liegt $\mathcal{O}$ in dem endlich erzeugten o-Modul $o\alpha_1/d + \cdots + o\alpha_n/d$. Jedes Ideal von $\mathcal{O}$ ist ebenfalls in diesem endlich erzeugten o-Modul enthalten und ist daher selbst ein endlich erzeugter o-Modul, also erst recht ein endlich erzeugter $\mathcal{O}$-Modul. Dies zeigt, daß $\mathcal{O}$ noethersch ist, wenn $L|K$ separabel ist. Es mag erlaubt sein, sich mit diesem Fall zunächst zufrieden zu geben und die Prüfung des allgemeinen Falles einem dafür günstigen Augenblick zu überlassen. Wir führen den Beweis in einem allgemeinen Rahmen in § 12 (vgl. (12.8)). □

Für ein Primideal $\mathfrak{p}$ von o gilt stets

$$\mathfrak{p}\mathcal{O} \neq \mathcal{O}.$$

In der Tat, sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ ($\mathfrak{p} \neq 0$), so daß $\pi o = \mathfrak{p}\mathfrak{a}$ mit $\mathfrak{p} \nmid \mathfrak{a}$, also $\mathfrak{p} + \mathfrak{a} = o$. Schreiben wir $1 = b + s$, $b \in \mathfrak{p}$, $s \in \mathfrak{a}$, so ist $s \notin \mathfrak{p}$ und $s\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = \pi o$. Wäre jetzt $\mathfrak{p}\mathcal{O} = \mathcal{O}$, so folgte $s\mathcal{O} = s\mathfrak{p}\mathcal{O} \subseteq \pi\mathcal{O}$, also $s = \pi x$ mit $x \in \mathcal{O} \cap K = o$, d.h. $s \in \mathfrak{p}$, Widerspruch!

Ein Primideal $\mathfrak{p} \neq 0$ des Ringes o zerfällt in $\mathcal{O}$ in eindeutiger Weise in ein Produkt von Primidealen,

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}.$$

Anstelle von $\mathfrak{p}\mathcal{O}$ setzt man häufig kurz $\mathfrak{p}$. Die auftretenden Primideale $\mathfrak{P}_i$ sind gerade diejenigen Primideale $\mathfrak{P}$ von $\mathcal{O}$, die über $\mathfrak{p}$ liegen, d.h. für die

$$\mathfrak{p} = \mathfrak{P} \cap o$$

gilt. Hierfür schreiben wir auch kurz $\mathfrak{P}|\mathfrak{p}$ und nennen $\mathfrak{P}$ einen Primteiler von $\mathfrak{p}$. Der Exponent e_i heißt der **Verzweigungsindex** und der Körpergrad

$$f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}]$$

der **Trägheitsgrad** von $\mathfrak{P}_i$ über $\mathfrak{p}$. Zwischen den Zahlen e_i, f_i und dem Körpergrad $n = [L : K]$ besteht bei einer separablen Erweiterung $L|K$ die folgende Gesetzmäßigkeit.

(8.2) Satz. *Ist $L|K$ separabel, so gilt die* **fundamentale Gleichung**

$$\sum_{i=1}^{r} e_i f_i = n.$$

Beweis: Der Beweis beruht auf dem chinesischen Restsatz

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}.$$

$\mathcal{O}/\mathfrak{p}\mathcal{O}$ und $\mathcal{O}/\mathfrak{P}_i^{e_i}$ sind Vektorräume über dem Körper $\kappa = o/\mathfrak{p}$, und es genügt zu zeigen, daß

$$\dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n \quad \text{und} \quad \dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = e_i f_i.$$

Zum Beweis der ersten Gleichung seien $\omega_1, \dots, \omega_m \in \mathcal{O}$ Repräsentanten einer Basis $\bar{\omega}_1, \dots, \bar{\omega}_m$ von $\mathcal{O}/\mathfrak{p}\mathcal{O}$ über κ (wir haben im Beweis zu (8.1) gesehen, daß $\mathcal{O}$ ein endlich erzeugter o-Modul ist, d.h. $\dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) < \infty$). Es genügt zu zeigen, daß $\omega_1, \dots, \omega_m$ eine Basis von

$L|K$ ist. Angenommen, die $\omega_1, \ldots, \omega_m$ sind linear abhängig über K und damit über o. Es gibt dann nicht sämtlich verschwindende Elemente $a_1, \ldots, a_m \in o$ mit

$$a_1\omega_1 + \cdots + a_m\omega_m = 0\,.$$

Wir betrachten das Ideal $\mathfrak{a} = (a_1, \ldots, a_m)$ von o und können ein $a \in \mathfrak{a}^{-1}$ wählen mit $a \notin \mathfrak{a}^{-1}\mathfrak{p}$, also $a\mathfrak{a} \not\subseteq \mathfrak{p}$. Dann liegen die Elemente $aa_1, \ldots, aa_m$ in o , aber nicht alle in $\mathfrak{p}$. In der Kongruenz

$$aa_1\omega_1 + \cdots + aa_m\omega_m \equiv 0 \bmod \mathfrak{p}$$

erhalten wir somit eine lineare Abhängigkeit der $\bar{\omega}_1, \ldots, \bar{\omega}_m$ über κ, Widerspruch. Die $\omega_1, \ldots, \omega_m$ sind also linear unabhängig über K.

Zum Beweis, daß die ω_i eine Basis von $L|K$ bilden, betrachten wir die o-Moduln $M = o\omega_1 + \cdots + o\omega_m$ und $N = \mathcal{O}/M$. Wegen $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$ gilt $\mathfrak{p}N = N$. Da $L|K$ separabel ist, so ist $\mathcal{O}$ und damit auch N ein endlich erzeugter o-Modul (vgl. S. 47). Ist $\alpha_1, \ldots, \alpha_s$ ein Erzeugendensystem von N, so gilt

$$\alpha_i = \sum_j a_{ij}\alpha_j \quad \text{mit } a_{ij} \in \mathfrak{p}\,.$$

Sei A die Matrix $(a_{ij}) - I$, I die s-reihige Einheitsmatrix, und B die zu A **adjungierte** Matrix, die aus den $(s-1)$-reihigen Unterdeterminanten von A gebildet wird. Dann ist $A(\alpha_1, \ldots, \alpha_s)^t = 0$ und $BA = dI$, $d = \det(A)$, (vgl. (2.3)), also

$$0 = BA(\alpha_1, \ldots, \alpha_s)^t = (d\alpha_1, \ldots, d\alpha_s)^t\,,$$

und somit $dN = 0$, d.h. $d\mathcal{O} \subseteq M = o\omega_1 + \cdots + o\omega_m$. Es ist $d \neq 0$, denn wenn wir die Determinante $d = \det((a_{ij}) - I)$ entwickeln, so erhalten wir $d \equiv (-1)^s \bmod \mathfrak{p}$ wegen $a_{ij} \in \mathfrak{p}$. Es ergibt sich somit $L = dL = K\omega_1 + \cdots + K\omega_m$. In der Tat ist also $\omega_1, \ldots, \omega_m$ eine Basis von $L|K$.

Zum Beweis der zweiten Gleichung betrachten wir die absteigende Kette

$$\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \cdots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq (0)$$

von κ-Vektorräumen. Die Quotienten $\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}$ dieser Kette sind isomorph zu $\mathcal{O}/\mathfrak{P}_i$, denn wenn $\alpha \in \mathfrak{P}_i^{\nu} \setminus \mathfrak{P}_i^{\nu+1}$ ist, hat der Homomorphismus

$$\mathcal{O} \to \mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}, \quad a \mapsto a\alpha,$$

den Kern $\mathfrak{P}_i$ und ist surjektiv, weil $\mathfrak{P}_i^{\nu}$ der ggT von $\mathfrak{P}_i^{\nu+1}$ und $(\alpha) = \alpha\mathcal{O}$ ist, so daß $\mathfrak{P}_i^{\nu} = \alpha\mathcal{O} + \mathfrak{P}_i^{\nu+1}$. Wegen $f_i = [\mathcal{O}/\mathfrak{P}_i : \kappa]$ erhalten wir $\dim_\kappa(\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}) = f_i$ und damit

$$\dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = \sum_{\nu=0}^{e_i-1} \dim_\kappa(\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}) = e_i f_i\,. \qquad \square$$

Sei jetzt die separable Erweiterung $L|K$ durch ein ganzes, primitives Element $\theta \in \mathcal{O}$ mit dem Minimalpolynom

$$p(X) \in o[X]$$

gegeben, $L = K(\theta)$. Wir erhalten dann über die Art der Zerlegung von $\mathfrak{p}$ in $\mathcal{O}$ ein Resultat, das zwar nicht vollständig ist, aber dennoch typisch und durch seine Einfachheit schlagend. Die Unvollständigkeit besteht darin, daß man endlich viele Primideale ausschließen muß und nur diejenigen betrachten kann, die zum **Führer** des Ringes $o[\theta]$ teilerfremd sind. Unter diesem Führer versteht man das größte in $o[\theta]$ gelegene Ideal $\mathfrak{F}$ von $\mathcal{O}$, d.h.

$$\mathfrak{F} = \{\alpha \in \mathcal{O} \mid \alpha\mathcal{O} \subseteq o[\theta]\}.$$

Da $\mathcal{O}$ ein endlich erzeugter o-Modul ist (vgl. Beweis zu (8.1)), ist $\mathfrak{F} \neq 0$.

(8.3) Satz. *Sei $\mathfrak{p}$ ein zum Führer $\mathfrak{F}$ von $o[\theta]$ teilerfremdes Primideal von o, und sei*

$$\bar{p}(X) = \bar{p}_1(X)^{e_1} \dots \bar{p}_r(X)^{e_r}$$

die Zerlegung des Polynoms $\bar{p}(X) = p(X) \bmod \mathfrak{p}$ in irreduzible Faktoren $\bar{p}_i(X) = p_i(X) \bmod \mathfrak{p}$ über dem Restklassenkörper $o/\mathfrak{p}$, $p_i(X) \in o[X]$ normiert. Dann sind

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}, \quad i = 1, \dots, r,$$

die verschiedenen über $\mathfrak{p}$ liegenden Primideale von $\mathcal{O}$. Der Trägheitsgrad f_i von $\mathfrak{P}_i$ ist der Grad von $\bar{p}_i(X)$, und es gilt

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}.$$

Beweis: Setzen wir $\mathcal{O}' = o[\theta]$ und $\bar{o} = o/\mathfrak{p}$, so erhalten wir kanonische Isomorphismen

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \bar{o}[X]/(\bar{p}(X)).$$

Der erste Isomorphismus beruht auf der Teilerfremdheit $\mathfrak{p}\mathcal{O} + \mathfrak{F} = \mathcal{O}$. Wegen $\mathfrak{F} \subseteq \mathcal{O}'$ folgt $\mathcal{O} = \mathfrak{p}\mathcal{O} + \mathcal{O}'$, d.h. der Homomorphismus $\mathcal{O}' \to \mathcal{O}/\mathfrak{p}\mathcal{O}$ ist surjektiv. Er hat den Kern $\mathfrak{p}\mathcal{O} \cap \mathcal{O}'$, und dieser ist gleich $\mathfrak{p}\mathcal{O}'$, denn wegen $(\mathfrak{p}, \mathfrak{F} \cap o) = 1$ ist $\mathfrak{p}\mathcal{O} \cap \mathcal{O}' = (\mathfrak{p} + \mathfrak{F})(\mathfrak{p}\mathcal{O} \cap \mathcal{O}') \subseteq \mathfrak{p}\mathcal{O}'$.

Der zweite Isomorphismus ergibt sich durch den surjektiven Homomorphismus

$$o[X] \to \bar{o}[X]/(\bar{p}(X)).$$

Der Kern ist das durch $\mathfrak{p}$ und $p(X)$ erzeugte Ideal, und wegen $\mathcal{O}' = o[\theta] = o[X]/(p(X))$ wird $\mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \bar{o}[X]/(\bar{p}(X))$.

Wegen $\bar{p}(X) = \prod_{i=1}^{r} \bar{p}_i(X)^{e_i}$ liefert schließlich der chinesische Restsatz den Isomorphismus

$$\bar{o}[X]/(\bar{p}(X)) \cong \bigoplus_{i=1}^{r} \bar{o}[X]/(\bar{p}_i(X))^{e_i}.$$

Dies zeigt, daß die Primideale des Ringes $R = \bar{o}[X]/(\bar{p}(X))$ die durch $\bar{p}_i(X) \bmod \bar{p}(X)$ erzeugten Hauptideale $(\bar{p}_i)$ sind, $i = 1, \ldots, r$, daß der Grad $[R/(\bar{p}_i) : \bar{o}]$ gleich dem Grad des Polynoms $\bar{p}_i(X)$ ist, und daß

$$(0) = (\bar{p}) = \bigcap_{i=1}^{r} (\bar{p}_i)^{e_i}.$$

Wegen der Isomorphie $\bar{o}[X]/(\bar{p}[X]) \cong \mathcal{O}/\mathfrak{p}\mathcal{O}$, $f(X) \mapsto f(\theta)$, haben wir im Ring $\overline{\mathcal{O}} = \mathcal{O}/\mathfrak{p}\mathcal{O}$ die gleichen Verhältnisse: Die Primideale $\overline{\mathfrak{P}}_i$ von $\overline{\mathcal{O}}$ entsprechen den Primidealen $(\bar{p}_i)$ und sind die durch $p_i(\theta) \bmod \mathfrak{p}\mathcal{O}$ erzeugten Hauptideale, der Grad $[\overline{\mathcal{O}}/\overline{\mathfrak{P}}_i : \bar{o}]$ ist der Grad des Polynoms $\bar{p}_i(X)$, und es ist $(0) = \bigcap_{i=1}^{r} \overline{\mathfrak{P}}_i^{e_i}$. Sei nun $\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}$ das Urbild von $\overline{\mathfrak{P}}_i$ unter dem kanonischen Homomorphismus

$$\mathcal{O} \to \mathcal{O}/\mathfrak{p}\mathcal{O}.$$

Dann durchläuft $\mathfrak{P}_i$, $i = 1, \ldots, r$, die über $\mathfrak{p}$ gelegenen Primideale von $\mathcal{O}$, es ist $f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}]$ der Grad des Polynoms $\bar{p}_i(X)$, es ist $\mathfrak{P}_i^{e_i}$ das Urbild von $\overline{\mathfrak{P}}_i^{e_i}$ (wegen $e_i = \#\{\overline{\mathfrak{P}}^{\nu} | \nu \in \mathbb{N}\}$) und $\mathfrak{p}\mathcal{O} \supseteq \bigcap_{i=1}^{r} \mathfrak{P}_i^{e_i}$, also $\mathfrak{p}\mathcal{O} \mid \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ und damit $\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ wegen $\sum e_i f_i = n$. □

Das Primideal $\mathfrak{p}$ heißt **voll zerlegt** (oder **total zerlegt**) in L, wenn in der Zerlegung

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$$

$r = n = [L : K]$ ist, also $e_i = f_i = 1$ für alle $i = 1, \ldots, r$. $\mathfrak{p}$ heißt **unzerlegt**, wenn $r = 1$ ist, wenn es also nur ein einziges Primideal von L über $\mathfrak{p}$ gibt. Durch die fundamentale Gleichung

$$\sum_{i=1}^{r} e_i f_i = n$$

klärt sich die Namensgebung für die Trägheitsgrade auf: Je kleiner die Trägheitsgrade sind, desto fleißiger zerfällt $\mathfrak{p}$ in verschiedene Primideale.

Das Primideal $\mathfrak{P}_i$ in der Zerlegung $\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ heißt **unverzweigt** über o (oder über K), wenn $e_i = 1$ und die Restkörpererweiterung $\mathcal{O}/\mathfrak{P}_i | o/\mathfrak{p}$ separabel ist. Sonst heißt es **verzweigt**, und man sagt, es sei **rein verzweigt**, wenn überdies $f_i = 1$ ist. Das Primideal $\mathfrak{p}$ heißt

unverzweigt, wenn alle $\mathfrak{P}_i$ unverzweigt sind, sonst verzweigt. Die Erweiterung $L|K$ selbst heißt unverzweigt, wenn alle Primideale $\mathfrak{p}$ von K in L unverzweigt sind.

Der Fall, daß ein Primideal $\mathfrak{p}$ von K in L verzweigt ist, ist eine Ausnahmeerscheinung. Es gilt der

(8.4) Satz. *Ist $L|K$ separabel, so gibt es nur endlich viele in L verzweigte Primideale von K.*

Beweis: Sei $\theta \in \mathcal{O}$ ein primitives Element für L, d.h. $L = K(\theta)$, und $p(X) \in o[X]$ sein Minimalpolynom. Sei

$$d = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \in o$$

die Diskriminante von $p(X)$ (vgl. § 2, S. 11). Dann ist jedes zu d und zum Führer $\mathfrak{F}$ von $o[\theta]$ teilerfremde Primideal $\mathfrak{p}$ von K unverzweigt. In der Tat, wegen (8.3) sind die Verzweigungsindizes $e_i = 1$, wenn sie 1 sind in der Zerlegung von $\bar{p}(X) = p(X) \bmod \mathfrak{p}$ in $o/\mathfrak{p}$, also sicher dann, wenn $\bar{p}(X)$ keine mehrfachen Nullstellen hat. Dies aber ist hier der Fall, weil die Diskriminante $\bar{d} = d \bmod \mathfrak{p}$ von $\bar{p}(X)$ von Null verschieden ist. Die Restkörpererweiterungen $\mathcal{O}/\mathfrak{P}_i | o/\mathfrak{p}$ werden durch $\bar{\theta} = \theta \bmod \mathfrak{P}_i$ erzeugt, sind also separabel. Daher ist $\mathfrak{p}$ unverzweigt. □

Die genaue Beschreibung der verzweigten Primideale wird durch die **Diskriminante** von $\mathcal{O}|o$ gegeben. Diese ist das Ideal $\mathfrak{d}$ von o, das durch die Diskriminanten $d(\omega_1, \ldots, \omega_n)$ aller in $\mathcal{O}$ gelegenen Basen $\omega_1, \ldots, \omega_n$ von $L|K$ erzeugt wird. Wir werden in Kapitel III, § 2 zeigen, daß die Primteiler von $\mathfrak{d}$ genau die in L verzweigten Primideale sind.

Beispiel: Das Zerlegungsgesetz der Primzahlen p im **quadratischen Zahlkörper** $\mathbb{Q}(\sqrt{a})$ steht in engstem Zusammenhang mit dem berühmten **Gaußschen Reziprozitätsgesetz**. Letzteres betrifft die Frage nach der ganzzahligen Lösbarkeit der diophantischen Gleichung

$$x^2 + by = a\,, \quad (a, b \in \mathbb{Z})\,,$$

der einfachsten unter den nicht-trivialen. Die Behandlung dieser Gleichung läßt sich unmittelbar auf den Fall zurückführen, wo b eine ungerade Primzahl p ist und $(a, p) = 1$ (Aufgabe 6). Dies wollen wir im folgenden annehmen. Es handelt sich dann um die Frage, ob a **quadratischer Rest** $\bmod p$ ist, d.h. ob die Kongruenz

$$x^2 \equiv a \bmod p$$

lösbar ist oder nicht, mit anderen Worten, ob für das Element $\bar{a} = a \bmod p \in \mathbb{F}_p^*$ die Gleichung $\bar{x}^2 = \bar{a}$ im Körper $\mathbb{F}_p$ lösbar ist oder nicht. Man führt hierzu das **Legendresymbol** $\left(\frac{a}{p}\right)$ ein, das für jede zu p teilerfremde rationale Zahl a durch $\left(\frac{a}{p}\right) = 1$ oder -1 definiert ist, je nachdem $x^2 \equiv a \bmod p$ lösbar oder unlösbar ist. Dieses Symbol ist multiplikativ,

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

was darauf beruht, daß die Gruppe $\mathbb{F}_p^*$ zyklisch von der Ordnung $p-1$ ist und die Gruppe $\mathbb{F}_p^{*2}$ der Quadrate somit den Index 2 besitzt, d.h. $\mathbb{F}_p^*/\mathbb{F}_p^{*2} \cong \mathbb{Z}/2\mathbb{Z}$. Wegen $\left(\frac{a}{p}\right) = 1 \iff \bar{a} \in \mathbb{F}_p^{*2}$ ergibt sich auch

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Mit der Primzerlegung steht das Symbol $\left(\frac{a}{p}\right)$ bei quadratfreiem a in der folgenden Beziehung. $\left(\frac{a}{p}\right) = 1$ bedeutet

$$x^2 - a \equiv (x-\alpha)(x+\alpha) \bmod p$$

mit $\alpha \in \mathbb{Z}$. Der Führer von $\mathbb{Z}[\sqrt{a}]$ im Ring der ganzen Zahlen von $\mathbb{Q}(\sqrt{a})$ ist ein Teiler von 2 (vgl. § 2, Aufgabe 4). Wir können daher den Satz (8.3) anwenden und erhalten den

(8.5) Satz. *Für quadratfreies a und $(p, 2a) = 1$ gilt*

$$\left(\frac{a}{p}\right) = 1 \iff p \text{ ist voll zerlegt in } \mathbb{Q}(\sqrt{a}).$$

Für das Legendresymbol hat man nun die folgende merkwürdige Gesetzmäßigkeit, die wie keine andere die Entwicklung der algebraischen Zahlentheorie geprägt hat.

(8.6) Theorem (Gaußsches Reziprozitätsgesetz). *Für zwei verschiedene ungerade Primzahlen l und p gilt*

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

und man hat die beiden „Ergänzungssätze“

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

Beweis: Aus $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$ folgt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ wegen $p \neq 2$.

Zur Bestimmung von $\left(\frac{2}{p}\right)$ rechnen wir im Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen. Dort gilt wegen $(1+i)^2 = 2i$

$$(1+i)^p = (1+i)((1+i)^2)^{\frac{p-1}{2}} = (1+i)i^{\frac{p-1}{2}}2^{\frac{p-1}{2}},$$

und wegen $(1+i)^p \equiv 1 + i^p \bmod p$ und $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \bmod p$ folgt

$$\left(\frac{2}{p}\right)(1+i)i^{\frac{p-1}{2}} \equiv 1 + i(-1)^{\frac{p-1}{2}} \bmod p.$$

Durch eine leichte Rechnung erhält man hieraus

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p-1}{4}} \bmod p \quad \text{bzw.} \quad \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p+1}{4}} \bmod p,$$

je nachdem $\frac{p-1}{2}$ gerade oder ungerade ist. Weil $\frac{p^2-1}{8} = \frac{p-1}{4}\frac{p+1}{2} = \frac{p+1}{4}\frac{p-1}{2}$, folgt $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Zum Beweis der ersten Formel rechnen wir im Ring $\mathbb{Z}[\zeta]$, wobei ζ eine primitive l-te Einheitswurzel ist. Wir betrachten die **Gaußsche Summe**

$$\tau = \sum_{a \in (\mathbb{Z}/l)^*} \left(\frac{a}{l}\right)\zeta^a$$

und zeigen, daß

$$\tau^2 = \left(\frac{-1}{l}\right)l.$$

Dazu lassen wir a und b die Gruppe $(\mathbb{Z}/l\,\mathbb{Z})^*$ durchlaufen, setzen $c = ab^{-1}$ und erhalten unter Beachtung von $\left(\frac{b}{l}\right) = \left(\frac{b^{-1}}{l}\right)$

$$\left(\frac{-1}{l}\right)\tau^2 = \sum_{a,b}\left(\frac{-ab}{l}\right)\zeta^{a+b} = \sum_{a,b}\left(\frac{ab^{-1}}{l}\right)\zeta^{a-b} = \sum_{b,c}\left(\frac{c}{l}\right)\zeta^{bc-b}$$

$$= \sum_{c \neq 1}\left(\frac{c}{l}\right)\sum_b \zeta^{b(c-1)} + \sum_b\left(\frac{1}{l}\right).$$

Nun ist $\sum_c \left(\frac{c}{l}\right) = 0$, was man durch Multiplikation der Summe mit einem Symbol $\left(\frac{x}{l}\right) = -1$ sieht, und wenn wir $\xi = \zeta^{c-1}$ setzen, so wird $\sum_b \zeta^{b(c-1)} = \xi + \xi^2 + \cdots + \xi^{l-1} = -1$, also in der Tat

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

Hieraus und aus $\left(\frac{l}{p}\right) \equiv l^{\frac{p-1}{2}} \bmod p$ und $\left(\frac{-1}{l}\right) = (-1)^{\frac{l-1}{2}}$ schließen wir weiter

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

Andererseits ist

$$\tau^p \equiv \sum_a \left(\frac{a}{l}\right)\zeta^{ap} \equiv \left(\frac{p}{l}\right)\sum_a \left(\frac{ap}{l}\right)\zeta^{ap} \equiv \left(\frac{p}{l}\right)\tau \bmod p\,,$$

so daß

$$\tau\left(\frac{p}{l}\right) \equiv \tau(-1)^{\frac{l-1}{2}\frac{p-1}{2}}\left(\frac{l}{p}\right) \bmod p\,.$$

Multiplikation mit τ und Kürzung durch $\pm l$ ergibt das gewünschte Resultat. □

Wir haben das Gaußsche Reziprozitätsgesetz durch eine kunstreiche Rechnung bewiesen. Wir werden aber in § 10 sehen, daß sich der wahre Grund für seine Gültigkeit im Zerlegungsgesetz der Primzahlen im Körper $\mathbb{Q}(\zeta)$ der l-ten Einheitswurzeln zeigt. Die benutzten Gaußschen Summen haben jedoch eine übergeordnete theoretische Bedeutung, wie sich noch zeigen wird (vgl. VII, § 2 und § 6).

Aufgabe 1. Sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale von $\mathfrak{o}$, so gilt $\mathfrak{a} = \mathfrak{a}\mathcal{O}\cap\mathfrak{o}$ und $\mathfrak{a}|\mathfrak{b} \iff \mathfrak{a}\mathcal{O}|\mathfrak{b}\mathcal{O}$.

Aufgabe 2. Zu jedem ganzen Ideal $\mathfrak{A}$ von $\mathcal{O}$ gibt es ein $\theta \in \mathcal{O}$ mit zu $\mathfrak{A}$ teilerfremdem Führer $\mathfrak{F} = \{\alpha \in \mathcal{O} \mid \alpha\mathcal{O} \subseteq \mathfrak{o}[\theta]\}$, so daß $L = K(\theta)$.

Aufgabe 3. Ist ein Primideal $\mathfrak{p}$ von K voll zerlegt in den beiden separablen Erweiterungen $L|K$ und $L'|K$, so auch im Kompositum.

Aufgabe 4. Ein Primideal $\mathfrak{p}$ von K ist genau dann in der separablen Erweiterung $L|K$ voll zerlegt, wenn es voll zerlegt ist in der normalen Hülle $N|K$ von $L|K$.

Aufgabe 5. Für einen Zahlkörper K gilt die Aussage des Satzes (8.3) über die Primzerlegung in der Erweiterung $K(\theta)$ für alle Primideale $\mathfrak{p} \nmid (\mathcal{O} : \mathfrak{o}[\theta])$.

Aufgabe 6. Für eine natürliche Zahl $b > 1$ ist eine ganze, zu b teilerfremde Zahl a quadratischer Rest $\bmod b$ genau dann, wenn sie quadratischer Rest modulo jedem Primteiler p von b ist und wenn $a \equiv 1 \bmod 4$, falls $4|m$, $8\nmid m$, bzw. $a \equiv 1 \bmod 8$, falls $8|m$.

Aufgabe 7. Sei $(a,p) = 1$ und $a\nu \equiv r_\nu \bmod p$, $\nu = 1,\dots,p-1$, $0 < r_\nu < p$. Dann durchläuft r_ν eine Permutation π der Zahlen $1,\dots,p-1$. Zeige: $\operatorname{sgn}\pi = (\frac{a}{p})$.

Aufgabe 8. Sei $a_n = \frac{\varepsilon^n - \varepsilon'^n}{\sqrt{5}}$, wobei $\varepsilon = \frac{1+\sqrt{5}}{2}$, $\varepsilon' = \frac{1-\sqrt{5}}{2}$ (a_n ist die n-te Fibonacci-Zahl). Ist p eine Primzahl $\neq 2, 5$, so gilt

$$a_p \equiv \left(\frac{p}{5}\right) \bmod p\,.$$

Aufgabe 9. Untersuche das Legendresymbol $(\frac{3}{p})$ als Funktion von $p > 3$. Zeige, daß die Eigenschaft von 3, quadratischer Rest oder Nichtrest $\bmod p$ zu sein, nur von der Restklasse $p \bmod 12$ abhängt.

Aufgabe 10. Zeige, daß die Anzahl der Lösungen von $x^2 \equiv a \bmod p$ gleich $1 + (\frac{a}{p})$ ist.

Aufgabe 11. Zeige, daß die Anzahl der Lösungen der Kongruenz $ax^2 + bx + c \equiv 0 \bmod p$ mit $(a,p) = 1$ gleich $1 + (\frac{b^2-4ac}{p})$ ist.

§ 9. Hilbertsche Verzweigungstheorie

Eine besonders interessante und wichtige Wendung nimmt die Frage nach der Primzerlegung in einer endlichen Erweiterung $L|K$, wenn wir annehmen, daß $L|K$ galoissch ist, und die Primideale der Aktion der Galoisgruppe

$$G = G(L|K)$$

aussetzen. Es entsteht dann die von *David Hilbert* (1862–1943) in die Zahlentheorie eingeführte „Verzweigungstheorie". Mit a ist offenbar auch σa für jedes $\sigma \in G$ im Ring $\mathcal{O}$ der ganzen Elemente von L gelegen, d.h. G operiert auf $\mathcal{O}$. Ist nun $\mathfrak{P}$ ein Primideal von $\mathcal{O}$ über $\mathfrak{p}$, so ist auch $\sigma\mathfrak{P}$ für jedes $\sigma \in G$ ein Primideal über $\mathfrak{p}$, denn es ist

$$\sigma\mathfrak{P} \cap \mathcal{O} = \sigma(\mathfrak{P} \cap \mathcal{O}) = \sigma\mathfrak{p} = \mathfrak{p}\,.$$

Die $\sigma\mathfrak{P}$, $\sigma \in G$, heißen die zu $\mathfrak{P}$ **konjugierten** Primideale.

(9.1) Satz. *Die Galoisgruppe G operiert transitiv auf der Menge der über $\mathfrak{p}$ gelegenen Primideale $\mathfrak{P}$ von $\mathcal{O}$, d.h. diese Primideale sind sämtlich zueinander konjugiert.*

Beweis: Seien $\mathfrak{P}$ und $\mathfrak{P}'$ zwei Primideale über $\mathfrak{p}$. Angenommen $\mathfrak{P}' \neq \sigma\mathfrak{P}$ für alle $\sigma \in G$. Nach dem chinesischen Restsatz gibt es dann ein $x \in \mathcal{O}$ mit

$$x \equiv 0 \bmod \mathfrak{P}' \quad \text{und} \quad x \equiv 1 \bmod \sigma\mathfrak{P} \quad \text{für alle} \quad \sigma \in G.$$

Dann liegt die Norm $N_{L|K}(x) = \prod_{\sigma \in G} \sigma x$ in $\mathfrak{P}' \cap \mathcal{O} = \mathfrak{p}$. Andererseits ist $x \notin \sigma\mathfrak{P}$ für alle $\sigma \in G$, also $\sigma x \notin \mathfrak{P}$ für alle $\sigma \in G$, und daher $\prod_{\sigma \in G} \sigma x \notin \mathfrak{P} \cap \mathcal{O} = \mathfrak{p}$, Widerspruch. □

(9.2) Definition. *Ist $\mathfrak{P}$ ein Primideal von $\mathcal{O}$, so heißt die Untergruppe*

$$G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$$

die **Zerlegungsgruppe** *von $\mathfrak{P}$ über K. Der Fixkörper*

$$Z_{\mathfrak{P}} = \{x \in L \mid \sigma x = x \quad \textit{für alle} \quad \sigma \in G_{\mathfrak{P}}\}$$

heißt der **Zerlegungskörper** *von $\mathfrak{P}$ über K.*

Die Zerlegungsgruppe sagt auf gruppentheoretische Weise, in wieviele verschiedene Primideale ein Primideal $\mathfrak{p}$ von o in $\mathcal{O}$ zerfällt. Ist nämlich $\mathfrak{P}$ eines von ihnen und durchläuft σ ein Repräsentantensystem für die Nebenklassen in $G/G_{\mathfrak{P}}$, so durchläuft $\sigma\mathfrak{P}$ die verschiedenen Primideale über $\mathfrak{p}$ genau einmal, d.h. ihre Anzahl ist der Index $(G : G_{\mathfrak{P}})$. Insbesondere gilt

$$\begin{array}{lllll} G_{\mathfrak{P}} = 1 & \Longleftrightarrow & Z_{\mathfrak{P}} = L & \Longleftrightarrow & \mathfrak{p} \quad \text{ist voll zerlegt,} \\ G_{\mathfrak{P}} = G & \Longleftrightarrow & Z_{\mathfrak{P}} = K & \Longleftrightarrow & \mathfrak{p} \quad \text{ist unzerlegt.} \end{array}$$

Die Zerlegungsgruppe eines zu $\mathfrak{P}$ konjugierten Primideals $\sigma\mathfrak{P}$ ist die konjugierte Untergruppe

$$G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1},$$

denn für $\tau \in G$ gilt

$$\begin{aligned} \tau \in G_{\sigma\mathfrak{P}} &\Longleftrightarrow \tau\sigma\mathfrak{P} = \sigma\mathfrak{P} \Longleftrightarrow \sigma^{-1}\tau\sigma\mathfrak{P} = \mathfrak{P} \\ &\Longleftrightarrow \sigma^{-1}\tau\sigma \in G_{\mathfrak{P}} \Longleftrightarrow \tau \in \sigma G_{\mathfrak{P}} \sigma^{-1}. \end{aligned}$$

Bemerkung: Die Zerlegungsgruppe regelt die Primzerlegung auch im Fall einer nicht-galoisschen Erweiterung. Sind U und V Untergruppen einer Gruppe G, so erhält man in G die Äquivalenzrelation

$$\sigma \sim \sigma' \Longleftrightarrow \sigma' = u\sigma v \quad \text{mit } u \in U,\ v \in V.$$

Die Äquivalenzklassen

$$U\sigma V = \{u\sigma v \mid u \in U,\ v \in V\}$$

heißen die **Doppelnebenklassen** von $G \bmod d U, V$. Die Menge dieser Doppelnebenklassen, in die G zerfällt, wird mit $U\backslash G/V$ bezeichnet.

Ist nun $L|K$ eine beliebige separable Erweiterung, so betten wir sie ein in eine galoissche Erweiterung $N|K$ mit der Galoisgruppe G und betrachten in G die Untergruppe $H = G(N|L)$. Sei $\mathfrak{p}$ ein Primideal von K und $P_\mathfrak{p}$ die Menge der über $\mathfrak{p}$ liegenden Primideale von L. Ist dann $\mathfrak{P}$ ein über $\mathfrak{p}$ liegendes Primideal von N, so ist die Zuordnung

$$H\backslash G/G_\mathfrak{P} \to P_\mathfrak{p}\,, \quad H\sigma G_\mathfrak{P} \mapsto \sigma\mathfrak{P} \cap L\,,$$

eine wohldefinierte Bijektion. Der Beweis ist dem Leser überlassen.

Im galoisschen Fall sind die Trägheitsgrade $f_1, \ldots, f_r$ und die Verzweigungsindizes $e_1, \ldots, e_r$ in der Primzerlegung

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$$

eines Primideals $\mathfrak{p}$ von K jeweils einander gleich,

$$f_1 = \cdots = f_r = f\,, \quad e_1 = \cdots = e_r = e\,.$$

Denn wenn wir $\mathfrak{P} = \mathfrak{P}_1$ setzen, so ist $\mathfrak{P}_i = \sigma_i\mathfrak{P}$ für passendes $\sigma_i \in G$, und der Isomorphismus $\sigma_i : \mathcal{O} \to \mathcal{O}$ induziert einen Isomorphismus

$$\mathcal{O}/\mathfrak{P} \xrightarrow{\sim} \mathcal{O}/\sigma_i\mathfrak{P}\,, \quad a \bmod \mathfrak{P} \mapsto \sigma_i a \bmod \sigma_i\mathfrak{P}\,,$$

so daß

$$f_i = [\,\mathcal{O}/\sigma_i\mathfrak{P} : o/\mathfrak{p}\,] = [\,\mathcal{O}/\mathfrak{P} : o/\mathfrak{p}\,], \quad i = 1, \ldots, r\,.$$

Wegen $\sigma_i(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$ ergibt sich ferner aus

$$\mathfrak{P}^\nu | \mathfrak{p}\mathcal{O} \iff \sigma_i(\mathfrak{P}^\nu) | \sigma_i(\mathfrak{p}\mathcal{O}) \iff (\sigma_i\mathfrak{P})^\nu | \mathfrak{p}\mathcal{O}$$

die Gleichheit der e_i, $i = 1, \ldots, r$. Die Primzerlegung von $\mathfrak{p}$ in $\mathcal{O}$ nimmt also im galoisschen Fall die einfache Gestalt

$$\mathfrak{p} = (\prod_\sigma \sigma\mathfrak{P})^e$$

an, wobei σ ein Repräsentantensystem für $G/G_\mathfrak{P}$ durchläuft. Der Zerlegungskörper $Z_\mathfrak{P}$ von $\mathfrak{P}$ über K hat für die Zerlegung von $\mathfrak{p}$ und die Zahlen e und f folgende Bedeutung.

(9.3) Satz. *Sei $\mathfrak{P}_Z = \mathfrak{P} \cap Z_\mathfrak{P}$ das unter $\mathfrak{P}$ liegende Primideal von $Z_\mathfrak{P}$. Dann gilt:*

(i) *$\mathfrak{P}_Z$ ist unzerlegt in L, d.h. $\mathfrak{P}$ ist das einzige über $\mathfrak{P}_Z$ liegende Primideal von L.*

(ii) $\mathfrak{P}$ *hat über* $Z_{\mathfrak{P}}$ *den Verzweigungsindex* e *und den Trägheitsgrad* f.

(iii) Verzweigungsindex und Trägheitsgrad von $\mathfrak{P}_Z$ *über* K *sind beide gleich 1.*

Beweis: (i) Wegen $G(L|Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$ sind die über $\mathfrak{P}_Z$ liegenden Primideale $\sigma\mathfrak{P}$, $\sigma \in G(L|Z_{\mathfrak{P}})$, gleich $\mathfrak{P}$.
(ii) Da die Verzweigungsindizes und Trägheitsgrade im galoisschen Fall gleich sind, lautet die fundamentale Gleichung

$$n = efr\,,$$

wobei $n := \#G$, $r = (G : G_{\mathfrak{P}})$. Daher ist $\#G_{\mathfrak{P}} = [\,L : Z_{\mathfrak{P}}\,] = ef$. Sei e' bzw. e'' der Verzweigungsindex von $\mathfrak{P}$ über $Z_{\mathfrak{P}}$ bzw. von $\mathfrak{P}_Z$ über K. Dann ist $\mathfrak{p} = \mathfrak{P}_Z^{e''} \cdot \ldots$ in $Z_{\mathfrak{P}}$ und $\mathfrak{P}_Z = \mathfrak{P}^{e'}$ in L, also $\mathfrak{p} = \mathfrak{P}^{e''e'} \cdot \ldots$, d.h. $e = e'e''$. Das gleiche Resultat $f = f'f''$ erhält man offensichtlich für die Trägheitsgrade. Die fundamentale Gleichung für die Zerlegung von $\mathfrak{P}_Z$ in L lautet $[\,L : Z_{\mathfrak{P}}\,] = e'f'$, d.h. es ist $e'f' = ef$ und somit $e' = e$, $f' = f$, $e'' = f'' = 1$. □

Der Verzweigungsindex e und der Trägheitsgrad f besitzen eine weitere interessante gruppentheoretische Interpretation. Jedes $\sigma \in G_{\mathfrak{P}}$ induziert nämlich wegen $\sigma\mathcal{O} = \mathcal{O}$ und $\sigma\mathfrak{P} = \mathfrak{P}$ einen Automorphismus

$$\bar{\sigma} : \mathcal{O}/\mathfrak{P} \to \mathcal{O}/\mathfrak{P}\,, \quad a \bmod \mathfrak{P} \mapsto \sigma a \bmod \mathfrak{P}\,,$$

des Restklassenkörpers $\mathcal{O}/\mathfrak{P}$. Setzt man $\kappa(\mathfrak{P}) = \mathcal{O}/\mathfrak{P}$ und $\kappa(\mathfrak{p}) = o/\mathfrak{p}$, so gilt der

(9.4) Satz. *Die Erweiterung* $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ *ist normal, und man hat einen surjektiven Homomorphismus*

$$G_{\mathfrak{P}} \to G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})).$$

Beweis: Der Trägheitsgrad von $\mathfrak{P}_Z$ über K ist gleich 1, d.h. $Z_{\mathfrak{P}}$ hat den gleichen Restklassenkörper $\kappa(\mathfrak{p})$ wie K bzgl. $\mathfrak{p}$. Wir können daher $Z_{\mathfrak{P}} = K$, also $G_{\mathfrak{P}} = G$ annehmen. Sei $\theta \in \mathcal{O}$ ein Repräsentant eines Elementes $\bar{\theta} \in \kappa(\mathfrak{P})$ und $f(X)$ bzw. $\bar{g}(X)$ das Minimalpolynom von θ über K bzw. von $\bar{\theta}$ über $\kappa(\mathfrak{p})$. Dann ist $\bar{\theta} = \theta \bmod \mathfrak{p}$ Nullstelle des Polynoms $\bar{f}(X) = f(X) \bmod \mathfrak{p}$, d.h. $\bar{g}(X)$ teilt $\bar{f}(X)$. Da $L|K$ normal ist, so zerfällt $f(X)$ über $\mathcal{O}$ in Linearfaktoren. Daher zerfällt $\bar{f}(X)$ und

somit auch $\bar{g}(X)$ über $\kappa(\mathfrak{P})$ in Linearfaktoren, d.h. $\kappa(\mathfrak{P}) \mid \kappa(\mathfrak{p})$ ist normal.

Sei jetzt $\bar{\theta}$ ein primitives Element für die maximale separable Teilerweiterung von $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ und

$$\bar{\sigma} \in G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) = G(\kappa(\mathfrak{p})(\bar{\theta})|\kappa(\mathfrak{p}))\,.$$

Dann ist $\bar{\sigma}\bar{\theta}$ Nullstelle von $\bar{g}(X)$, also von $\bar{f}(X)$, d.h. es gibt eine Nullstelle θ' von $f(X)$ mit $\theta' \equiv \bar{\sigma}\bar{\theta} \bmod \mathfrak{P}$. θ' ist konjugiert zu θ, d.h. $\theta' = \sigma\theta$ mit einem $\sigma \in G(L|K)$. Wegen $\sigma\theta \equiv \bar{\sigma}\bar{\theta} \bmod \mathfrak{P}$ wird σ unter dem fraglichen Homomorphismus auf $\bar{\sigma}$ abgebildet, der damit surjektiv ist. □

(9.5) Definition. *Der Kern $I_{\mathfrak{P}} \subseteq G_{\mathfrak{P}}$ des Homomorphismus*

$$G_{\mathfrak{P}} \to G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$$

heißt die **Trägheitsgruppe** *von $\mathfrak{P}$ über K. Der Fixkörper*

$$T_{\mathfrak{P}} = \{x \in L \mid \sigma x = x \quad \text{für alle} \quad \sigma \in I_{\mathfrak{P}}\}$$

heißt der **Trägheitskörper** *von $\mathfrak{P}$ über K.*

Mit dem Trägheitskörper $T_{\mathfrak{P}}$ erhalten wir die Körperkette

$$K \subseteq Z_{\mathfrak{P}} \subseteq T_{\mathfrak{P}} \subseteq L$$

und haben die exakte Sequenz

$$1 \to I_{\mathfrak{P}} \to G_{\mathfrak{P}} \to G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) \to 1\,.$$

Es gilt hierüber der

(9.6) Satz. *Die Erweiterung $T_{\mathfrak{P}}|Z_{\mathfrak{P}}$ ist normal, und es gilt*

$$G(T_{\mathfrak{P}}|Z_{\mathfrak{P}}) \cong G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))\,, \quad G(L|T_{\mathfrak{P}}) = I_{\mathfrak{P}}\,.$$

Ist die Restkörpererweiterung $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ separabel, so ist

$$\#I_{\mathfrak{P}} = [\,L : T_{\mathfrak{P}}\,] = e\,, \quad (G_{\mathfrak{P}} : I_{\mathfrak{P}}) = [\,T_{\mathfrak{P}} : Z_{\mathfrak{P}}\,] = f\,.$$

In diesem Fall gilt für das unter $\mathfrak{P}$ liegende Primideal $\mathfrak{P}_T$ von $T_{\mathfrak{P}}$:

(i) Der Verzweigungsindex von $\mathfrak{P}$ über $\mathfrak{P}_T$ ist e und der Trägheitsgrad ist 1.

(ii) Der Verzweigungsindex von $\mathfrak{P}_T$ über $\mathfrak{P}_Z$ ist 1 und der Trägheitsgrad ist f.

Beweis: Die ersten Behauptungen folgen aus $\#G_{\mathfrak{P}} = ef$, so daß nur die Aussagen unter (i) und (ii) zu zeigen sind. Sie folgen mit der fundamentalen Gleichung alle aus $\kappa(\mathfrak{P}_T) = \kappa(\mathfrak{P})$. Beachtet man, daß die Trägheitsgruppe $I_{\mathfrak{P}}$ von $\mathfrak{P}$ über K gleichzeitig die Trägheitsgruppe von $\mathfrak{P}$ über $T_{\mathfrak{P}}$ ist, so folgt, wenn man den Satz (9.4) auf die Erweiterung $L|T_{\mathfrak{P}}$ anwendet, $G(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_T)) = 1$, also $\kappa(\mathfrak{P}_T) = \kappa(\mathfrak{P})$. □

In dem Bild

$$K \overset{1}{\underset{1}{-}} Z_{\mathfrak{P}} \overset{1}{\underset{f}{-}} T_{\mathfrak{P}} \overset{e}{\underset{1}{-}} L$$

haben wir die Verzweigungsindizes der einzelnen Körpererweiterungen oben und die Trägheitsgrade unten vermerkt. Insbesondere gilt im Falle der Separabilität von $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$

$$I_{\mathfrak{P}} = 1 \iff T_{\mathfrak{P}} = L \iff \mathfrak{p} \text{ ist unverzweigt in } L\,.$$

In diesem Fall kann man die Galoisgruppe $G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) \cong G_{\mathfrak{P}}$ der Restkörpererweiterung als Untergruppe von $G = G(L|K)$ ansehen.

Die Hilbertsche Verzweigungstheorie gehört mit vielen Verfeinerungen und Verallgemeinerungen ihrer Natur nach der Bewertungstheorie an, die wir im nächsten Kapitel entwickeln werden (vgl. Kap. II, § 9).

Aufgabe 1. Ist $L|K$ eine galoissche Erweiterung algebraischer Zahlkörper mit nicht-zyklischer Galoisgruppe, so gibt es höchstens endlich viele unzerlegte Primideale von K.

Aufgabe 2. Ist $L|K$ eine galoissche Erweiterung algebraischer Zahlkörper und $\mathfrak{P}$ ein über K unverzweigtes Primideal (d.h. $\mathfrak{p} = \mathfrak{P} \cap K$ ist unverzweigt in L), so gibt es genau einen Automorphismus $\varphi_{\mathfrak{P}} \in G(L|K)$ mit

$$\varphi_{\mathfrak{P}} a \equiv a^q \bmod \mathfrak{P} \quad \text{für alle } a \in \mathcal{O}\,,$$

wobei $q = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})]$, den **Frobenius-Automorphismus**. Die Zerlegungsgruppe $G_{\mathfrak{P}}$ ist zyklisch, und $\varphi_{\mathfrak{P}}$ ist ein Erzeugendes von $G_{\mathfrak{P}}$.

Aufgabe 3. Sei $L|K$ eine auflösbare Erweiterung vom Primzahlgrad p (nicht notwendig galoissch). Besitzt dann das unverzweigte Primideal $\mathfrak{p}$ in L zwei Primfaktoren $\mathfrak{P}$ und $\mathfrak{P}'$ vom Grade 1, so ist es sogar voll zerlegt (Satz von *F.K. Schmidt*).

Hinweis: Benutze den folgenden Satz von *Galois* (vgl. [75], Kap. II, § 3): Ist G eine transitive auflösbare Permutationsgruppe vom Primzahlgrad p, so gibt es außer 1 keine Permutation $\sigma \in G$, die zwei verschiedene Ziffern festläßt.

Aufgabe 4. Sei $L|K$ eine endliche (nicht notwendig galoissche) Erweiterung algebraischer Zahlkörper und $N|K$ die normale Hülle von $L|K$. Zeige: Ein Primideal $\mathfrak{p}$ von K ist genau dann voll zerlegt in L, wenn es voll zerlegt in N ist.

Hinweis: Benutze die Doppelmodul-Zerlegung $H\backslash G/G_{\mathfrak{P}}$, wobei $G = G(N|K)$, $H = G(N|L)$ und $G_{\mathfrak{P}}$ die Zerlegungsgruppe eines Primideals $\mathfrak{P}$ über $\mathfrak{p}$ ist.

§ 10. Kreisteilungskörper

Die Begriffsbildungen und Ergebnisse der bisher entwickelten Theorie haben einen Abstraktionsgrad erreicht, dem jetzt etwas Konkretes entgegengestellt werden soll. Wir wollen die durch die allgemeine Theorie gewonnenen Einsichten am Beispiel des **n-ten Kreisteilungskörpers** erproben und explizieren, also am Körper $\mathbb{Q}(\zeta)$, wobei ζ eine **primitive n-te Einheitswurzel** ist. Unter allen Zahlkörpern nimmt dieser Körper eine zentrale Sonderstellung ein und wird hier nicht nur als ein lehrreiches Beispiel vorgestellt, sondern als ein wesentlicher Baustein der weiterführenden Theorie.

Unser erstes Ziel soll sein, die ganzen Zahlen des Körpers $\mathbb{Q}(\zeta)$ in expliziter Weise zu bestimmen. Wir benötigen dazu das

(10.1) Lemma. *Sei n eine Primzahlpotenz l^ν und $\lambda = 1 - \zeta$. Dann ist im Ring $\mathcal{O}$ der ganzen Zahlen von $\mathbb{Q}(\zeta)$ das Hauptideal (λ) ein Primideal vom Grad 1, und es gilt*

$$l\mathcal{O} = (\lambda)^d, \quad \text{wobei} \quad d = \varphi(l^\nu) = [\,\mathbb{Q}(\zeta) : \mathbb{Q}\,].$$

Ferner hat die Basis $1, \zeta, \ldots, \zeta^{d-1}$ von $\mathbb{Q}(\zeta)|\mathbb{Q}$ die Diskriminante

$$d(1, \zeta, \ldots, \zeta^{d-1}) = \pm l^s, \quad s = l^{\nu-1}(\nu l - \nu - 1).$$

Beweis: Das Minimalpolynom von ζ über $\mathbb{Q}$ ist das n-te Kreisteilungspolynom

$$\phi_n(X) = (X^{l^\nu} - 1)/(X^{l^{\nu-1}} - 1) = X^{l^{\nu-1}(l-1)} + \cdots + X^{l^{\nu-1}} + 1.$$

Setzen wir $X = 1$, so ergibt sich die Gleichung

$$l = \prod_{g \in (\mathbb{Z}/n\mathbb{Z})^*} (1 - \zeta^g).$$

Nun ist $1 - \zeta^g = \varepsilon_g(1 - \zeta)$ mit der ganzen Zahl $\varepsilon_g = \frac{1-\zeta^g}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{g-1}$. Ist g' eine Zahl mit $gg' \equiv 1 \bmod l^\nu$, so ist $\frac{1-\zeta}{1-\zeta^g} = \frac{1-(\zeta^g)^{g'}}{1-\zeta^g} =$

$1 + \zeta^g + \cdots + (\zeta^g)^{g'-1}$ ebenfalls ganz, d.h. ε_g ist eine Einheit. Es folgt $l = \varepsilon(1-\zeta)^{\varphi(l^\nu)}$ mit der Einheit $\varepsilon = \prod_g \varepsilon_g$, also $l\mathcal{O} = (\lambda)^{\varphi(l^\nu)}$. Wegen $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(l^\nu)$ zeigt die fundamentale Gleichung (8.2), daß (λ) ein Primideal vom Grad 1 ist.

Seien $\zeta = \zeta_1, \ldots, \zeta_d$ die Konjugierten von ζ. Dann ist $\phi_n(X) = \prod_{i=1}^d (X - \zeta_i)$ und (vgl. § 2, S. 11)

$$\pm d(1, \zeta, \ldots, \zeta^{d-1}) = \prod_{i \neq j} (\zeta_i - \zeta_j) = \prod_{i=1}^d \phi_n'(\zeta_i) = N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\phi_n'(\zeta)) .$$

Differenziert man die Gleichung

$$(X^{l^{\nu-1}} - 1)\phi_n(X) = X^{l^\nu} - 1$$

und setzt ζ ein, so erhält man

$$(\xi - 1)\phi_n'(\zeta) = l^\nu \zeta^{-1}$$

mit der primitiven l-ten Einheitswurzel $\xi = \zeta^{l^{\nu-1}}$. Für sie gilt $N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi - 1) = \pm l$, so daß

$$N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\xi - 1) = N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi - 1)^{l^{\nu-1}} = \pm l^{l^{\nu-1}} .$$

Beachten wir, daß ζ^{-1} die Norm ± 1 hat, so erhalten wir

$$d(1, \zeta, \ldots, \zeta^{d-1}) = \pm N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\phi_n'(\zeta)) = \pm l^{\nu l^{\nu-1}(l-1) - l^{\nu-1}} = \pm l^s$$

mit $s = l^{\nu-1}(\nu l - \nu - 1)$. □

Die ganzen Zahlen von $\mathbb{Q}(\zeta)$ bestimmen sich jetzt für beliebiges n wie folgt:

(10.2) Satz. *Für den Ring $\mathcal{O}$ der ganzen Zahlen von $\mathbb{Q}(\zeta)$ ist $1, \zeta, \ldots, \zeta^{d-1}$, $d = \varphi(n)$, eine Ganzheitsbasis, d.h.*

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{d-1} = \mathbb{Z}[\zeta] .$$

Beweis: Wir beweisen den Satz zuerst im Fall, daß n eine Primzahlpotenz l^ν ist. Wegen $d(1, \zeta, \ldots, \zeta^{d-1}) = \pm l^s$ erhalten wir nach (2.9)

$$l^s \mathcal{O} \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O} .$$

Setzen wir $\lambda = 1 - \zeta$, so ist nach Lemma (10.1) $\mathcal{O}/\lambda\mathcal{O} \cong \mathbb{Z}/l\mathbb{Z}$, also $\mathcal{O} = \mathbb{Z} + \lambda\mathcal{O}$, und erst recht

$$\lambda\mathcal{O} + \mathbb{Z}[\zeta] = \mathcal{O} .$$

Multiplizieren wir dies mit λ und setzen das Ergebnis $\lambda\mathfrak{o} = \lambda^2\mathfrak{o} + \lambda\mathbb{Z}[\zeta]$ ein, so ergibt sich

$$\lambda^2\mathfrak{o} + \mathbb{Z}[\zeta] = \mathfrak{o}\,,$$

und wenn wir so fortfahren,

$$\lambda^t\mathfrak{o} + \mathbb{Z}[\zeta] = \mathfrak{o} \quad \text{für alle} \quad t \geq 1\,.$$

Für $t = s\varphi(l^\nu)$ folgt hieraus wegen $l\mathfrak{o} = \lambda^{\varphi(l^\nu)}\mathfrak{o}$ (vgl. (10.1))

$$\mathfrak{o} = \lambda^t\mathfrak{o} + \mathbb{Z}[\zeta] = l^s\mathfrak{o} + \mathbb{Z}[\zeta] = \mathbb{Z}[\zeta]\,.$$

Im allgemeinen Fall sei $n = l_1^{\nu_1} \ldots l_r^{\nu_r}$. Dann ist $\zeta_i = \zeta^{n/l_i^{\nu_i}}$ eine primitive $l_i^{\nu_i}$-te Einheitswurzel, und es ist

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1)\cdots\mathbb{Q}(\zeta_r)$$

und $\mathbb{Q}(\zeta_1)\cdots\mathbb{Q}(\zeta_{i-1}) \cap \mathbb{Q}(\zeta_i) = \mathbb{Q}$. Für jedes $i = 1, \ldots, r$ bilden die Elemente $1, \zeta_i, \ldots, \zeta_i^{d_i-1}$, $d_i = \varphi(l_i^{\nu_i})$, nach dem soeben Bewiesenen eine Ganzheitsbasis von $\mathbb{Q}(\zeta_i)|\mathbb{Q}$. Da die Diskriminanten $d(1, \zeta_i, \ldots, \zeta_i^{d_i-1}) = \pm l_i^{s_i}$ paarweise teilerfremd sind, so schließen wir aus (2.11) in sukzessiver Weise, daß die Elemente $\zeta_1^{j_1} \cdot \ldots \cdot \zeta_r^{j_r}$, $j_i = 0, \ldots, d_i - 1$, eine Ganzheitsbasis von $\mathbb{Q}(\zeta)|\mathbb{Q}$ bilden. Jedes dieser Elemente ist aber eine Potenz von ζ. Daher kann man jedes $\alpha \in \mathfrak{o}$ als ein Polynom $\alpha = f(\zeta)$ mit Koeffizienten in $\mathbb{Z}$ schreiben. Da ζ über $\mathbb{Q}$ den Grad $\varphi(n)$ hat, so läßt sich der Grad des Polynoms $f(\zeta)$ auf $\varphi(n) - 1$ reduzieren. Man erhält so eine Darstellung

$$\alpha = a_0 + a_1\zeta + \cdots + a_{\varphi(n)-1}\zeta^{\varphi(n)-1}\,.$$

$1, \zeta, \ldots, \zeta^{\varphi(n)-1}$ ist also in der Tat eine Ganzheitsbasis. □

Nachdem wir wissen, daß $\mathbb{Z}[\zeta]$ der Ring der ganzen Zahlen des Körpers $\mathbb{Q}(\zeta)$ ist, ist es uns jetzt möglich, auch das Zerlegungsgesetz der Primzahlen p in Primideale von $\mathbb{Q}(\zeta)$ explizit anzugeben. Es ist von schönster Einfachheit.

(10.3) Satz. *Sei $n = \prod_p p^{\nu_p}$ die Primzerlegung von n, und für jede Primzahl p sei f_p die kleinste natürliche Zahl, so daß*

$$p^{f_p} \equiv 1 \bmod n/p^{\nu_p}\,.$$

Dann findet in $\mathbb{Q}(\zeta)$ die Zerlegung

$$p = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r)^{\varphi(p^{\nu_p})}$$

statt, wobei $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ verschiedene Primideale vom gleichen Grade f_p sind.

Beweis: Wegen $o = \mathbb{Z}[\zeta]$ ist der Führer von $\mathbb{Z}[\zeta]$ gleich 1, und wir können für jede Primzahl p den Satz (8.3) anwenden. Danach zerfällt p auf die gleiche Weise in Primfaktoren wie das Minimalpolynom $\phi_n(X)$ von ζ in irreduzible Faktoren mod p. Wir müssen also nur zeigen, daß

$$\phi_n(X) \equiv (p_1(X) \cdot \ldots \cdot p_r(X))^{\varphi(p^{\nu_p})} \bmod p\,,$$

wobei $p_1(X), \ldots, p_r(X)$ verschiedene irreduzible Polynome über $\mathbb{Z}/p\mathbb{Z}$ vom Grade f_p sind. Wir setzen dazu $n = p^{\nu_p} m$. Durchläuft ξ_i bzw. η_j die primitiven m-ten bzw. p^{ν_p}-ten Einheitswurzeln, so durchlaufen die Produkte $\xi_i \eta_j$ gerade die primitiven n-ten Einheitswurzeln, d.h. es gilt in o

$$\phi_n(X) = \prod_{i,j} (X - \xi_i \eta_j)\,.$$

Wegen $X^{p^{\nu_p}} - 1 \equiv (X-1)^{p^{\nu_p}} \bmod p$ ist $\eta_j \equiv 1 \bmod \mathfrak{p}$ mit einem beliebigen Primideal $\mathfrak{p} | p$, d.h.

$$\phi_n(X) \equiv \prod_i (X - \xi_i)^{\varphi(p^{\nu_p})} = \phi_m(X)^{\varphi(p^{\nu_p})} \bmod \mathfrak{p}\,.$$

Hieraus folgt die Kongruenz

$$\phi_n(X) \equiv \phi_m(X)^{\varphi(p^{\nu_p})} \bmod p\,.$$

Beachten wir, daß f_p die kleinste Zahl mit $p^{f_p} \equiv 1 \bmod m$ ist, so ist klar, daß wir durch diese Kongruenz auf den Fall $p \nmid n$, also $\varphi(p^{\nu_p}) = \varphi(1) = 1$ zurückgeführt sind.

Da die Charakteristik p von $o/\mathfrak{p}$ nicht in n aufgeht, so haben $X^n - 1$ und nX^{n-1} in $o/\mathfrak{p}$ keine gemeinsame Nullstelle, d.h. $X^n - 1 \bmod \mathfrak{p}$ hat keine mehrfachen Nullstellen. Beim Übergang $o \to o/\mathfrak{p}$ wird also die Gruppe μ_n der n-ten Einheitswurzeln bijektiv auf die Gruppe der n-ten Einheitswurzeln von $o/\mathfrak{p}$ abgebildet. Insbesondere bleibt die primitive n-te Einheitswurzel ζ modulo $\mathfrak{p}$ eine primitive n-te Einheitswurzel. Der kleinste Erweiterungskörper von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, der sie enthält, ist der Körper $\mathbb{F}_{p^{f_p}}$, denn seine multiplikative Gruppe $\mathbb{F}^*_{p^{f_p}}$ ist zyklisch von der Ordnung $p^{f_p} - 1$. Daher ist $\mathbb{F}_{p^{f_p}}$ der Zerfällungskörper des reduzierten Kreisteilungspolynoms

$$\bar{\phi}_n(X) = \phi_n(X) \bmod p\,.$$

Dieses hat als Teiler von $X^n - 1 \bmod p$ keine mehrfachen Nullstellen, und wenn

$$\bar{\phi}_n(X) = \bar{p}_1(X) \cdot \ldots \cdot \bar{p}_r(X)$$

seine Zerlegung in irreduzible Faktoren über $\mathbb{F}_p$ ist, so ist jedes $\bar{p}_i(X)$ das Minimalpolynom einer primitiven n-ten Einheitswurzel $\bar{\xi} \in \mathbb{F}^*_{p^{f_p}}$, hat also den Grad f_p. Damit ist der Satz bewiesen. □

Wir heben zwei Sonderfälle des obigen Zerlegungsgesetzes hervor:

(10.4) Korollar. *Eine Primzahl p ist genau dann verzweigt in $\mathbb{Q}(\zeta)$, wenn*

$$n \equiv 0 \bmod p,$$

es sei denn $p = 2 = (4, n)$. Eine Primzahl $p \neq 2$ ist genau dann voll zerlegt in $\mathbb{Q}(\zeta)$, wenn

$$p \equiv 1 \bmod n.$$

Die Vollständigkeit der Resultate über die Ganzheitsbasis und die Primzerlegung im Körper $\mathbb{Q}(\zeta)$ setzt sich bei der Betrachtung der Einheitengruppe und der Idealklassengruppe nicht fort. Die sich in diesem Zusammenhang bietenden Probleme gehören vielmehr zu den schwierigsten, die die algebraische Zahlentheorie stellt. Andererseits begegnet man hier einer Fülle ganz überraschender Gesetzmäßigkeiten, die der Gegenstand einer erst in jüngerer Zeit entstandenen Theorie geworden sind, der **Iwasawa-Theorie.**

Durch das Zerlegungsgesetz (10.3) im Kreisteilungskörper erfährt das Gaußsche Reziprozitätsgesetz (8.6) seine eigentliche Erklärung. Dies beruht auf dem folgenden

(10.5) Satz. *Seien l und p ungerade Primzahlen, $l^* = (-1)^{\frac{l-1}{2}} l$ und ζ eine primitive l-te Einheitswurzel. Dann gilt:*

p ist voll zerlegt in $\mathbb{Q}(\sqrt{l^*})$ $\iff$ p zerfällt in $\mathbb{Q}(\zeta)$ in eine gerade Zahl von Primidealen.

Beweis: Die kleine Rechnung in § 8, S. 54 hat uns gezeigt, daß $l^* = \tau^2$ mit $\tau = \sum_{a \in (\mathbb{Z}/l\mathbb{Z})^*} \left(\frac{a}{l}\right) \zeta^a$, so daß $\mathbb{Q}(\sqrt{l^*}) \subseteq \mathbb{Q}(\zeta)$. Ist p voll zerlegt in $\mathbb{Q}(\sqrt{l^*})$, $p = \mathfrak{p}_1 \mathfrak{p}_2$, so überführt ein Automorphismus σ von $\mathbb{Q}(\zeta)$ mit $\sigma \mathfrak{p}_1 = \mathfrak{p}_2$ die Menge der über $\mathfrak{p}_1$ liegenden Primideale bijektiv in die Menge der über $\mathfrak{p}_2$ liegenden Primideale. Daher ist die Anzahl der über p liegenden Primideale von $\mathbb{Q}(\zeta)$ gerade. Nehmen wir umgekehrt das letztere an, so ist der Index der Zerlegungsgruppe $G_\mathfrak{p}$, also der Grad $[Z_\mathfrak{p} : \mathbb{Q}]$ des Zerlegungskörpers eines Primideals $\mathfrak{p}$ von $\mathbb{Q}(\zeta)$ über p gerade. Da $G(\mathbb{Q}(\zeta)|\mathbb{Q})$ zyklisch ist, folgt $\mathbb{Q}(\sqrt{l^*}) \subseteq Z_\mathfrak{p}$. Der Trägheitsgrad

von $\mathfrak{p} \cap Z_{\mathfrak{p}}$ über $\mathbb{Q}$ ist 1 nach (9.3), also auch der von $\mathfrak{p} \cap \mathbb{Q}(\sqrt{l^*})$. Hieraus folgt, daß p voll zerlegt ist in $\mathbb{Q}(\sqrt{l^*})$. □

Mit diesem Satz ergibt sich für zwei ungerade Primzahlen l und p das Reziprozitätsgesetz

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

wie folgt. Es genügt zu zeigen, daß

$$\left(\frac{l^*}{p}\right) = \left(\frac{p}{l}\right)$$

ist, denn mit dem ganz elementaren Resultat $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (vgl. § 8, S. 54) folgt dann

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

Nach (8.5) und (10.5) ist $(\frac{l^*}{p}) = 1$ genau dann, wenn p im Körper $\mathbb{Q}(\zeta)$ der l-ten Einheitswurzeln in eine gerade Anzahl von Primidealen zerfällt. Nach (10.3) ist diese Anzahl $r = \frac{l-1}{f}$, wobei f die kleinste Zahl mit $p^f \equiv 1 \bmod l$ ist, d.h. r ist genau dann gerade, wenn f ein Teiler von $\frac{l-1}{2}$ ist. Dies aber ist gleichbedeutend mit $p^{(l-1)/2} \equiv 1 \bmod l$. Da ein Element in der zyklischen Gruppe $\mathbb{F}_l^*$ genau dann eine in $\frac{l-1}{2}$ aufgehende Ordnung hat, wenn es in $\mathbb{F}_l^{*2}$ liegt, so ist die letzte Kongruenz gleichbedeutend mit $\left(\frac{p}{l}\right) = 1$. Es ist also in der Tat $\left(\frac{l^*}{p}\right) = \left(\frac{p}{l}\right)$.

Das Gaußsche Reziprozitätsgesetz war der historische Ausgangspunkt der Entwicklung der algebraischen Zahlentheorie. Es wurde von *Euler* entdeckt, von *Gauss* aber als erstem bewiesen. Die Suche nach ähnlichen Gesetzen für höhere Potenzreste, d.h. für die Kongruenzen $x^n \equiv a \bmod p$, $n > 2$, hat die Zahlentheorie für eine lange Zeit beherrscht. Das Bemühen um dieses Problem, das die Betrachtung des n-ten Kreisteilungskörpers erzwang, führte *Kummer* zu seiner bahnbrechenden Entdeckung der Idealtheorie, deren Grundlagen wir in den vorangegangenen Paragraphen gelegt und deren Wirkung wir am Beispiel der Kreisteilungskörper erfolgreich erprobt haben. Die Weiterentwicklung dieser Theorie hat zu einer allumfassenden Verallgemeinerung des Gaußschen Reziprozitätsgesetzes geführt, dem **Artinschen Reziprozitätsgesetz**, einem Höhepunkt in der Geschichte der Zahlentheorie

von bezwingendem Reiz. Dieses Gesetz ist der Hauptsatz der **Klassenkörpertheorie**, die wir in Kapitel IV–VI entwickeln werden.

Aufgabe 1 (Dirichletscher Primzahlsatz). Zu jeder natürlichen Zahl n gibt es unendlich viele Primzahlen $p \equiv 1 \bmod n$.

Hinweis: Angenommen, es gebe nur endlich viele. Sei P ihr Produkt. Sei ϕ_n das n-te Kreisteilungspolynom. Nicht alle Zahlen $\phi_n(xnP)$, $x \in \mathbb{Z}$, können gleich 1 sein. Sei $p|\phi_n(xnP)$ für passendes x. Leite hieraus einen Widerspruch her. (Der Dirichletsche Primzahlsatz gilt allgemeiner für $p \equiv a \bmod n$, $(a,n) = 1$ (vgl. VII, (5.14) und VII, § 13)).

Aufgabe 2. Zu jeder endlichen abelschen Gruppe A gibt es eine galoissche Erweiterung $L|\mathbb{Q}$ mit der Galoisgruppe $G(L|\mathbb{Q}) \cong A$.

Hinweis: Benutze Aufgabe 1.

Aufgabe 3. Jeder quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ ist in einem Kreiskörper $\mathbb{Q}(\zeta_n)$ enthalten, ζ_n eine primitive n-te Einheitswurzel.

Aufgabe 4. Man beschreibe die quadratischen Teilkörper von $\mathbb{Q}(\zeta_n)|\mathbb{Q}$, wenn n ungerade ist.

Aufgabe 5. Man zeige, daß $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$ die quadratischen Teilkörper von $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ sind, wenn $n = 2^q$, $q \geq 3$.

§ 11. Lokalisierung

„Lokalisierung" bedeutet Quotientenbildung, wie sie uns im vertrautesten Fall beim Übergang eines Integritätsbereiches A zu seinem Quotientenkörper

$$K = \left\{ \frac{a}{b} \mid a \in A,\, b \in A \setminus \{0\} \right\}$$

begegnet. Wählt man anstelle von $A \setminus \{0\}$ eine beliebige nicht leere Teilmenge $S \subseteq A \setminus \{0\}$, die unter der Multiplikation abgeschlossen ist, so erhält man allgemeiner in der Menge

$$AS^{-1} = \left\{ \frac{a}{s} \in K \mid a \in A,\, s \in S \right\}$$

wieder einen Ring. Der wichtigste Fall einer solchen multiplikativen Teilmenge ist das Komplement $S = A \setminus \mathfrak{p}$ eines Primideals $\mathfrak{p}$ von A. In diesem Fall schreibt man $A_\mathfrak{p}$ anstelle von AS^{-1} und nennt den Ring $A_\mathfrak{p}$ die **Lokalisierung** von A bei $\mathfrak{p}$. Bei Problemstellungen, die sich auf ein einziges Primideal $\mathfrak{p}$ von A beziehen, ist es oft günstig, von A zur Lokalisierung $A_\mathfrak{p}$ überzugehen. Sie vergißt alles, was nichts mit $\mathfrak{p}$ zu tun

hat und bringt dafür die auf $\mathfrak{p}$ bezogenen Eigenschaften klarer heraus. Z.B. ist die Zuordnung

$$\mathfrak{q} \mapsto \mathfrak{q}A_{\mathfrak{p}}$$

eine 1-1-Korrespondenz zwischen den Primidealen $\mathfrak{q} \subseteq \mathfrak{p}$ von A und den Primidealen von $A_{\mathfrak{p}}$. Für eine multiplikative Menge S gilt allgemeiner der

(11.1) Satz. *Die Zuordnungen*

$$\mathfrak{q} \mapsto \mathfrak{q}S^{-1} \quad \textit{und} \quad \mathfrak{Q} \mapsto \mathfrak{Q} \cap A$$

sind zueinander inverse 1-1-Korrespondenzen zwischen den Primidealen $\mathfrak{q} \subseteq A \setminus S$ *von* A *und den Primidealen* $\mathfrak{Q}$ *von* AS^{-1}.

Beweis: Ist $\mathfrak{q} \subseteq A \setminus S$ ein Primideal von A, so ist

$$\mathfrak{Q} = \mathfrak{q}S^{-1} = \left\{ \frac{q}{s} \mid q \in \mathfrak{q},\ s \in S \right\}$$

ein Primideal von AS^{-1}. In der Tat, mit der offenkundigen Bedeutung der Buchstaben folgt aus $\frac{a}{s}\frac{a'}{s'} \in \mathfrak{Q}$, also aus $\frac{aa'}{ss'} = \frac{q}{s''}$, daß $s''aa' = qss' \in \mathfrak{q}$, d.h. $aa' \in \mathfrak{q}$ wegen $s'' \notin \mathfrak{q}$, und somit a oder $a' \in \mathfrak{q}$, d.h. $\frac{a}{s}$ oder $\frac{a'}{s'} \in \mathfrak{Q}$. Ferner gilt

$$\mathfrak{q} = \mathfrak{Q} \cap A\,,$$

denn aus $\frac{q}{s} = a \in \mathfrak{Q} \cap A$ folgt $q = as \in \mathfrak{q}$, also $a \in \mathfrak{q}$ wegen $s \notin \mathfrak{q}$.

Sei umgekehrt $\mathfrak{Q}$ ein beliebiges Primideal von AS^{-1}. Dann ist $\mathfrak{q} = \mathfrak{Q} \cap A$ offensichtlich ein Primideal von A, und es gilt $\mathfrak{q} \subseteq A \setminus S$, denn enthielte $\mathfrak{q}$ ein $s \in S$, so wäre $1 = s \cdot \frac{1}{s} \in \mathfrak{Q}$ wegen $\frac{1}{s} \in AS^{-1}$. Ferner gilt

$$\mathfrak{Q} = \mathfrak{q}S^{-1}\,,$$

denn wenn $\frac{a}{s} \in \mathfrak{Q}$, so ist $a = \frac{a}{s} \cdot s \in \mathfrak{Q} \cap A = \mathfrak{q}$, also $\frac{a}{s} = a\frac{1}{s} \in \mathfrak{q}S^{-1}$. Die Zuordnungen $\mathfrak{q} \mapsto \mathfrak{q}S^{-1}$ und $\mathfrak{Q} \mapsto \mathfrak{Q} \cap A$ sind daher zueinander invers, womit der Satz bewiesen ist. □

In aller Regel ist S das Komplement der Vereinigung $\bigcup_{\mathfrak{p} \in X} \mathfrak{p}$ einer Menge X von Primidealen von A. Man schreibt in diesem Fall

$$A(X) = \left\{ \frac{f}{g} \mid f, g \in A,\ g \not\equiv 0 \bmod \mathfrak{p} \quad \text{für} \quad \mathfrak{p} \in X \right\}$$

anstelle von AS^{-1}. Die Primideale von $A(X)$ entsprechen nach (11.1) umkehrbar eindeutig den Primidealen von A, die in $\bigcup_{\mathfrak{p}\in X}\mathfrak{p}$ enthalten sind, alle anderen werden beim Übergang von A nach $A(X)$ außer Betracht gesetzt. Ist z.B. A ein Dedekindring, so überleben in $A(X)$ nur die Primideale aus X.

Für den Fall, daß X nur aus dem Primideal $\mathfrak{p}$ besteht, ist $A(X)$ die Lokalisierung

$$A_{\mathfrak{p}} = \left\{ \frac{f}{g} \mid f, g \in A,\ g \not\equiv 0 \bmod \mathfrak{p} \right\}$$

von A bei $\mathfrak{p}$. Über sie gilt das

(11.2) Korollar. *Ist $\mathfrak{p}$ ein Primideal von A, so ist $A_{\mathfrak{p}}$ ein* **lokaler Ring**, *d.h. $A_{\mathfrak{p}}$ besitzt ein einziges maximales Ideal, nämlich $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$. Man hat eine kanonische Einbettung*

$$A/\mathfrak{p} \hookrightarrow A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}},$$

durch die $A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$ zum Quotientenkörper von $A/\mathfrak{p}$ wird. Ist insbesondere $\mathfrak{p}$ ein maximales Ideal von A, so gilt

$$A/\mathfrak{p}^n \cong A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}^n \quad \text{für} \quad n \geq 1.$$

Beweis: Da die Ideale von $A_{\mathfrak{p}}$ umkehrbar eindeutig den in $\mathfrak{p}$ enthaltenen Idealen entsprechen, so ist $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$ das einzige maximale. Wir betrachten den Homomorphismus

$$f : A/\mathfrak{p}^n \to A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}^n, \quad a \bmod \mathfrak{p}^n \mapsto a \bmod \mathfrak{m}_{\mathfrak{p}}^n.$$

Für $n = 1$ ist f injektiv wegen $\mathfrak{p} = \mathfrak{m}_{\mathfrak{p}} \cap A$, so daß $A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}A_{\mathfrak{p}}$ der Quotientenkörper von $A/\mathfrak{p}$ wird. Sei $\mathfrak{p}$ maximal und $n \geq 1$. Für jedes $s \in A \setminus \mathfrak{p}$ gilt $\mathfrak{p}^n + sA = A$, d.h. $\bar{s} = s \bmod \mathfrak{p}^n$ ist eine Einheit in $A/\mathfrak{p}^n$. Für $n = 1$ ist dies wegen der Maximalität von $\mathfrak{p}$ klar und folgt für $n \geq 1$ mit vollständiger Induktion: $A = \mathfrak{p}^{n-1} + sA \Rightarrow \mathfrak{p} = \mathfrak{p}A = \mathfrak{p}(\mathfrak{p}^{n-1} + sA) \subsetneq \mathfrak{p}^n + sA \Rightarrow \mathfrak{p}^n + sA = A$.

Injektivität von f: Sei $a \in A$ mit $a \in \mathfrak{m}_{\mathfrak{p}}^n$, d.h. $a = b/s$ mit $b \in \mathfrak{p}^n$, $s \notin \mathfrak{p}$, also $as = b \in \mathfrak{p}^n$, so daß $\bar{a}\bar{s} = 0$ in $A/\mathfrak{p}^n$ und somit $\bar{a} = 0$ in $A/\mathfrak{p}^n$.

Surjektivität von f: Sei $a/s \in A_{\mathfrak{p}}$, $a \in A$, $s \notin \mathfrak{p}$. Dann gibt es nach dem Obigen ein $a' \in A$ mit $a \equiv a's \bmod \mathfrak{p}^n$, so daß $a/s \equiv a' \bmod \mathfrak{p}^n A_{\mathfrak{p}}$, d.h. $a/s \bmod \mathfrak{m}_{\mathfrak{p}}^n$ liegt im Bild von f. □

Bei einem lokalen Ring mit dem maximalen Ideal $\mathfrak{m}$ ist jedes Element $a \notin \mathfrak{m}$ eine Einheit, denn da das Hauptideal (a) in keinem anderen

maximalen Ideal liegen kann, so ist $(a) = A$. Es gilt also

$$A^* = A \setminus \mathfrak{m}.$$

Die einfachsten lokalen Ringe sind nach den Körpern die **diskreten Bewertungsringe**.

(11.3) Definition. *Ein diskreter Bewertungsring ist ein Hauptidealring $\mathfrak{o}$ mit einem einzigen maximalen Ideal $\mathfrak{p} \neq 0$.*

Das maximale Ideal ist von der Form $\mathfrak{p} = (\pi) = \pi\mathfrak{o}$ mit einem Primelement π. Da jedes nicht in $\mathfrak{p}$ gelegene Element eine Einheit ist, so ist π bis auf Assoziierte das einzige Primelement von $\mathfrak{o}$. Jedes von Null verschiedene Element von $\mathfrak{o}$ hat daher die Form $\varepsilon\pi^n$, $\varepsilon \in \mathfrak{o}^*$, $n \geq 0$. Allgemeiner läßt sich jedes Element $a \neq 0$ im Quotientenkörper K eindeutig in der Form

$$a = \varepsilon\pi^n, \quad \varepsilon \in \mathfrak{o}^*, \quad n \in \mathbb{Z},$$

schreiben. Der Exponent n heißt die **Bewertung** von a. Er wird mit $v(a)$ bezeichnet und ist offenbar durch die Gleichung

$$(a) = \mathfrak{p}^{v(a)}$$

bestimmt. Die Bewertung ist eine Funktion

$$v : K^* \to \mathbb{Z}.$$

Erweitert man sie auf K durch $v(0) = \infty$, so zeigt eine leichte Rechnung, daß sie die Bedingungen

$$v(ab) = v(a) + v(b), \quad v(a+b) \geq \min\{v(a), v(b)\}$$

erfüllt. Durch diese harmlos aussehende Funktion entsteht eine Theorie, die das ganze nächste Kapitel einnehmen wird.

Die diskreten Bewertungsringe treten als die Lokalisierungen der Dedekindringe auf. Dies beruht auf dem

(11.4) Satz. *Ist $\mathfrak{o}$ ein Dedekindring und $S \subseteq \mathfrak{o} \setminus \{0\}$ eine multiplikative Teilmenge, so ist auch $\mathfrak{o}S^{-1}$ ein Dedekindring.*

Beweis: Sei $\mathfrak{A}$ ein Ideal von $\mathfrak{o}S^{-1}$ und $\mathfrak{a} = \mathfrak{A} \cap \mathfrak{o}$. Dann ist $\mathfrak{A} = \mathfrak{a}S^{-1}$, denn wenn $\frac{a}{s} \in \mathfrak{A}$, $a \in \mathfrak{o}$, $s \in S$, so ist $a = s \cdot \frac{a}{s} \in \mathfrak{A} \cap \mathfrak{o} = \mathfrak{a}$, also $\frac{a}{s} = a \cdot \frac{1}{s} \in \mathfrak{a}S^{-1}$. Mit $\mathfrak{a}$ ist daher auch $\mathfrak{A}$ endlich erzeugt, d.h. $\mathfrak{o}S^{-1}$

ist noethersch. Aus (11.1) folgt, daß jedes Primideal von $\mathfrak{o}S^{-1}$ maximal ist, da dies in $\mathfrak{o}$ gilt. Schließlich ist $\mathfrak{o}S^{-1}$ ganzabgeschlossen, denn wenn $x \in K$ der Gleichung

$$x^n + \frac{a_1}{s_1}x^{n-1} + \cdots + \frac{a_n}{s_n} = 0$$

mit Koeffizienten $\frac{a_i}{s_i} \in \mathfrak{o}S^{-1}$ genügt, so zeigt die Multiplikation dieser Gleichung mit der n-ten Potenz von $s = s_1 \ldots s_n$, daß sx ganz über $\mathfrak{o}$ ist, also $sx \in \mathfrak{o}$ und somit $x \in \mathfrak{o}S^{-1}$. Daher ist $\mathfrak{o}S^{-1}$ ein Dedekindring.□

(11.5) Satz. *Sei $\mathfrak{o}$ ein noetherscher Integritätsbereich. $\mathfrak{o}$ ist genau dann ein Dedekindring, wenn die Lokalisierungen $\mathfrak{o}_\mathfrak{p}$ für alle Primideale $\mathfrak{p} \neq 0$ diskrete Bewertungsringe sind.*

Beweis: Ist $\mathfrak{o}$ ein Dedekindring, so sind es auch die Lokalisierungen $\mathfrak{o}_\mathfrak{p}$. Das maximale Ideal $\mathfrak{m} = \mathfrak{p}\mathfrak{o}_\mathfrak{p}$ ist das einzige Primideal von $\mathfrak{o}_\mathfrak{p}$. Wählt man ein $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$, so muß daher $(\pi) = \mathfrak{m}$ und ferner $\mathfrak{m}^n = (\pi^n)$ gelten. Daher ist $\mathfrak{o}_\mathfrak{p}$ ein Hauptidealring, also ein diskreter Bewertungsring.

Durchläuft $\mathfrak{p}$ alle Primideale $\neq 0$ von $\mathfrak{o}$, so gilt in jedem Falle

$$\mathfrak{o} = \bigcap_\mathfrak{p} \mathfrak{o}_\mathfrak{p} .$$

Ist nämlich $\frac{a}{b} \in \bigcap_\mathfrak{p} \mathfrak{o}_\mathfrak{p}$, $a, b \in \mathfrak{o}$, so ist

$$\mathfrak{a} = \{x \in \mathfrak{o} \mid xa \in b\mathfrak{o}\}$$

ein Ideal, das in keinem Primideal von $\mathfrak{o}$ enthalten sein kann, denn für jedes $\mathfrak{p}$ können wir $\frac{a}{b} = \frac{c}{s}$ mit $c \in \mathfrak{o}$, $s \notin \mathfrak{p}$ schreiben, so daß $sa = bc$, also $s \in \mathfrak{a} \setminus \mathfrak{p}$ ist. Da $\mathfrak{a}$ in keinem maximalen Ideal liegt, folgt $\mathfrak{a} = \mathfrak{o}$, also $a = 1 \cdot a \in b\mathfrak{o}$, d.h. $\frac{a}{b} \in \mathfrak{o}$.

Sind nun die $\mathfrak{o}_\mathfrak{p}$ diskrete Bewertungsringe, so sind sie als Hauptidealringe ganzabgeschlossen (vgl. § 2), d.h. auch $\mathfrak{o} = \bigcap_\mathfrak{p} \mathfrak{o}_\mathfrak{p}$ ist ganzabgeschlossen. Aus (11.1) folgt ferner, daß jedes Primideal $\mathfrak{p}$ von $\mathfrak{o}$ maximal ist, da dies in $\mathfrak{o}_\mathfrak{p}$ gilt. Daher ist $\mathfrak{o}$ ein Dedekindring. □

Bei einem Dedekindring $\mathfrak{o}$ haben wir zu jedem Primideal $\mathfrak{p} \neq 0$ den diskreten Bewertungsring $\mathfrak{o}_\mathfrak{p}$ und die zugehörige Bewertung

$$v_\mathfrak{p} : K^* \to \mathbb{Z}$$

des Quotientenkörpers. Die Bedeutung dieser Bewertungen liegt in ihrer Beziehung zur Primzerlegung. Ist $x \in K^*$ und

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}}$$

die Primidealzerlegung des Hauptideals (x), so ist

$$\nu_\mathfrak{p} = v_\mathfrak{p}(x)$$

für alle $\mathfrak{p}$. Denn für ein festes Primideal $\mathfrak{q} \neq 0$ von $\mathcal{O}$ folgt (wegen $\mathfrak{p}\mathcal{O}_\mathfrak{q} = \mathcal{O}_\mathfrak{q}$ für $\mathfrak{p} \neq \mathfrak{q}$) aus der ersten Gleichung

$$x\mathcal{O}_\mathfrak{q} = (\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}})\mathcal{O}_\mathfrak{q} = \mathfrak{q}^{\nu_\mathfrak{q}}\mathcal{O}_\mathfrak{q} = \mathfrak{m}_\mathfrak{q}^{\nu_\mathfrak{q}} ,$$

also in der Tat $v_\mathfrak{q}(x) = \nu_\mathfrak{q}$. Die Bewertungen $v_\mathfrak{p}$ werden aufgrund dieser Beziehung auch **Exponential-Bewertungen** genannt.

Man führe sich vor Augen, daß die Lokalisierung des Ringes $\mathbb{Z}$ nach dem Primideal $(p) = p\mathbb{Z}$ durch

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ p \nmid b \right\}$$

gegeben ist. Das maximale Ideal $p\mathbb{Z}_{(p)}$ besteht aus allen Brüchen a/b mit $p|a$, $p \nmid b$, und die Einheitengruppe aus allen Brüchen a/b mit $p \nmid ab$. Die zu $\mathbb{Z}_{(p)}$ gehörige Bewertung

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

heißt die ***p*-adische Bewertung** von $\mathbb{Q}$. Der Wert $v_p(x)$ eines Elementes $x \in \mathbb{Q}^*$ ergibt sich durch

$$v_p(x) = \nu ,$$

wenn $x = p^\nu a/b$ mit zu p teilerfremden ganzen Zahlen a, b ist.

Für eine Menge X von Primidealen $\neq 0$ des Dedekindringes $\mathcal{O}$, die fast alle Primideale von $\mathcal{O}$ enthält, wollen wir zum Schluß $\mathcal{O}$ mit dem Ring

$$\mathcal{O}(X) = \left\{ \frac{f}{g} \mid f, g \in \mathcal{O},\ g \not\equiv 0 \bmod \mathfrak{p} \quad \text{für} \quad \mathfrak{p} \in X \right\}$$

vergleichen. Die Primideale $\neq 0$ von $\mathcal{O}(X)$ sind nach (11.1) durch $\mathfrak{p}_X = \mathfrak{p}\mathcal{O}(X)$ gegeben, $\mathfrak{p} \in X$, und man prüft sofort, daß $\mathcal{O}$ und $\mathcal{O}(X)$ die gleichen Lokalisierungen

$$\mathcal{O}_\mathfrak{p} = \mathcal{O}(X)_{\mathfrak{p}_X}$$

haben. Wir bezeichnen mit $Cl(\mathcal{O})$ bzw. $Cl(\mathcal{O}(X))$ die Idealklassengruppen von $\mathcal{O}$ und $\mathcal{O}(X)$. Sie werden zusammen mit den Einheitengruppen $\mathcal{O}^*$ und $\mathcal{O}(X)^*$ durch den folgenden Satz verglichen.

(11.6) Satz. *Wir haben eine kanonische exakte Sequenz*

$$1 \to \mathcal{O}^* \to \mathcal{O}(X)^* \to \bigoplus_{\mathfrak{p} \notin X} K^*/\mathcal{O}_\mathfrak{p}^* \to Cl(\mathcal{O}) \to Cl(\mathcal{O}(X)) \to 1\,,$$

und es ist $K^*/\mathcal{O}_\mathfrak{p}^* \cong \mathbb{Z}$.

Beweis: Der erste Pfeil ist die Inklusion, und der zweite wird durch die Inklusion $\mathcal{O}(X)^* \to K^*$ und die anschließenden Projektionen $K^* \to K^*/\mathcal{O}_\mathfrak{p}^*$ induziert. Liegt $a \in \mathcal{O}(X)^*$ im Kern, so ist $a \in \mathcal{O}_\mathfrak{p}$ für $\mathfrak{p} \notin X$ und für $\mathfrak{p} \in X$ sowieso wegen $\mathcal{O}_\mathfrak{p} = \mathcal{O}(X)_{\mathfrak{p}X}$, also $a \in \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p}^* = \mathcal{O}^*$ (vgl. das Argument im Beweis zu (11.5)). Dies zeigt die Exaktheit bei $\mathcal{O}(X)^*$. Der Pfeil

$$\bigoplus_{\mathfrak{p} \notin X} K^*/\mathcal{O}_\mathfrak{p}^* \to Cl(\mathcal{O})$$

wird induziert durch die Zuordnung

$$\bigoplus_{\mathfrak{p} \notin X} \alpha_\mathfrak{p} \bmod \mathcal{O}_\mathfrak{p}^* \quad \mapsto \quad \prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}\,,$$

wobei $v_\mathfrak{p} : K^* \to \mathbb{Z}$ die zu $\mathcal{O}_\mathfrak{p}$ gehörige Exponentialbewertung von K ist. Sei $\bigoplus_{\mathfrak{p} \notin X} \alpha_\mathfrak{p} \bmod \mathcal{O}_\mathfrak{p}^*$ ein Element im Kern, d.h.

$$\prod_{\mathfrak{p} \notin X} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} = (\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(\alpha)}$$

mit einem $\alpha \in K^*$. Wegen der eindeutigen Primzerlegung bedeutet dies $v_\mathfrak{p}(\alpha) = 0$ für $\mathfrak{p} \in X$ und $v_\mathfrak{p}(\alpha_\mathfrak{p}) = v_\mathfrak{p}(\alpha)$ für $\mathfrak{p} \notin X$. Hieraus folgt $\alpha \in \bigcap_{\mathfrak{p} \in X} \mathcal{O}_\mathfrak{p}^* = \mathcal{O}(X)^*$ und $\alpha \equiv \alpha_\mathfrak{p} \bmod \mathcal{O}_\mathfrak{p}^*$. Dies zeigt die Exaktheit in der Mitte. Der Pfeil

$$Cl(\mathcal{O}) \to Cl(\mathcal{O}(X))$$

wird durch die Zuordnung $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}(X)$ induziert. Die Klassen der Primideale $\mathfrak{p} \in X$ werden auf die Klassen der Primideale von $\mathcal{O}(X)$ abgebildet. Da $Cl(\mathcal{O}(X))$ durch diese Klassen erzeugt wird, so ist der Pfeil surjektiv. Für $\mathfrak{p} \notin X$ ist $\mathfrak{p}\mathcal{O}(X) = (1)$, und dies bedeutet, daß der Kern aus den Klassen der Ideale $\prod_{\mathfrak{p} \notin X} \mathfrak{p}^{\nu_\mathfrak{p}}$ besteht. Dies aber ist offensichtlich das Bild des vorangehenden Pfeils. Daher ist die ganze Sequenz exakt. Die Bewertung $v_\mathfrak{p} : K^* \to \mathbb{Z}$ liefert schließlich den Isomorphismus $K^*/\mathcal{O}_\mathfrak{p}^* \cong \mathbb{Z}$. □

Für den Ring $\mathcal{O}_K$ der ganzen Zahlen eines algebraischen Zahlkörpers K ergeben sich aus diesem Satz die folgenden Resultate. Sei S eine endliche Menge von Primidealen von $\mathcal{O}_K$ (also nicht mehr eine multiplikative

Teilmenge) und X die Menge aller nicht in S gelegenen Primideale. Wir setzen

$$o_K^S = o_K(X)\,.$$

Die Einheiten dieses Ringes heißen die ***S*-Einheiten** und die Gruppe $Cl_K^S = Cl(o_K^S)$ die ***S*-Klassengruppe** von K.

(11.7) Korollar. *Für die Gruppe $K^S = (o_K^S)^*$ der S-Einheiten von K haben wir einen Isomorphismus*

$$K^S \cong \mu(K) \times \mathbb{Z}^{\#S+r+s-1}\,,$$

wobei r und s wie in § 5, S. 32 definiert sind.

Beweis: Die Torsionsgruppe von K^S ist die Gruppe $\mu(K)$ der Einheitswurzeln in K. Da $Cl(o)$ endlich ist, so erhalten wir aus der exakten Sequenz (11.6) und aus (7.4)

$$\mathrm{Rang}(K^S) = \mathrm{Rang}(o_K^*) + \mathrm{Rang}(\bigoplus_{\mathfrak{p}\in S} \mathbb{Z}) = \#S + r + s - 1$$

und damit das Korollar. □

(11.8) Korollar. *Die S-Klassengruppe $Cl_K^S = Cl(o_K^S)$ ist endlich.*

Aufgabe 1. Sei A ein beliebiger Ring, also nicht notwendig ein Integritätsbereich, M ein A-Modul und S eine multiplikativ abgeschlossene Teilmenge von A, $0 \notin S$. In $M \times S$ betrachte man die Äquivalenzrelation

$$(m,s) \sim (m',s') \iff \exists\, s'' \in S \quad \text{mit} \quad s''(s'm - sm') = 0\,.$$

Zeige, daß die Menge M_S der Äquivalenzklassen $\overline{(m,s)}$ einen A-Modul bildet und daß $M \to M_S$, $a \mapsto \overline{(a,1)}$, ein Homomorphismus ist. Insbesondere ist A_S ein Ring. Er heißt die **Lokalisierung** von A bzgl. S.

Aufgabe 2. Zeige, daß in der obigen Situation die Primideale von A_S umkehrbar eindeutig den Primidealen von A entsprechen, die zu S disjunkt sind. Sind $\mathfrak{p} \subseteq A$ und $\mathfrak{p}_S \subseteq A_S$ aufeinander bezogen, so ist $A_S/\mathfrak{p}_S$ die Lokalisierung von $A/\mathfrak{p}$ bzgl. des Bildes von S.

Aufgabe 3. Sei $f : M \to N$ ein Homomorphismus von A-Moduln. Dann sind die folgenden Bedingungen äquivalent.

(i) f ist injektiv (surjektiv).
(ii) $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ ist injektiv (surjektiv) für jedes Primideal $\mathfrak{p}$.
(iii) $f_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ ist injektiv (surjektiv) für jedes maximale Ideal $\mathfrak{m}$.

Aufgabe 4. Seien S und T zwei multiplikative Teilmengen von A und T^* das Bild von T in A_S. Dann ist $A_{ST} \cong (A_S)_{T^*}$.

Aufgabe 5. Sei $f : A \to B$ ein Homomorphismus von Ringen und S eine multiplikative abgeschlossene Teilmenge mit $f(S) \subseteq B^*$. Dann induziert f einen kanonischen Homomorphismus $A_S \to B$.

Aufgabe 6. Sei A ein Integritätsbereich. Ist die Lokalisierung A_S ganz über A, so ist $A_S = A$.

Aufgabe 7 (Nakayama Lemma). Sei A ein lokaler Ring mit dem maximalen Ideal $\mathfrak{m}$, M ein A-Modul und $N \subseteq M$ ein Untermodul, so daß M/N endlich erzeugt ist. Dann gilt:

$$M = N + \mathfrak{m}M \Rightarrow M = N.$$

§ 12. Ordnungen

Der Ring o_K der ganzen Zahlen eines algebraischen Zahlkörpers K steht mit seiner ausgezeichneten Eigenschaft, ein Dedekindring zu sein, im Vordergrund des Interesses. Durch wichtige theoretische sowie praktische Umstände wird man jedoch zu einer Allgemeinheit gedrängt, die darüber hinaus Ringe in die Theorie der algebraischen Zahlen einbezieht, welche, wie etwa der Ring

$$o = \mathbb{Z} + \mathbb{Z}\sqrt{5} \subseteq \mathbb{Q}(\sqrt{5}),$$

nicht notwendig ganzabgeschlossen sind. Es sind dies die wie folgt definierten **Ordnungen**.

(12.1) Definition. *Sei $K|\mathbb{Q}$ ein algebraischer Zahlkörper vom Grade n. Eine Ordnung von K ist ein Teilring o von o_K, der eine Ganzheitsbasis der Länge n besitzt. Der Ring o_K heißt die* **Hauptordnung** *von K.*

Konkret erhält man die Ordnungen als die Ringe

$$o = \mathbb{Z}[\alpha_1, \ldots, \alpha_r],$$

wobei $\alpha_1, \ldots, \alpha_r$ ganze Zahlen mit $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$ sind. Als Untermodul des freien $\mathbb{Z}$-Moduls o_K besitzt ja o eine $\mathbb{Z}$-Basis, die wegen $\mathbb{Q}o = K$ gleichzeitig eine Basis von $K|\mathbb{Q}$ sein muß , also die Länge n hat. Häufig treten die Ordnungen als Multiplikatorenringe auf und finden in dieser Eigenschaft ihre praktischen Anwendungen. Ist etwa $\alpha_1, \ldots, \alpha_n$ irgendeine Basis von $K|\mathbb{Q}$ und $M = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, so ist

$$o_M = \{\alpha \in K \mid \alpha M \subseteq M\}$$

eine Ordnung. Die theoretische Bedeutung der Ordnungen besteht aber darin, daß mit ihnen die „Singularitäten" zugelassen werden, die bei der Betrachtung der Dedekindringe mit ihren „regulären" Lokalisierungen $\mathcal{O}_\mathfrak{p}$ ausgeschlossen sind. Was hiermit gemeint ist, wird im nächsten Paragraphen erläutert.

Im vorigen Paragraphen haben wir Lokalisierungen des Dedekindringes $\mathcal{O}_K$ betrachtet. Dies sind Erweiterungsringe von $\mathcal{O}_K$, die zwar ganzabgeschlossen sind, aber nicht mehr ganz über $\mathbb{Z}$. Hier betrachten wir die Ordnungen. Dies sind Unterringe von $\mathcal{O}_K$, die zwar ganz sind über $\mathbb{Z}$, aber nicht mehr ganzabgeschlossen. Als gemeinsame Verallgemeinerung dieser beiden Ringtypen betrachten wir jetzt alle **eindimensionalen noetherschen Integritätsbereiche**. Damit sind die noetherschen Integritätsbereiche gemeint, in denen jedes Primideal $\mathfrak{p} \neq 0$ ein maximales Ideal ist. Die Bezeichnung „eindimensional" rührt von der allgemeinen Definition der **Krull-Dimension** her als der maximalen Länge d einer Primidealkette $\mathfrak{p}_0 \underset{\neq}{\subset} \mathfrak{p}_1 \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} \mathfrak{p}_d$.

(12.2) Satz. *Eine Ordnung $\mathcal{O}$ von K ist ein eindimensionaler noetherscher Integritätsbereich.*

Beweis: Da $\mathcal{O}$ ein endlich erzeugter $\mathbb{Z}$-Modul vom Rang $n = [K : \mathbb{Q}]$ ist, so ist auch jedes Ideal $\mathfrak{a}$ ein endlich erzeugter $\mathbb{Z}$-Modul, erst recht also ein endlich erzeugter $\mathcal{O}$-Modul. Daher ist $\mathcal{O}$ noethersch. Ist $\mathfrak{p} \neq 0$ ein Primideal und $a \in \mathfrak{p} \cap \mathbb{Z}$, $a \neq 0$, so ist $a\mathcal{O} \subseteq \mathfrak{p} \subseteq \mathcal{O}$, d.h. $\mathfrak{p}$ und $\mathcal{O}$ haben den gleichen Rang n. Daher ist $\mathcal{O}/\mathfrak{p}$ ein endlicher Integritätsbereich, also ein Körper, und somit $\mathfrak{p}$ ein maximales Ideal. □

Im folgenden sei $\mathcal{O}$ stets ein eindimensionaler noetherscher Integritätsbereich und K sein Quotientenkörper. Als Verschärfung des chinesischen Restsatzes beweisen wir zunächst den

(12.3) Satz. *Ist $\mathfrak{a} \neq 0$ ein Ideal von $\mathcal{O}$, so gilt*

$$\mathcal{O}/\mathfrak{a} \cong \bigoplus_{\mathfrak{p}} \mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p} = \bigoplus_{\mathfrak{p} \supseteq \mathfrak{a}} \mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p} \,.$$

Beweis: Sei $\tilde{\mathfrak{a}}_\mathfrak{p} = \mathcal{O} \cap \mathfrak{a}\mathcal{O}_\mathfrak{p}$. Für fast alle $\mathfrak{p}$ ist $\mathfrak{p} \not\supseteq \mathfrak{a}$ und damit $\mathfrak{a}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$, also $\tilde{\mathfrak{a}}_\mathfrak{p} = \mathcal{O}$. Ferner ist $\mathfrak{a} = \bigcap_\mathfrak{p} \tilde{\mathfrak{a}}_\mathfrak{p} = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \tilde{\mathfrak{a}}_\mathfrak{p}$, weil für jedes $a \in \bigcap_\mathfrak{p} \tilde{\mathfrak{a}}_\mathfrak{p}$

das Ideal $\mathfrak{b} = \{x \in \mathcal{O} \mid xa \in \mathfrak{a}\}$ wegen $s_\mathfrak{p} a \in \mathfrak{a}$ für ein $s_\mathfrak{p} \notin \mathfrak{p}$ in keinem der maximalen Ideale $\mathfrak{p}$ liegt, so daß $\mathfrak{b} = \mathcal{O}$, also $a = 1 \cdot a \in \mathfrak{a}$ ist. Aus (11.1) folgt, daß $\mathfrak{p}$ das einzige $\tilde{\mathfrak{a}}_\mathfrak{p}$ umfassende Primideal ist, falls $\mathfrak{p} \supseteq \mathfrak{a}$. Für zwei verschiedene Primideale $\mathfrak{p}$ und $\mathfrak{q}$ von $\mathcal{O}$ kann das Ideal $\tilde{\mathfrak{a}}_\mathfrak{p} + \tilde{\mathfrak{a}}_\mathfrak{q}$ daher in keinem maximalen Ideal enthalten sein, so daß $\tilde{\mathfrak{a}}_\mathfrak{p} + \tilde{\mathfrak{a}}_\mathfrak{q} = \mathcal{O}$ ist. Der chinesische Restsatz (3.6) liefert jetzt die Isomorphie

$$\mathcal{O}/\mathfrak{a} \cong \bigoplus_{\mathfrak{p} \supseteq \mathfrak{a}} \mathcal{O}/\tilde{\mathfrak{a}}_\mathfrak{p} ,$$

und es ist $\mathcal{O}/\tilde{\mathfrak{a}}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}$, da $\bar{\mathfrak{p}} = \mathfrak{p} \bmod \tilde{\mathfrak{a}}_\mathfrak{p}$ das einzige maximale Ideal von $\mathcal{O}/\tilde{\mathfrak{a}}_\mathfrak{p}$ ist. □

Für den Ring $\mathcal{O}$ bilden die gebrochenen Ideale von $\mathcal{O}$, d.h. die endlich erzeugten $\mathcal{O}$-Untermoduln $\neq 0$ des Quotientenkörpers K keine Gruppe mehr, es sei denn, $\mathcal{O}$ ist dedekindsch. Man beschränkt sich daher auf die Betrachtung der **invertierbaren Ideale**, d.h. der gebrochenen Ideale $\mathfrak{a}$ von $\mathcal{O}$, für die ein gebrochenes Ideal $\mathfrak{b}$ existiert mit

$$\mathfrak{a}\mathfrak{b} = \mathcal{O} .$$

Diese bilden trivialerweise eine abelsche Gruppe. Das Inverse zu $\mathfrak{a}$ ist stets das gebrochene Ideal

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\} ,$$

denn es ist das größte mit $\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}$. Die invertierbaren Ideale von $\mathcal{O}$ lassen sich als diejenigen gebrochenen Ideale charakterisieren, die „lokal" Hauptideale sind:

(12.4) Satz. *Ein gebrochenes Ideal $\mathfrak{a}$ von $\mathcal{O}$ ist genau dann invertierbar, wenn*

$$\mathfrak{a}_\mathfrak{p} = \mathfrak{a}\mathcal{O}_\mathfrak{p}$$

für jedes Primideal $\mathfrak{p} \neq 0$ ein gebrochenes Hauptideal von $\mathcal{O}_\mathfrak{p}$ ist.

Beweis: Sei $\mathfrak{a}$ ein invertierbares Ideal und $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Dann ist $1 = \sum_{i=1}^{r} a_i b_i$ mit $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$, und es können nicht alle $a_i b_i \in \mathcal{O}_\mathfrak{p}$ im maximalen Ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ sein, so daß etwa $a_1 b_1$ eine Einheit in $\mathcal{O}_\mathfrak{p}$ ist. Es folgt, daß $\mathfrak{a}_\mathfrak{p} = a_1\mathcal{O}_\mathfrak{p}$ ist, denn für $x \in \mathfrak{a}_\mathfrak{p}$ ist $xb_1 \in \mathfrak{a}_\mathfrak{p}\mathfrak{b} = \mathcal{O}_\mathfrak{p}$, also $x = xb_1(b_1a_1)^{-1}a_1 \in a_1\mathcal{O}_\mathfrak{p}$.

Sei umgekehrt $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}\mathcal{O}_\mathfrak{p}$ für jedes $\mathfrak{p}$ ein Hauptideal $a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$, $a_\mathfrak{p} \in K^*$. Wir dürfen $a_\mathfrak{p} \in \mathfrak{a}$ annehmen. Wir behaupten, daß das gebrochene Ideal

$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$ ein Inverses zu $\mathfrak{a}$ ist. Wäre dies nicht der Fall, so gäbe es ein maximales Ideal $\mathfrak{p}$ mit $\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{p} \subset \mathcal{O}$. Seien $a_1, \ldots, a_n$ Erzeugende von $\mathfrak{a}$. Wegen $a_i \in a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ können wir $a_i = a_\mathfrak{p}\frac{b_i}{s_i}$ mit $b_i \in \mathcal{O}$, $s_i \in \mathcal{O} \setminus \mathfrak{p}$ schreiben, so daß $s_i a_i \in a_\mathfrak{p}\mathcal{O}$. Wenn $s = s_1 \ldots s_n$ gesetzt ist, so ist $sa_i \in a_\mathfrak{p}\mathcal{O}$ für $i = 1, \ldots, n$, also $sa_\mathfrak{p}^{-1}\mathfrak{a} \subseteq \mathcal{O}$ und damit $sa_\mathfrak{p}^{-1} \in \mathfrak{a}^{-1}$. Es folgt $s = sa_\mathfrak{p}^{-1}a_\mathfrak{p} \in \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{p}$, Widerspruch. □

Wir bezeichnen die Gruppe der invertierbaren Ideale von $\mathcal{O}$ mit $J(\mathcal{O})$. Sie enthält die Gruppe $P(\mathcal{O})$ der gebrochenen Hauptideale $a\mathcal{O}$, $a \in K^*$.

(12.5) Definition. *Die Faktorgruppe*

$$Pic(\mathcal{O}) = J(\mathcal{O})/P(\mathcal{O})$$

heißt die **Picardgruppe** *des Ringes* $\mathcal{O}$.

Im Falle, daß $\mathcal{O}$ ein Dedekindring ist, ist die Picardgruppe natürlich mit der Idealklassengruppe Cl_K identisch. Im allgemeinen erhalten wir für $J(\mathcal{O})$ und $Pic(\mathcal{O})$ die folgende Beschreibung.

(12.6) Satz. *Die Zuordnung* $\mathfrak{a} \mapsto (\mathfrak{a}_\mathfrak{p}) = (\mathfrak{a}\mathcal{O}_\mathfrak{p})$ *liefert einen Isomorphismus*

$$J(\mathcal{O}) \cong \bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p}).$$

Identifiziert man die Untergruppe $P(\mathcal{O})$ *mit ihrem Bild in der direkten Summe, so wird*

$$Pic(\mathcal{O}) \cong (\bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p}))/P(\mathcal{O}).$$

Beweis: Für jedes $\mathfrak{a} \in J(\mathcal{O})$ ist $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}\mathcal{O}_\mathfrak{p}$ nach (12.4) ein Hauptideal, und es ist $\mathfrak{a}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ für fast alle $\mathfrak{p}$, denn $\mathfrak{a}$ liegt nur in endlich vielen maximalen Idealen $\mathfrak{p}$. Wir erhalten daher einen Homomorphismus

$$J(\mathcal{O}) \to \bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p}), \quad \mathfrak{a} \mapsto (\mathfrak{a}_\mathfrak{p}).$$

Dieser ist injektiv, denn wenn $\mathfrak{a}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ für alle $\mathfrak{p}$ ist, so ist $\mathfrak{a} \subseteq \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p} = \mathcal{O}$ (vgl. den Beweis zu (11.5)), und es muß $\mathfrak{a} = \mathcal{O}$ gelten, weil sonst ein maximales Ideal $\mathfrak{p}$ mit $\mathfrak{a} \subseteq \mathfrak{p} \subset \mathcal{O}$ existierte, so daß $\mathfrak{a}_\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_\mathfrak{p} \neq \mathcal{O}_\mathfrak{p}$.

Zum Beweis der Surjektivität sei $(a_\mathfrak{p}\mathcal{O}_\mathfrak{p}) \in \bigoplus_\mathfrak{p} P(\mathcal{O}_\mathfrak{p})$ gegeben. Dann ist der $\mathcal{O}$-Untermodul

$$\mathfrak{a} = \bigcap_\mathfrak{p} a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$$

von K ein gebrochenes Ideal, denn wegen $a_\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ für fast alle $\mathfrak{p}$ gibt es ein $c \in \mathcal{O}$ mit $ca_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$ für alle $\mathfrak{p}$, d.h. $c\mathfrak{a} \subseteq \bigcap_\mathfrak{p} \mathcal{O}_\mathfrak{p} = \mathcal{O}$. Wir haben zu zeigen, daß

$$\mathfrak{a}\mathcal{O}_\mathfrak{p} = a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$$

für jedes $\mathfrak{p}$ gilt. Die Inklusion $\subseteq$ ist trivial. Zum Beweis von $a_\mathfrak{p}\mathcal{O}_\mathfrak{p} \subseteq \mathfrak{a}\mathcal{O}_\mathfrak{p}$ wählen wir ein $c \in \mathcal{O}$, $c \neq 0$, so daß $ca_\mathfrak{p}^{-1}a_\mathfrak{q} \in \mathcal{O}$ für die endlich vielen $\mathfrak{q}$, für die $a_\mathfrak{p}^{-1}a_\mathfrak{q} \notin \mathcal{O}_\mathfrak{q}$. Nach dem chinesischen Restsatz (12.3) finden wir ein $a \in \mathcal{O}$ mit

$$a \equiv c \bmod \mathfrak{p} \quad \text{und} \quad a \in ca_\mathfrak{p}^{-1}a_\mathfrak{q}\mathcal{O}_\mathfrak{q} \quad \text{für} \quad \mathfrak{q} \neq \mathfrak{p}\,.$$

Dann ist $\varepsilon = ac^{-1}$ eine Einheit in $\mathcal{O}_\mathfrak{p}$ und $a_\mathfrak{p}\varepsilon \in \bigcap_\mathfrak{q} a_\mathfrak{q}\mathcal{O}_\mathfrak{q} = \mathfrak{a}$, also

$$a_\mathfrak{p}\mathcal{O}_\mathfrak{p} = (a_\mathfrak{p}\varepsilon)\mathcal{O}_\mathfrak{p} \subseteq \mathfrak{a}\mathcal{O}_\mathfrak{p}\,. \qquad \square$$

Geht man vom Ring $\mathcal{O}$ zu seiner **Normalisierung** $\tilde{\mathcal{O}}$ über, d.h. zum ganzen Abschluß von $\mathcal{O}$ in K, so erhält man einen Dedekindring. Dies ist jedoch nicht ganz einfach zu beweisen, weil $\tilde{\mathcal{O}}$ i.a. kein endlich erzeugter $\mathcal{O}$-Modul ist. Wir haben jedoch immer das

(12.7) Lemma. *Sei $\mathcal{O}$ ein eindimensionaler noetherscher Integritätsbereich und $\tilde{\mathcal{O}}$ seine Normalisierung. Dann ist $\tilde{\mathcal{O}}/\mathfrak{a}\tilde{\mathcal{O}}$ für jedes Ideal $\mathfrak{a} \neq 0$ von $\mathcal{O}$ ein endlich erzeugter $\mathcal{O}$-Modul.*

Beweis: Sei $a \in \mathfrak{a}$, $a \neq 0$. Dann ist $\tilde{\mathcal{O}}/\mathfrak{a}\tilde{\mathcal{O}}$ ein Quotient von $\tilde{\mathcal{O}}/a\tilde{\mathcal{O}}$, d.h. es genügt zu zeigen, daß $\tilde{\mathcal{O}}/a\tilde{\mathcal{O}}$ ein endlich erzeugter $\mathcal{O}$-Modul ist. Wir betrachten dazu in $\mathcal{O}$ die absteigende Kette der $a\mathcal{O}$ enthaltenden Ideale

$$\mathfrak{a}_m = (a^m\tilde{\mathcal{O}} \cap \mathcal{O}, a\mathcal{O})\,.$$

Diese Kette wird stationär. In der Tat, die Primideale des Ringes $\mathcal{O}/a\mathcal{O}$ sind nicht nur maximal, sondern auch minimal, d.h. $\mathcal{O}/a\mathcal{O}$ ist ein 0-dimensionaler noetherscher Ring. In einem solchen Ring wird jede absteigende Idealkette stationär (vgl. § 3, Aufgabe 7). Wird nun die Kette $\bar{\mathfrak{a}}_m = \mathfrak{a}_m \bmod a\mathcal{O}$ stationär bei n, so gilt das gleiche für die Kette $\mathfrak{a}_m$. Wir zeigen, daß für dieses n

$$\tilde{\mathcal{O}} \subseteq a^{-n}\mathcal{O} + a\tilde{\mathcal{O}}$$

gilt. Zum Beweis sei $\beta = \frac{b}{c} \in \tilde{o}$, $b, c \in o$. Wenden wir die absteigende Kettenbedingung auf den Ring o/co und die Idealkette $(\bar{a}^m)$ mit $\bar{a} = a \bmod co$ an, so wird $(\bar{a}^h) = (\bar{a}^{h+1})$, d.h. wir finden ein $x \in o$ mit $a^h \equiv xa^{h+1} \bmod co$, also $(1 - xa)a^h \in co$, und daher

$$\beta = \frac{b}{c}(1 - xa) + \beta xa = \frac{b}{a^h}\frac{(1 - xa)a^h}{c} + \beta xa \in a^{-h}o + a\tilde{o}\,.$$

Sei h die kleinstmögliche Zahl mit $\beta \in a^{-h}o + a\tilde{o}$. Es genügt dann zu zeigen, daß $h \leq n$. Angenommen $h > n$. Schreiben wir

$$(*) \qquad \beta = \frac{u}{a^h} + a\tilde{u} \quad \text{mit } u \in o,\ \tilde{u} \in \tilde{o}\,,$$

so ist $u = a^h(\beta - a\tilde{u}) \in a^h\tilde{o} \cap o \subseteq \mathfrak{a}_h = \mathfrak{a}_{h+1}$ wegen $h > n$, also $u = a^{h+1}\tilde{u}' + au'$, $u' \in o$, $\tilde{u}' \in \tilde{o}$. Dies in $(*)$ eingesetzt ergibt

$$\beta = \frac{u'}{a^{h-1}} + a(\tilde{u} + \tilde{u}') \in a^{1-h}o + a\tilde{o}\,.$$

Dies aber widerspricht der Minimalität von h. Es gilt somit in der Tat $\tilde{o} \subseteq a^{-n}o + a\tilde{o}$.

$\tilde{o}/a\tilde{o}$ wird hiermit ein Untermodul des durch $a^{-n} \bmod a\tilde{o}$ erzeugten o-Moduls $(a^{-n}o + a\tilde{o})/a\tilde{o}$ und ist daher selbst ein endlich erzeugter o-Modul, q.e.d. □

(12.8) Satz *(KRULL-AKIZUKI). Sei o ein eindimensionaler noetherscher Integritätsbereich mit dem Quotientenkörper K, $L|K$ eine endliche Erweiterung und $\mathcal{O}$ der ganze Abschluß von o in L. Dann ist $\mathcal{O}$ ein Dedekindring.*

Beweis: Man schließt wie bei (3.1), daß $\mathcal{O}$ ganzabgeschlossen ist und daß jedes Primideal $\neq 0$ maximal ist. Bleibt zu zeigen, daß $\mathcal{O}$ noethersch ist. Sei $\omega_1, \ldots, \omega_n$ eine in $\mathcal{O}$ gelegene Basis von $L|K$. Dann ist der Ring $\mathcal{O}_0 = o[\omega_1, \ldots, \omega_n]$ ein endlich erzeugter o-Modul und daher noethersch, weil o noethersch ist. Wir schließen wie zuvor, daß $\mathcal{O}_0$ eindimensional ist, und sind damit auf den Fall $L = K$ zurückgeführt. Ist nun $\mathfrak{A}$ ein Ideal von $\mathcal{O}$ und $a \in \mathfrak{A} \cap o$, $a \neq 0$, so ist $\mathcal{O}/a\mathcal{O}$ nach dem obigen Lemma ein endlich erzeugter o-Modul. Da o noethersch ist, ist damit auch der o-Untermodul $\mathfrak{A}/a\mathcal{O}$ endlich erzeugt, also der $\mathcal{O}$-Modul $\mathfrak{A}$ ebenfalls. □

Bemerkung: Der obige Beweis ist dem Buch [82] von KAPLANSKY entnommen (s. aber auch [101]). Er zeigt zugleich die allgemeine Gültig-

keit des Satzes (8.1) über die Erweiterungen eines Dedekindringes, den wir nur für den Fall einer separablen Erweiterung $L|K$ bewiesen hatten.

Wir wollen im folgenden den eindimensionalen noetherschen Integritätsbereich o mit seiner Normalisierung $\tilde{o}$ vergleichen. Die Tatsache, daß $\tilde{o}$ ein Dedekindring ist, ist evident und bedarf nicht des langen Beweises von (12.8), wenn wir die folgende Voraussetzung machen:

(*) o ist ein Integritätsbereich, dessen Normalisierung $\tilde{o}$ ein endlich erzeugter o-Modul ist.

Diese Bedingung soll für alles weitere gelten. Sie schließt pathologische Situationen aus und ist in allen interessierenden Fällen erfüllt, insbesondere für die Ordnungen in einem algebraischen Zahlkörper.

Die Einheitengruppen und die Picardgruppen von o und $\tilde{o}$ werden durch den folgenden Satz miteinander verglichen.

(12.9) Satz. *Man hat eine kanonische exakte Sequenz*

$$1 \to o^* \to \tilde{o}^* \to \bigoplus_{\mathfrak{p}} \tilde{o}_{\mathfrak{p}}^*/o_{\mathfrak{p}}^* \to Pic(o) \to Pic(\tilde{o}) \to 1\,.$$

In der Summe durchläuft $\mathfrak{p}$ *die Primideale* $\neq 0$ *von* o, *und es bedeutet* $\tilde{o}_{\mathfrak{p}}$ *den ganzen Abschluß von* $o_{\mathfrak{p}}$ *in* K.

Beweis: Durchläuft $\tilde{\mathfrak{p}}$ die Primideale von $\tilde{o}$, so ist nach (12.6)

$$J(\tilde{o}) \cong \bigoplus_{\tilde{\mathfrak{p}}} P(\tilde{o}_{\tilde{\mathfrak{p}}})\,.$$

Ist $\mathfrak{p}$ ein Primideal von o, so zerfällt $\mathfrak{p}\tilde{o}$ im Dedekindring $\tilde{o}$ in ein Produkt

$$\mathfrak{p}\tilde{o} = \tilde{\mathfrak{p}}_1^{e_1} \dots \tilde{\mathfrak{p}}_r^{e_r},$$

d.h. es gibt nur endlich viele Primideale von $\tilde{o}$ über $\mathfrak{p}$. Das gleiche trifft für den ganzen Abschluß $\tilde{o}_{\mathfrak{p}}$ von $o_{\mathfrak{p}}$ zu. Da jedes von Null verschiedene Primideal von $\tilde{o}_{\mathfrak{p}}$ über $\mathfrak{p}o_{\mathfrak{p}}$ liegen muß , so besitzt $\tilde{o}_{\mathfrak{p}}$ nur endlich viele Primideale und ist damit ein Hauptidealring (vgl. § 3, Aufgabe 4). Wegen (12.6) folgt somit

$$P(\tilde{o}_{\mathfrak{p}}) = J(\tilde{o}_{\mathfrak{p}}) \cong \bigoplus_{\tilde{\mathfrak{p}} \supseteq \mathfrak{p}} P(\tilde{o}_{\tilde{\mathfrak{p}}})$$

und daher

$$J(\tilde{o}) \cong \bigoplus_{\mathfrak{p}} \bigoplus_{\tilde{\mathfrak{p}} \supseteq \mathfrak{p}} P(\tilde{o}_{\tilde{\mathfrak{p}}}) \cong \bigoplus_{\mathfrak{p}} P(\tilde{o}_{\mathfrak{p}})\,.$$

Beachten wir, daß $P(R) \cong K^*/R^*$ für jeden Integritätsbereich R mit dem Quotientenkörper K , so erhalten wir das kommutative exakte Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^*/\mathfrak{o}^* & \longrightarrow & \bigoplus_{\mathfrak{p}} K^*/\mathfrak{o}_{\mathfrak{p}}^* & \longrightarrow & Pic(\mathfrak{o}) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & K^*/\tilde{\mathfrak{o}}^* & \longrightarrow & \bigoplus_{\mathfrak{p}} K^*/\tilde{\mathfrak{o}}_{\mathfrak{p}}^* & \longrightarrow & Pic(\tilde{\mathfrak{o}}) & \longrightarrow & 1. \end{array}$$

Für ein solches Diagramm hat man ganz allgemein das bekannte **Schlangenlemma**, d.h. man hat in kanonischer Weise eine exakte Sequenz

$$\begin{aligned} 1 \to \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\beta) \to \mathrm{Ker}(\gamma) \xrightarrow{\delta} \\ \mathrm{Coker}(\alpha) \to \mathrm{Coker}(\beta) \to \mathrm{Coker}(\gamma) \to 1 \end{aligned}$$

zwischen den Kernen und Kokernen von α, β, γ (vgl. [23], Ch. III, § 3, Lemma 3.3). In unserem besonderen Fall sind α und β und damit auch γ surjektiv, während

$$\mathrm{Ker}(\alpha) = \tilde{\mathfrak{o}}^*/\mathfrak{o}^* \quad \text{und} \quad \mathrm{Ker}(\beta) = \bigoplus_{\mathfrak{p}} \tilde{\mathfrak{o}}_{\mathfrak{p}}^*/\mathfrak{o}_{\mathfrak{p}}^* .$$

Damit aber ergibt sich die exakte Sequenz

$$1 \to \mathfrak{o}^* \to \tilde{\mathfrak{o}}^* \to \bigoplus_{\mathfrak{p}} \tilde{\mathfrak{o}}_{\mathfrak{p}}^*/\mathfrak{o}_{\mathfrak{p}}^* \to Pic(\mathfrak{o}) \to Pic(\tilde{\mathfrak{o}}) \to 1 . \qquad \square$$

Ein Primideal $\mathfrak{p} \neq 0$ von $\mathfrak{o}$ heißt **regulär**, wenn $\mathfrak{o}_{\mathfrak{p}}$ ganzabgeschlossen, also ein diskreter Bewertungsring ist. Für die regulären Primideale sind die Summanden $\tilde{\mathfrak{o}}_{\mathfrak{p}}^*/\mathfrak{o}_{\mathfrak{p}}^*$ in (12.9) trivial. Es gibt nur endlich viele nicht-reguläre Primideale von $\mathfrak{o}$, nämlich die Teiler des **Führers** von $\mathfrak{o}$. Er ist als das größte in $\mathfrak{o}$ enthaltene Ideal von $\tilde{\mathfrak{o}}$ definiert, also durch

$$\mathfrak{f} = \{a \in \tilde{\mathfrak{o}} \mid a\tilde{\mathfrak{o}} \subseteq \mathfrak{o}\} .$$

Da $\tilde{\mathfrak{o}}$ ein endlich erzeugter $\mathfrak{o}$-Modul ist, ist $\mathfrak{f} \neq 0$.

(12.10) Satz. *Für ein Primideal $\mathfrak{p} \neq 0$ von $\mathfrak{o}$ gilt:*

$$\mathfrak{p} \nmid \mathfrak{f} \iff \mathfrak{p} \quad \textit{ist regulär.}$$

In diesem Fall ist $\tilde{\mathfrak{p}} = \mathfrak{p}\tilde{\mathfrak{o}}$ ein Primideal von $\tilde{\mathfrak{o}}$ und $\mathfrak{o}_{\mathfrak{p}} = \tilde{\mathfrak{o}}_{\tilde{\mathfrak{p}}}$.

Beweis: Sei $\mathfrak{p} \nmid \mathfrak{f}$ vorausgesetzt, d.h. $\mathfrak{p} \not\supseteq \mathfrak{f}$, und sei $t \in \mathfrak{f} \setminus \mathfrak{p}$. Dann ist $t\tilde{\mathcal{O}} \subseteq \mathcal{O}$, also $\tilde{\mathcal{O}} \subseteq \frac{1}{t}\mathcal{O} \subseteq \mathcal{O}_\mathfrak{p}$. Ist $\mathfrak{m} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ das maximale Ideal von $\mathcal{O}_\mathfrak{p}$ und setzen wir $\tilde{\mathfrak{p}} = \mathfrak{m} \cap \tilde{\mathcal{O}}$, so ist $\tilde{\mathfrak{p}}$ ein Primideal von $\tilde{\mathcal{O}}$ mit $\mathfrak{p} \subseteq \tilde{\mathfrak{p}} \cap \mathcal{O}$, also $\mathfrak{p} = \tilde{\mathfrak{p}} \cap \mathcal{O}$ wegen der Maximalität von $\mathfrak{p}$. Trivialerweise ist $\mathcal{O}_\mathfrak{p} \subseteq \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$, und wenn umgekehrt $\frac{a}{s} \in \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$, $a \in \tilde{\mathcal{O}}$, $s \in \tilde{\mathcal{O}} \setminus \tilde{\mathfrak{p}}$, so ist $ta \in \mathcal{O}$ und $ts \in \mathcal{O} \setminus \mathfrak{p}$, also $\frac{a}{s} = \frac{ta}{ts} \in \mathcal{O}_\mathfrak{p}$. Daher gilt $\mathcal{O}_\mathfrak{p} = \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$. Nach (11.5) ist $\mathcal{O}_\mathfrak{p}$ damit ein Bewertungsring, d.h. $\mathfrak{p}$ ist regulär.

Überdies gilt $\tilde{\mathfrak{p}} = \mathfrak{p}\tilde{\mathcal{O}}$. In der Tat, $\tilde{\mathfrak{p}}$ ist das einzige Primideal von $\tilde{\mathcal{O}}$ über $\mathfrak{p}$, denn ist $\tilde{\mathfrak{q}}$ ein weiteres, so ist $\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}} = \mathcal{O}_\mathfrak{p} \subseteq \tilde{\mathcal{O}}_{\tilde{\mathfrak{q}}}$, und damit

$$\tilde{\mathfrak{p}} = \tilde{\mathcal{O}} \cap \tilde{\mathfrak{p}}\mathcal{O}_{\tilde{\mathfrak{p}}} \subseteq \tilde{\mathcal{O}} \cap \tilde{\mathfrak{q}}\mathcal{O}_{\tilde{\mathfrak{q}}} = \tilde{\mathfrak{q}} ,$$

also $\tilde{\mathfrak{p}} = \tilde{\mathfrak{q}}$. Es folgt, daß $\mathfrak{p}\tilde{\mathcal{O}} = \tilde{\mathfrak{p}}^e$, $e \geq 1$, und weiter $\mathfrak{m} = \mathfrak{p}\mathcal{O}_\mathfrak{p} = (\mathfrak{p}\tilde{\mathcal{O}})\mathcal{O}_\mathfrak{p} = \tilde{\mathfrak{p}}^e\mathcal{O}_\mathfrak{p} = \mathfrak{m}^e$, d.h. $e = 1$ und daher $\tilde{\mathfrak{p}} = \mathfrak{p}\tilde{\mathcal{O}}$.

Sei umgekehrt $\mathcal{O}_\mathfrak{p}$ ein diskreter Bewertungsring. Als Hauptidealring ist er ganzabgeschlossen, und da $\tilde{\mathcal{O}}$ über $\mathcal{O}$ ganz ist, erst recht also über $\mathcal{O}_\mathfrak{p}$, so ist $\tilde{\mathcal{O}} \subseteq \mathcal{O}_\mathfrak{p}$. Sei $x_1, \ldots, x_n$ ein Erzeugendensystem des $\mathcal{O}$-Moduls $\tilde{\mathcal{O}}$. Wir können dann schreiben $x_i = \frac{a_i}{s_i}$, $a_i \in \mathcal{O}$, $s_i \in \mathcal{O} \setminus \mathfrak{p}$. Setzen wir $s = s_1 \ldots s_n \in \mathcal{O} \setminus \mathfrak{p}$, so gilt $sx_1, \ldots, sx_n \in \mathcal{O}$ und damit $s\tilde{\mathcal{O}} \subseteq \mathcal{O}$, d.h. $s \in \mathfrak{f} \setminus \mathfrak{p}$. Daher gilt $\mathfrak{p} \nmid \mathfrak{f}$. □

Für die Summe $\bigoplus_\mathfrak{p} \tilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^*$ in (12.9) erhalten wir jetzt die folgende einfache Beschreibung.

(12.11) Satz. $\bigoplus_\mathfrak{p} \tilde{\mathcal{O}}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^* \cong (\tilde{\mathcal{O}}/\mathfrak{f})^*/(\mathcal{O}/\mathfrak{f})^*$.

Beweis: Wir wenden mehrmals den chinesischen Restsatz (12.3) an. Danach ist

$$\mathcal{O}/\mathfrak{f} \cong \bigoplus_\mathfrak{p} \mathcal{O}_\mathfrak{p}/\mathfrak{f}\mathcal{O}_\mathfrak{p} . \tag{1}$$

Der ganze Abschluß $\tilde{\mathcal{O}}_\mathfrak{p}$ von $\mathcal{O}_\mathfrak{p}$ hat nur die endlich vielen über $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ gelegenen Primideale. Sie haben die Lokalisierungen $\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$, wobei $\tilde{\mathfrak{p}}$ die über $\mathfrak{p}$ gelegenen Primideale von $\tilde{\mathcal{O}}$ durchläuft. $\tilde{\mathcal{O}}_\mathfrak{p}$ ist gleichzeitig die Lokalisierung von $\tilde{\mathcal{O}}$ nach der multiplikativen Teilmenge $\tilde{\mathcal{O}} \setminus \tilde{\mathfrak{p}}$. Da $\mathfrak{f}$ ein Ideal von $\tilde{\mathcal{O}}$ ist, so folgt $\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p} = \mathfrak{f}\mathcal{O}_\mathfrak{p}$. Der chinesische Restsatz liefert

$$\tilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p} \cong \bigoplus_{\tilde{\mathfrak{p}} \supseteq \mathfrak{p}} \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}/\mathfrak{f}\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}$$

und

$$\tilde{\mathcal{O}}/\mathfrak{f} \cong \bigoplus_\mathfrak{p} \bigoplus_{\tilde{\mathfrak{p}} \supseteq \mathfrak{p}} \tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}}/\mathfrak{f}\tilde{\mathcal{O}}_{\tilde{\mathfrak{p}}} \cong \bigoplus_\mathfrak{p} \tilde{\mathcal{O}}_\mathfrak{p}/\mathfrak{f}\tilde{\mathcal{O}}_\mathfrak{p}. \tag{2}$$

Gehen wir zu den Einheitengruppen über, so erhalten wir aus (1) und (2)

$$(3) \qquad (\tilde{o}/\mathfrak{f})^*/(o/\mathfrak{f})^* \cong \bigoplus_{\mathfrak{p}} (\tilde{o}_\mathfrak{p}/\mathfrak{f}\tilde{o}_\mathfrak{p})^*/(o_\mathfrak{p}/\mathfrak{f}o_\mathfrak{p})^* .$$

Für $\mathfrak{f} \subseteq \mathfrak{p}$ betrachten wir jetzt den Homomorphismus

$$\varphi : \tilde{o}_\mathfrak{p}^* \to (\tilde{o}_\mathfrak{p}/\mathfrak{f}\tilde{o}_\mathfrak{p})^*/(o_\mathfrak{p}/\mathfrak{f}o_\mathfrak{p})^* .$$

Er ist surjektiv. In der Tat, ist $\varepsilon \bmod \mathfrak{f}\tilde{o}_\mathfrak{p}$ eine Einheit in $\tilde{o}_\mathfrak{p}/\mathfrak{f}\tilde{o}_\mathfrak{p}$, so ist ε eine Einheit in $\tilde{o}_\mathfrak{p}$. Dies liegt daran, daß die Einheiten in einem Ring gerade diejenigen Elemente sind, die in keinem maximalen Ideal enthalten sind, und daß die Urbilder der maximalen Ideale von $\tilde{o}_\mathfrak{p}/\mathfrak{f}\tilde{o}_\mathfrak{p}$ wegen $\mathfrak{f}\tilde{o}_\mathfrak{p} \subseteq \mathfrak{p}\tilde{o}_\mathfrak{p}$ gerade alle maximalen Ideale von $\tilde{o}_\mathfrak{p}$ ergeben. Der Kern von φ ist eine in $o_\mathfrak{p}$ enthaltene Untergruppe von $\tilde{o}_\mathfrak{p}^*$, die $o_\mathfrak{p}^*$ enthält, also mit $o_\mathfrak{p}^*$ identisch ist. Damit ergibt sich

$$\tilde{o}_\mathfrak{p}^*/o_\mathfrak{p}^* \cong (\tilde{o}_\mathfrak{p}/\mathfrak{f}\tilde{o}_\mathfrak{p})^*/(o_\mathfrak{p}/\mathfrak{f}o_\mathfrak{p})^* .$$

Dies bleibt auch für $\mathfrak{p} \not\supseteq \mathfrak{f}$ richtig, denn dann sind wegen (12.10) beide Seiten gleich 1. Zusammen mit (3) erhalten wir nun die Behauptung des Satzes. □

Auf das Studium der eindimensionalen noetherschen Integritätsbereiche sind wir durch die *Ordnungen* geführt worden. Für sie ergibt sich aus (12.9) und (12.11) als Verallgemeinerung des Dirichletschen Einheitensatzes und des Satzes von der Endlichkeit der Klassenzahl das

(12.12) Theorem. *Sei o eine Ordnung in einem algebraischen Zahlkörper K, o_K die Hauptordnung und $\mathfrak{f}$ der Führer von o.*

Dann sind die Gruppen o_K^*/o^* und $Pic(o)$ endlich, und es gilt

$$\#Pic(o) = \frac{h_K}{(o_K^* : o^*)} \frac{\#(o_K/\mathfrak{f})^*}{\#(o/\mathfrak{f})^*} ,$$

wobei h_K die Klassenzahl von K ist. Insbesondere ist

$$\mathrm{Rang}(o^*) = \mathrm{Rang}(o_K^*) = r + s - 1 .$$

Beweis: Nach (12.9) und (12.11) haben wir wegen $Pic(o_K) = Cl_K$ die exakte Sequenz

$$1 \to o_K^*/o^* \to (o_K/\mathfrak{f})^*/(o/\mathfrak{f})^* \to Pic(o) \to Cl_K \to 1 .$$

Hieraus folgt die Behauptung. □

Die Definition der Picardgruppe eines eindimensionalen noetherschen Integritätsbereiches o umgeht die Nicht-Eindeutigkeit der Primidealzerlegung, indem sie sich auf die Betrachtung der invertierbaren Ideale beschränkt und die Information, die in den nicht-invertierbaren liegt, beiseite schiebt. Es gibt eine andere wichtige Verallgemeinerung der Idealklassengruppe, die *alle* Primideale von o einbezieht und auf einer künstlichen Wiederherstellung der Zerlegungseindeutigkeit beruht. Diese heißt die **Divisorenklassengruppe** oder auch **Chowgruppe** von o. Ihre Definition geht aus von der freien abelschen Gruppe

$$Div(o) = \bigoplus_{\mathfrak{p}} \mathbb{Z}\mathfrak{p}$$

über der Menge aller maximalen Ideale $\mathfrak{p}$ von o (d.h. aller Primideale $\neq 0$). Dies ist die **Divisorengruppe** von o. Ihre Elemente sind die formalen Summen

$$D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p}$$

mit $n_{\mathfrak{p}} \in \mathbb{Z}$ und $n_{\mathfrak{p}} = 0$ für fast alle $\mathfrak{p}$ und werden die **Divisoren** (oder **0-Zykeln**) genannt. Es ist die Aussage des Korollars (3.9), daß die Divisorengruppe $Div(o)$ im Falle eines Dedekindringes mit der Idealgruppe kanonisch isomorph ist. Die additive Schreibweise und ihr Name rühren aus der Funktionentheorie her, wo die Divisoren für die analytischen Funktionen die gleiche Rolle spielen, wie die Ideale für die algebraischen Zahlen (vgl. III, § 3).

Um nun die Divisorenklassengruppe zu bilden, müssen wir jedem $f \in K^*$ einen „Hauptdivisor" $\operatorname{div}(f)$ zuordnen. Wir lassen uns für diese Definition vom Fall eines Dedekindringes leiten. Dort war das Hauptideal (f) durch

$$(f) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(f)}$$

gegeben, wobei $v_{\mathfrak{p}} : K^* \to \mathbb{Z}$ die $\mathfrak{p}$-adische Exponentialbewertung war, die zum Bewertungsring $o_{\mathfrak{p}}$ gehört. Im allgemeinen ist $o_{\mathfrak{p}}$ kein diskreter Bewertungsring mehr. Dennoch definiert $o_{\mathfrak{p}}$ einen Homomorphismus

$$\operatorname{ord}_{\mathfrak{p}} : K^* \to \mathbb{Z},$$

der eine Verallgemeinerung der Bewertungsfunktion darstellt. Ist $f = a/b \in K^*$, $a, b \in o$, so setzen wir

$$\operatorname{ord}_{\mathfrak{p}}(f) = l_{o_{\mathfrak{p}}}(o_{\mathfrak{p}}/ao_{\mathfrak{p}}) - l_{o_{\mathfrak{p}}}(o_{\mathfrak{p}}/bo_{\mathfrak{p}}),$$

wobei $l_{o_{\mathfrak{p}}}(M)$ die **Länge** eines $o_{\mathfrak{p}}$-Moduls M bezeichnet, also die maximale Länge einer echt absteigenden Kette

$$M = M_0 \underset{\neq}{\supset} M_1 \underset{\neq}{\supset} \dots \underset{\neq}{\supset} M_l = 0$$

von $\mathcal{O}_\mathfrak{p}$-Untermoduln. Ist speziell $\mathcal{O}_\mathfrak{p}$ ein diskreter Bewertungsring mit dem maximalen Ideal $\mathfrak{m}$, so ist der Wert $\nu = v_\mathfrak{p}(a)$ von $a \in \mathcal{O}_\mathfrak{p}$, $a \neq 0$, durch die Gleichung

$$a\mathcal{O}_\mathfrak{p} = \mathfrak{m}^\nu$$

bestimmt. Er ist gleich der Länge des $\mathcal{O}_\mathfrak{p}$-Moduls $\mathcal{O}_\mathfrak{p}/\mathfrak{m}^\nu$, denn die längste Untermodulkette ist

$$\mathcal{O}_\mathfrak{p}/\mathfrak{m}^\nu \supset \mathfrak{m}/\mathfrak{m}^\nu \supset \cdots \supset \mathfrak{m}^\nu/\mathfrak{m}^\nu = (0)\,.$$

In diesem Fall stimmt also die Ordnungsfunktion $\mathrm{ord}_\mathfrak{p}$ mit der Exponentialbewertung $v_\mathfrak{p}$ überein.

Die Homomorphie-Eigenschaft der Funktion $\mathrm{ord}_\mathfrak{p}$ entnimmt man aus der einfach zu beweisenden Tatsache, daß sich die Längenfunktion $l_{\mathcal{O}_\mathfrak{p}}$ multiplikativ auf kurzen exakten Sequenzen von $\mathcal{O}_\mathfrak{p}$-Moduln verhält.

Mit den Funktionen $\mathrm{ord}_\mathfrak{p} : K^* \to \mathbb{Z}$ können wir jetzt jedem Element $f \in K^*$ den Divisor

$$\mathrm{div}(f) = \sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(f)\mathfrak{p}$$

zuordnen und erhalten auf diese Weise einen kanonischen Homomorphismus

$$\mathrm{div} : K^* \to \mathit{Div}(\mathcal{O})\,.$$

Die Elemente $\mathrm{div}(f)$ heißen **Hauptdivisoren**. Sie bilden eine Untergruppe $\mathcal{P}(\mathcal{O})$ von $\mathit{Div}(\mathcal{O})$. Zwei Divisoren D und D', die sich nur um einen Hauptdivisor unterscheiden, heißen **rational äquivalent**.

(12.13) Definition. *Die Faktorgruppe*

$$CH^1(\mathcal{O}) = \mathit{Div}(\mathcal{O})/\mathcal{P}(\mathcal{O})$$

heißt die **Divisorenklassengruppe** *oder* **Chowgruppe** *von* $\mathcal{O}$.

Mit der Picardgruppe steht die Chowgruppe durch einen kanonischen Homomorphismus

$$\mathrm{div} : \mathit{Pic}(\mathcal{O}) \to CH^1(\mathcal{O})$$

in Verbindung, der wie folgt definiert ist. Ist $\mathfrak{a}$ ein invertierbares Ideal, so ist $\mathfrak{a}\mathcal{O}_\mathfrak{p}$ für jedes Primideal $\mathfrak{p} \neq 0$ nach (12.4) ein Hauptideal $a_\mathfrak{p}\mathcal{O}_\mathfrak{p}$, $a_\mathfrak{p} \in K^*$, und wir setzen

$$\mathrm{div}(\mathfrak{a}) = \sum_\mathfrak{p} -\mathrm{ord}_\mathfrak{p}(a_\mathfrak{p})\mathfrak{p}\,.$$

Wir erhalten hierdurch einen Homomorphismus

$$\mathrm{div} : J(\mathcal{O}) \to \mathit{Div}(\mathcal{O})$$

der Idealgruppe $J(\mathcal{O})$, welcher Hauptideale in Hauptdivisoren überführt und daher einen Homomorphismus

$$\mathrm{div} : Pic(\mathcal{O}) \to CH^1(\mathcal{O})$$

induziert. Für einen Dedekindring erhalten wir insbesondere:

(12.14) Satz. *Ist $\mathcal{O}$ ein Dedekindring, so ist*

$$\mathrm{div} : Pic(\mathcal{O}) \to CH^1(\mathcal{O})$$

ein Isomorphismus.

Aufgabe 1. Zeige, daß

$$\mathbb{C}[X,Y]/(XY-X),\ \mathbb{C}[X,Y]/(XY-1),$$
$$\mathbb{C}[X,Y]/(X^2-Y^3),\ \mathbb{C}[X,Y]/(Y^2-X^2-X^3)$$

eindimensionale noethersche Ringe sind. Welche von ihnen sind Integritätsbereiche? Bestimme deren Normalisierung.

Hinweis: Setze etwa im letzten Beispiel $t = X/Y$ und zeige, daß der Homomorphismus $\mathbb{C}[X,Y] \to \mathbb{C}[t]$, $t \mapsto t^2-1$, $Y \mapsto t(t^2-1)$, den Kern $(Y^2-X^2-X^3)$ besitzt.

Aufgabe 2. Seien a und b natürliche Zahlen, die keine Quadrate sind. Man zeige, daß die Grundeinheit der Ordnung $\mathbb{Z}+\mathbb{Z}\sqrt{a}$ des Körpers $\mathbb{Q}(\sqrt{a})$ auch die Grundeinheit der Ordnung $\mathbb{Z}+\mathbb{Z}\sqrt{a}+\mathbb{Z}\sqrt{-b}+\mathbb{Z}\sqrt{a}\sqrt{-b}$ im Körper $\mathbb{Q}(\sqrt{a},\sqrt{-b})$ ist.

Aufgabe 3. Sei K ein Zahlkörper vom Grade $n = [K:\mathbb{Q}]$. Ein vollständiger Modul in K ist eine Untergruppe der Form

$$M = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n\,,$$

wobei $\alpha_1,\ldots,\alpha_n$ linear unabhängige Elemente von K sind. Zeige, daß der Multiplikatorenring

$$\mathcal{O} = \{\alpha \in K \mid \alpha M \subseteq M\}$$

eine Ordnung in K, aber i.a. nicht die Hauptordnung ist.

Aufgabe 4. Bestimme den Multiplikatorenring $\mathcal{O}$ des vollständigen Moduls $M = \mathbb{Z}+\mathbb{Z}\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$. Zeige, daß $\varepsilon = 1+\sqrt{2}$ eine Grundeinheit von $\mathcal{O}$ ist. Bestimme sämtliche ganzzahligen Lösungen der „Pellschen Gleichung"

$$x^2 - 2y^2 = 7\,.$$

Hinweis: $N(x+y\sqrt{2}) = x^2-2y^2$, $N(3+\sqrt{2}) = N(5+3\sqrt{2}) = 7$.

Aufgabe 5. In einem eindimensionalen noetherschen Integritätsbereich sind die regulären Primideale $\neq 0$ gerade die invertierbaren Primideale.

§ 13. Eindimensionale Schemata

Die Theorie der algebraischen Zahlkörper, die zunächst von den Methoden der Arithmetik und der Algebra beherrscht wird, läßt sich in grundlegender Weise auch aus einer geometrischen Sicht behandeln, durch die sie auf vielfältige Art ganz neuartige Aspekte zeigt. Diese geometrische Interpretation beruht auf der Möglichkeit, die Zahlen als Funktionen auf einem topologischen Raum aufzufassen.

Zur Erläuterung gehen wir von den Polynomen

$$f(x) = a_n x^n + \cdots + a_0$$

mit komplexen Koeffizienten $a_i \in \mathbb{C}$ aus, die wir in direkter Weise als Funktionen auf der komplexen Zahlenebene ansehen können. Dieses Merkmal läßt sich rein algebraisch wie folgt formulieren. Sei $a \in \mathbb{C}$ ein Punkt der komplexen Zahlenebene. Die Gesamtheit aller Funktionen $f(x)$ im Polynomring $\mathbb{C}[x]$, die im Punkt a verschwinden, bilden das maximale Ideal $\mathfrak{p} = (x - a)$ von $\mathbb{C}[x]$. Die Punkte der komplexen Ebene entsprechen auf diese Weise umkehrbar eindeutig den maximalen Idealen von $\mathbb{C}[x]$, deren Gesamtheit wir mit

$$M = \operatorname{Max}(\mathbb{C}[x])$$

bezeichnen. Wir sehen M als neuen Raum an und können die Elemente $f(x)$ des Ringes $\mathbb{C}[x]$ als Funktionen auf M wie folgt interpretieren. Für jeden Punkt $\mathfrak{p} = (x - a)$ von M haben wir den kanonischen Isomorphismus

$$\mathbb{C}[x]/\mathfrak{p} \xrightarrow{\sim} \mathbb{C},$$

bei dem die Restklasse $f(x) \bmod \mathfrak{p}$ in $f(a)$ übergeht. Wir sehen daher diese Restklasse

$$f(\mathfrak{p}) := f(x) \bmod \mathfrak{p} \in \kappa(\mathfrak{p})$$

im Restklassenkörper $\kappa(\mathfrak{p}) = \mathbb{C}[x]/\mathfrak{p}$ als den „Wert“ von f im Punkte $\mathfrak{p} \in M$ an. Die Topologie auf $\mathbb{C}$ läßt sich in algebraischer Weise nicht auf M herüberziehen. Alles, was algebraisch zu retten ist, sind die durch die Gleichungen

$$f(x) = 0$$

definierten Punktmengen (also nur die endlichen Mengen und M selber), die als abgeschlossene Mengen erklärt werden. In der neuen Formulierung sind dies die Mengen

$$V(f) = \{\mathfrak{p} \in M \mid f(\mathfrak{p}) = 0\} = \{\mathfrak{p} \in M \mid \mathfrak{p} \supseteq (f(x))\}.$$

Die obige algebraische Interpretation der Funktionen führt nun zu der folgenden geometrischen Deutung ganz allgemeiner Ringe. Für einen beliebigen Ring $\mathcal{O}$ wird das **Spektrum**

$$X = \mathrm{Spec}(\mathcal{O})$$

als die Menge aller Primideale $\mathfrak{p}$ von $\mathcal{O}$ eingeführt. Die **Zariski-Topologie** auf X ist dadurch definiert, daß die Mengen

$$V(\mathfrak{a}) = \{\mathfrak{p} \mid \mathfrak{p} \supseteq \mathfrak{a}\}$$

als abgeschlossen erklärt werden, wobei $\mathfrak{a}$ die Ideale von $\mathcal{O}$ durchläuft. X wird damit zu einem topologischen Raum (man beachte $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab})$), der aber in aller Regel nicht hausdorffsch ist. Die abgeschlossenen Punkte entsprechen den maximalen Idealen von $\mathcal{O}$.

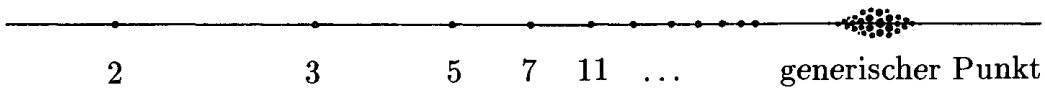
Die Elemente $f \in \mathcal{O}$ spielen die Rolle von Funktionen auf dem topologischen Raum X: Der „Wert" von f im Punkte $\mathfrak{p}$ wird durch

$$f(\mathfrak{p}) := f \bmod \mathfrak{p}$$

definiert und ist ein Element im Restklassenkörper $\kappa(\mathfrak{p})$, d.h. im Quotientenkörper von $\mathcal{O}/\mathfrak{p}$. Die Werte von f liegen also i.a. nicht mehr in ein- und demselben Körper.

Die Zulassung auch der nicht-maximalen Primideale als nicht-abgeschlossene Punkte erweist sich als überaus praktisch, hat aber auch einen sinnfälligen Grund. Im Fall des Ringes $\mathcal{O} = \mathbb{C}[x]$ etwa hat der Punkt $\mathfrak{p} = (0)$ den Restklassenkörper $\kappa(\mathfrak{p}) = \mathbb{C}(x)$. Der „Wert" eines Polynoms $f \in \mathbb{C}[x]$ in diesem Punkt ist $f(x)$ selbst, aufgefaßt als Element von $\mathbb{C}(x)$. Dieses Element sollte als der Wert von f an der **unbestimmten** Stelle x angesehen werden, die man sich überall und nirgends vorstellen darf. Diese Sichtweise geht einher mit der Tatsache, daß der Abschluß des Punktes $\mathfrak{p} = (0)$ in der Zariski-Topologie von X der ganze Raum X ist. $\mathfrak{p}$ heißt daher auch der **generische Punkt** von X.

Beispiel: Der Raum $X = \mathrm{Spec}(\mathbb{Z})$ wird durch eine Gerade



veranschaulicht. Man hat für jede Primzahl einen abgeschlossenen Punkt und überdies den generischen Punkt (0), dessen Abschluß ganz X ist. Die nicht-leeren offenen Mengen von X erhält man durch Wegwerfen endlich vieler Primzahlen $p_1, \ldots, p_n$. Die ganzen Zahlen $a \in \mathbb{Z}$ werden

als Funktionen auf X aufgefaßt, indem der Wert von a im Punkte (p) durch die Restklasse

$$a(p) = a \bmod p \in \mathbb{Z}/p\mathbb{Z}$$

erklärt wird. Als Wertekörper erhalten wir

$$\mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/7\mathbb{Z},\ \mathbb{Z}/11\mathbb{Z},\ldots,\mathbb{Q}.$$

Es tritt also jeder Primkörper genau einmal auf.

Eine wichtige Verfeinerung der geometrischen Interpretation der Elemente des Ringes o als Funktionen auf dem Raum $X = \mathrm{Spec}(o)$ ergibt sich durch die Bildung der **Strukturgarbe** o_X. Damit ist folgendes gemeint. Sei $U \neq \emptyset$ eine offene Teilmenge von X. Wenn o ein eindimensionaler Integritätsbereich ist, so ist der Ring der „regulären Funktionen" auf U durch

$$o(U) = \{\frac{f}{g} \mid g(\mathfrak{p}) \neq 0 \quad \text{für alle } \mathfrak{p} \in U\}$$

gegeben, also durch die Lokalisierung von o nach der multiplikativen Menge $S = o \setminus \bigcup_{\mathfrak{p}\in U} \mathfrak{p}$ (vgl. § 11). Im allgemeinen Fall wird $o(U)$ definiert als die Gesamtheit aller Elemente

$$s = (s_\mathfrak{p}) \in \prod_{\mathfrak{p}\in U} o_\mathfrak{p}\,,$$

die lokal Quotienten von zwei Elementen von o sind. Genauer bedeutet dies, daß es zu jedem $\mathfrak{p} \in U$ eine Umgebung $V \subseteq U$ von $\mathfrak{p}$ gibt und Elemente $f, g \in o$, derart daß für jedes $\mathfrak{q} \in V$ gilt: $g(\mathfrak{q}) \neq 0$ und $s_\mathfrak{q} = f/g$ in $o_\mathfrak{q}$. Die Quotientenbildung ist hier in dem allgemeineren Sinne der kommutativen Algebra gemeint (vgl. § 11, Aufgabe 1). Es ist dem Leser überlassen, zu prüfen, daß man bei einem eindimensionalen Integritätsbereich o die obige Definition zurückerhält.

Sind $V \subseteq U$ zwei offene Mengen von X, so induziert die Projektion

$$\prod_{\mathfrak{p}\in U} o_\mathfrak{p} \to \prod_{\mathfrak{p}\in V} o_\mathfrak{p}$$

einen Homomorphismus

$$\rho_{UV} : o(U) \to o(V)\,,$$

der die **Restriktion** von U nach V genannt wird. Das System der Ringe $o(U)$ und Abbildungen ρ_{UV} ist eine **Garbe** auf X. Darunter versteht man folgendes.

(13.1) Definition. *Sei X ein topologischer Raum. Eine* **Prägarbe** *$\mathcal{F}$ von abelschen Gruppen (Ringen etc.) besteht aus folgenden Daten:*

1) *Für jede offene Menge U ist eine abelsche Gruppe (ein Ring etc.) $\mathcal{F}(U)$ gegeben.*

2) *Für jede Inklusion $U \subseteq V$ ist ein Homomorphismus $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$ gegeben, Restriktion genannt.*

Diese Daten sind den folgenden Bedingungen unterworfen:

a) $\mathcal{F}(\emptyset) = 0$,

b) *ρ_{UU} ist die identische Abbildung* $\mathrm{id} : \mathcal{F}(U) \to \mathcal{F}(U)$,

c) $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$ *für offene Mengen* $W \subseteq V \subseteq U$.

Die Elemente $s \in \mathcal{F}(U)$ heißen die **Schnitte** der Prägarbe $\mathcal{F}$ über U. Ist $V \subseteq U$, so schreibt man $\rho_{UV}(s) = s|_V$. Die Definition der Prägarbe läßt sich kurz und bündig in der Sprache der Kategorien formulieren. Die offenen Mengen des topologischen Raumes X bilden eine Kategorie X_{top}, in der als einzige Morphismen die Inklusionen gelten. Eine Prägarbe von abelschen Gruppen (Ringen) ist nun nichts weiter als ein kontravarianter Funktor

$$\mathcal{F} : X_{\mathrm{top}} \to (ab)\,,\ (Ringe)$$

in die Kategorie der abelschen Gruppen (bzw. der Ringe) mit $\mathcal{F}(\emptyset) = 0$.

(13.2) Definition. *Eine Prägarbe $\mathcal{F}$ auf dem topologischen Raum X heißt eine* **Garbe**, *wenn für die offenen Überdeckungen $\{U_i\}$ der offenen Mengen U gilt:*

(i) Sind $s, s' \in \mathcal{F}(U)$ zwei Schnitte mit $s|_{U_i} = s'|_{U_i}$ für alle i, so ist $s = s'$.

(ii) Ist $s_i \in \mathcal{F}(U_i)$ eine Familie von Schnitten mit

$$s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$$

für alle i, j, so gibt es ein $s \in \mathcal{F}(U)$ mit $s|_{U_i} = s_i$ für alle i.

Unter dem **Halm** der Garbe $\mathcal{F}$ im Punkte $x \in X$ versteht man den direkten Limes (vgl. Kap. IV, § 2)

$$\mathcal{F}_x = \varinjlim_{U \ni x} \mathcal{F}(U)\,,$$

wobei U alle offenen Umgebungen von x durchläuft. Mit anderen Worten: In der disjunkten Vereinigung $\bigcup_{U \ni x} \mathcal{F}(U)$ heißen zwei Schnitte $s_U \in \mathcal{F}(U)$ und $s_V \in \mathcal{F}(V)$ äquivalent, wenn es eine Umgebung

$W \subseteq U \cap V$ von x gibt mit $s_U|_W = s_V|_W$. Die Äquivalenzklassen heißen **Keime** von Schnitten bei x und bilden die Elemente von $\mathcal{F}_x$.

Wir kehren zurück zum Spektrum $X = \mathrm{Spec}(\mathcal{O})$ eines Ringes $\mathcal{O}$ und erhalten den

(13.3) Satz. *Die Ringe $\mathcal{O}(U)$ bilden zusammen mit den Restriktionsabbildungen ρ_{UV} eine* **Garbe** *auf X. Diese wird mit $\mathcal{O}_X$ bezeichnet und heißt die* **Strukturgarbe** *auf X.*

Der Halm von $\mathcal{O}_X$ im Punkte $\mathfrak{p} \in X$ ist die Lokalisierung $\mathcal{O}_{\mathfrak{p}}$: $\mathcal{O}_{X,\mathfrak{p}} \cong \mathcal{O}_{\mathfrak{p}}$.

Der Beweis dieses Satzes ergibt sich unmittelbar aus den Definitionen. Das Paar $(X, \mathcal{O}_X)$ heißt ein **affines Schema**. Die Strukturgarbe $\mathcal{O}_X$ wird aber meistens bei der Benennung fortgelassen. Sei jetzt

$$\varphi : \mathcal{O} \to \mathcal{O}'$$

ein Homomorphismus von Ringen und $X = \mathrm{Spec}(\mathcal{O})$, $X' = \mathrm{Spec}(\mathcal{O}')$. φ induziert dann eine stetige Abbildung

$$f : X' \to X\,, \quad f(\mathfrak{p}') := \varphi^{-1}(\mathfrak{p}')\,,$$

und für jede offene Teilmenge U von X einen Homomorphismus

$$f_U^* : \mathcal{O}(U) \to \mathcal{O}(U')\,, \quad s \mapsto s \circ f|_{U'}\,,$$

wobei $U' = f^{-1}(U)$ ist. Die Abbildungen f_U^* haben die folgenden beiden Eigenschaften.

a) Sind $V \subseteq U$ offene Mengen, so ist das Diagramm

$$\begin{array}{ccc} \mathcal{O}(U) & \xrightarrow{f_U^*} & \mathcal{O}(U') \\ {\scriptstyle \rho_{UV}}\downarrow & & \downarrow{\scriptstyle \rho_{U'V'}} \\ \mathcal{O}(V) & \xrightarrow{f_V^*} & \mathcal{O}(V') \end{array}$$

kommutativ.

b) Für $\mathfrak{p}' \in U' \subseteq X'$ und $a \in \mathcal{O}(U)$ gilt

$$a(f(\mathfrak{p}')) = 0 \quad \Rightarrow \quad f_U^*(a)(\mathfrak{p}') = 0\,.$$

Eine stetige Abbildung $f : X' \to X$ zusammen mit einer Familie von Homomorphismen $f_U^* : \mathcal{O}(U) \to \mathcal{O}(U')$, die den Bedingungen a) und b) genügen, heißt ein **Morphismus** des Schemas X' in das Schema X. Bei der Benennung eines solchen Morphismus werden die Abbildungen

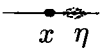
f_U^* meistens nicht erwähnt. Man kann zeigen, daß jeder Morphismus zwischen zwei affinen Schemata $X' = \operatorname{Spec}(\mathcal{O}')$ und $X = \operatorname{Spec}(\mathcal{O})$ in der oben beschriebenen Weise von einem Ringhomomorphismus $\varphi : \mathcal{O} \to \mathcal{O}'$ induziert wird.

Die Beweise der obigen Behauptungen sind einfach, zum Teil jedoch etwas länglich. Der Begriff des Schemas bildet die Grundlage einer sehr umfangreichen Theorie, die innerhalb der Mathematik eine zentrale Stellung einnimmt. Für eine Einführung in diese wichtige Disziplin seien die Bücher [51] und [104] empfohlen.

Wir beschränken uns jetzt auf die Betrachtung der noetherschen Integritätsbereiche $\mathcal{O}$ der Dimension ≤ 1 und wollen einige der bisher behandelten Sachverhalte durch die schematheoretische Deutung geometrisch veranschaulichen.

1. Körper. Ist K ein Körper, so besteht das Schema $\operatorname{Spec}(K)$ aus einem einzigen Punkt (0), auf dem der Körper K als Strukturgarbe sitzt. Man darf diese einpunktigen Schemata nicht als gleich ansehen, denn sie unterscheiden sich wesentlich in der Strukturgarbe.

2. Bewertungsringe. Ist $\mathcal{O}$ ein diskreter Bewertungsring mit dem maximalen Ideal $\mathfrak{p}$, so besteht das Schema $X = \operatorname{Spec}(\mathcal{O})$ aus zwei Punkten, dem abgeschlossenen Punkt $x = \mathfrak{p}$ mit dem Restklassenkörper $\kappa(\mathfrak{p}) = \mathcal{O}/\mathfrak{p}$ und dem generischen Punkt $\eta = (0)$ mit dem Restklassenkörper $\kappa(\eta) = K$, dem Quotientenkörper von $\mathcal{O}$. Man muß sich X als einen Punkt x mit einer infinitesimalen Umgebung vorstellen, die von dem generischen Punkt η durchlaufen wird:

$X :$ 

Diese Vorstellung rechtfertigt sich durch die folgende Betrachtung.

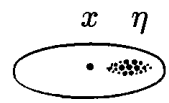
Die diskreten Bewertungsringe treten als Lokalisierungen

$$\mathcal{O}_{\mathfrak{p}} = \{\tfrac{f}{g} \mid f, g \in \mathcal{O},\ g(\mathfrak{p}) \neq 0\}$$

von Dedekindringen $\mathcal{O}$ auf. Es gibt keine Umgebung von $\mathfrak{p}$ in $X = \operatorname{Spec}(\mathcal{O})$, auf der alle Funktionen $\frac{f}{g} \in \mathcal{O}_{\mathfrak{p}}$ definiert sind, denn zu jedem Punkt $\mathfrak{q} \neq \mathfrak{p}$, $\mathfrak{q} \neq 0$, finden wir nach dem chinesischen Restsatz ein $g \in \mathcal{O}$ mit $g \equiv 0 \bmod \mathfrak{q}$ und $g \equiv 1 \bmod \mathfrak{p}$, so daß $\frac{1}{g} \in \mathcal{O}_{\mathfrak{p}}$ als Funktion nicht in $\mathfrak{q}$ definiert ist. Jedes Element $\frac{f}{g} \in \mathcal{O}_{\mathfrak{p}}$ ist aber auf einer genügend kleinen Umgebung definiert, so daß man sagen kann, daß alle Elemente $\frac{f}{g}$ des diskreten Bewertungsringes $\mathcal{O}_{\mathfrak{p}}$ auf dem „Keim“ einer Umgebung von $\mathfrak{p}$

als Funktionen leben. Als einen solchen „Umgebungskeim" von $\mathfrak{p}$ darf man sich daher $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$ denken.

Es sei auf eine kleine Diskrepanz in der Anschauung hingewiesen. Betrachtet man das Spektrum des eindimensionalen Ringes $\mathbb{C}[x]$, dessen Punkte die komplexe Zahlenebene ausmachen, so wird man sich die infinitesimale Umgebung $X_\mathfrak{p} = \mathrm{Spec}(\mathbb{C}[x]_\mathfrak{p})$ eines Punktes $\mathfrak{p} = (x - a)$ nicht als ein kleines Geradenstück vorstellen wollen, sondern als eine kleine Kreisscheibe:

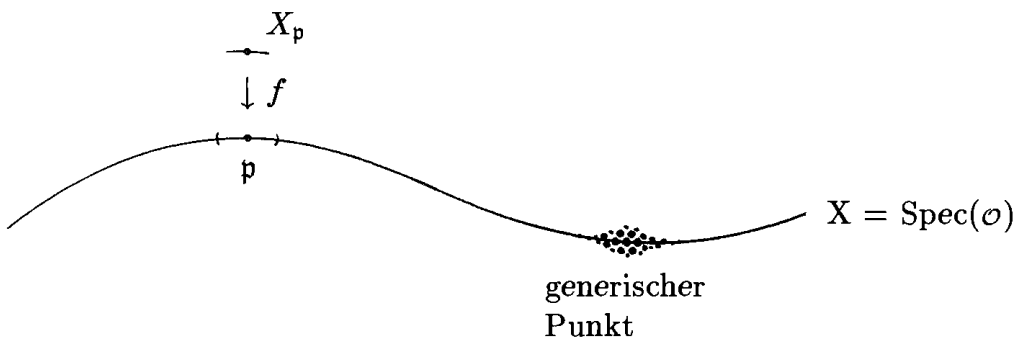


Dieser zweidimensionale Charakter haftet allen diskreten Bewertungsringen mit algebraisch abgeschlossenem Restklassenkörper an, jedoch erhält diese Anschauung ihre algebraische Rechtfertigung erst durch eine neue Topologie, die **Etaltopologie**, die sehr viel feiner ist als die Zariski-Topologie (vgl. [103], [132]).

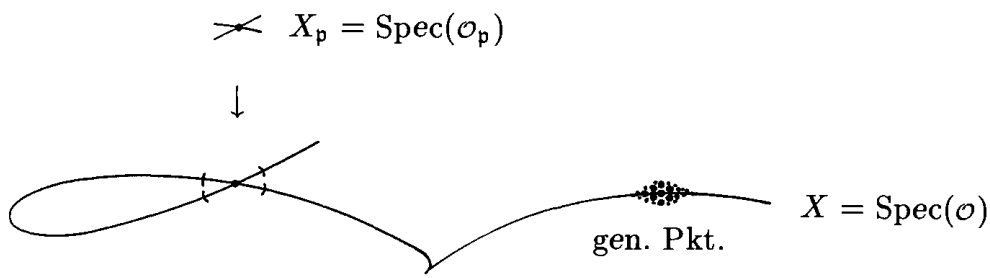
3. Dedekindringe. Das Spektrum $X = \mathrm{Spec}(\mathcal{O})$ eines Dedekindringes $\mathcal{O}$ stellt man sich als eine glatte Kurve vor. In jedem Punkt $\mathfrak{p}$ kann man die **Lokalisierung** $\mathcal{O}_\mathfrak{p}$ betrachten. Die Inklusion $\mathcal{O} \hookrightarrow \mathcal{O}_\mathfrak{p}$ induziert einen Morphismus

$$f : X_\mathfrak{p} = \mathrm{Spec}(\mathcal{O}_\mathfrak{p}) \to X\,,$$

durch den das Schema $X_\mathfrak{p}$ als „infinitesimale Umgebung" von $\mathfrak{p}$ aus X herausgehoben wird:



4. Singularitäten. Wir betrachten jetzt einen eindimensionalen noetherschen Integritätsbereich $\mathcal{O}$, der kein Dedekindring ist, wie z.B. eine Ordnung eines algebraischen Zahlkörpers, die von der Hauptordnung verschieden ist. Wieder sehen wir das Schema $X = \mathrm{Spec}(\mathcal{O})$ als eine Kurve an, jedoch als eine Kurve, die nicht mehr überall glatt ist, sondern in manchen Punkten „Singularitäten" hat.

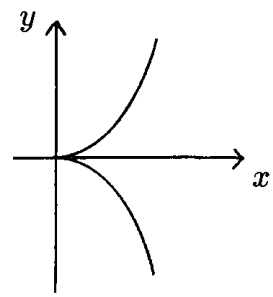


Dies sind genau diejenigen nicht-generischen Punkte $\mathfrak{p}$, für die die Lokalisierung $\mathcal{O}_\mathfrak{p}$ kein diskreter Bewertungsring mehr ist, das maximale Ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ also nicht mehr durch ein einziges Element erzeugt wird. Bei dem eindimensionalen Ring $\mathcal{O} = \mathbb{C}[x,y]/(y^2-x^3)$ zum Beispiel sind die abgeschlossenen Punkte des Schemas X durch die Primideale

$$\mathfrak{p} = (x-a, y-b) \bmod (y^2 - x^3)$$

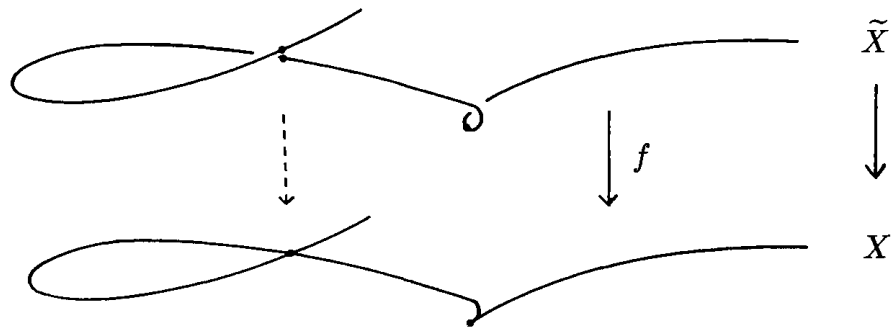
gegeben, wobei (a,b) die Punkte des $\mathbb{C}^2$ durchläuft, die der Gleichung

$$b^2 - a^3 = 0$$



genügen. Der einzige singuläre Punkt ist der Nullpunkt, der dem maximalen Ideal $\mathfrak{p}_0 = (\bar{x}, \bar{y})$ entspricht, wobei $\bar{x} = x \bmod (y^2-x^3)$, $\bar{y} = y \bmod (y^2 - x^3) \in \mathcal{O}$. Das maximale Ideal $\mathfrak{p}_0\mathcal{O}_{\mathfrak{p}_0}$ des lokalen Ringes wird durch die Elemente $\bar{x}, \bar{y}$ erzeugt, kann aber nicht durch ein einziges Element erzeugt werden.

5. Normalisierung. Die Bildung der Normalisierung $\tilde{\mathcal{O}}$ eines eindimensionalen noetherschen Integritätsbereiches $\mathcal{O}$ bedeutet geometrisch die *Auflösung* der soeben besprochenen Singularitäten. Ist nämlich $X = \mathrm{Spec}(\mathcal{O})$ und $\tilde{X} = \mathrm{Spec}(\tilde{\mathcal{O}})$, so induziert die Inklusion $\mathcal{O} \hookrightarrow \tilde{\mathcal{O}}$ einen Morphismus $f : \tilde{X} \to X$.



Da $\tilde{o}$ ein Dedekindring ist, so ist das Schema $\tilde{X}$ als glatt anzusehen. Ist $\mathfrak{p}\tilde{o} = \tilde{\mathfrak{p}}_1^{e_r} \dots \tilde{\mathfrak{p}}_r^{e_r}$ die Primzerlegung von $\mathfrak{p}$ in $\tilde{o}$, so sind $\tilde{\mathfrak{p}}_1, \dots, \tilde{\mathfrak{p}}_r$ die verschiedenen Punkte von $\tilde{X}$, die unter f auf $\mathfrak{p}$ abgebildet werden. Man kann zeigen, daß $\mathfrak{p}$ genau dann ein regulärer Punkt von X ist, d.h. ein Punkt, für den $o_\mathfrak{p}$ ein diskreter Bewertungsring ist, wenn $r = 1$, $e_1 = 1$ und $f_1 = (\tilde{o}/\tilde{\mathfrak{p}}_1 : o/\mathfrak{p}) = 1$ ist.

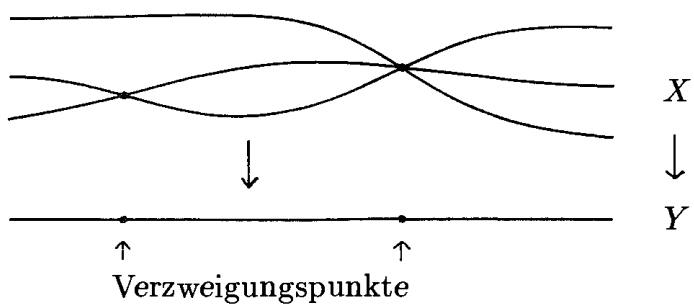
6. Erweiterungen. Sei o ein Dedekindring mit dem Quotientenkörper K, $L|K$ eine endliche separable Erweiterung und $\mathcal{O}$ der ganze Abschluß von o in L. Sei $Y = \mathrm{Spec}(o)$, $X = \mathrm{Spec}(\mathcal{O})$ und

$$f : X \to Y$$

der durch die Inklusion $o \hookrightarrow \mathcal{O}$ induzierte Morphismus. Ist $\mathfrak{p}$ ein maximales Ideal von o und

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

die Primzerlegung von $\mathfrak{p}$ in $\mathcal{O}$, so sind $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ die verschiedenen Punkte von X, die durch f auf $\mathfrak{p}$ abgebildet werden. Der Morphismus f ist eine „verzweigte Überlagerung". Er wird durch das folgende Bild veranschaulicht:



Dieses Bild spiegelt den algebraischen Sachverhalt allerdings nur dann korrekt wieder, wenn die Restklassenkörper von o (wie bei $\mathbb{C}[x]$)

algebraisch abgeschlossen sind. Dann liegen nach der fundamentalen Gleichung $\sum_i e_i f_i = n$ über jedem Punkt $\mathfrak{p}$ von Y genau $n = [L : K]$ Punkte $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ von X, es sei denn $\mathfrak{p}$ ist verzweigt in $\mathcal{O}$. Bei einem Verzweigungspunkt $\mathfrak{p}$ fallen gewissermaßen mehrere der Punkte $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ zusammen. Hiermit ist auch der Name „Verzweigungsideal" erklärt.

Ist $L|K$ galoissch mit der Galoisgruppe $G = G(L|K)$, so induziert jeder Automorphismus $\sigma \in G$ über $\sigma : \mathcal{O} \to \mathcal{O}$ einen Automorphismus von Schemata $\sigma : X \to X$. Da der Ring $\mathcal{O}$ festgelassen wird, so ist das Diagramm

$$\begin{array}{ccc} X & \xrightarrow{\sigma} & X \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle f} & \\ & Y & \end{array}$$

kommutativ. Einen solchen Automorphismus nennt man eine **Decktransformation** der verzweigten Überlagerung X/Y. Die Gruppe der Decktransformationen wird mit $\mathrm{Aut}_Y(X)$ bezeichnet. Wir haben also einen kanonischen Isomorphismus

$$G(L|K) \cong \mathrm{Aut}_Y(X)\,.$$

In Kap. II, § 7 werden wir sehen, daß das Kompositum zweier unverzweigter Erweiterungen von K wieder unverzweigt ist. Das in einem algebraischen Abschluß $\overline{K}$ von K gebildete Kompositum $\tilde{K}$ *aller* unverzweigten Erweiterungen $L|K$ heiße die **maximale unverzweigte Erweiterung**. Der ganze Abschluß $\tilde{\mathcal{O}}$ von $\mathcal{O}$ in $\tilde{K}$ ist zwar noch ein eindimensionaler Integritätsbereich, ist aber i.a. nicht mehr noethersch, und es liegen über einem Primideal $\mathfrak{p} \neq 0$ von $\mathcal{O}$ in aller Regel unendlich viele Primideale. Das Schema $\tilde{Y} = \mathrm{Spec}(\tilde{\mathcal{O}})$ mit dem Morphismus

$$f : \tilde{Y} \to Y$$

heißt die **universelle Überlagerung** von Y. Sie spielt bei den Schemata die gleiche Rolle wie in der Topologie die universelle Überlagerung $\tilde{X} \to X$ eines topologischen Raumes. Da dort die Gruppe der Decktransformationen $\mathrm{Aut}_X(\tilde{X})$ kanonisch isomorph zur Fundamentalgruppe $\pi_1(X)$ ist, so wird hier die **Fundamentalgruppe** des Schemas Y durch

$$\pi_1(Y) = \mathrm{Aut}_Y(\tilde{Y}) = G(\tilde{K}|K)$$

definiert. Hiermit ist eine erste Verbindung der Galoistheorie mit der klassischen Topologie geknüpft. Sie setzt sich in erheblichem Umfange fort durch die Betrachtung der **Etaltopologie**.

Die in diesem Paragraphen dargelegte geometrische Betrachtungsweise der algebraischen Zahlkörper erfährt eine überzeugende Bekräftigung durch die Theorie der Funktionenkörper und der algebraischen Kurven über einem endlichen Körper $\mathbb{F}_p$, mit der sie in engster Analogiebeziehung steht.

§ 14. Funktionenkörper

Zum Schluß dieses Kapitels wollen wir in kurzen Andeutungen auf die Theorie der **Funktionenkörper** eingehen, die den algebraischen Zahlkörpern in frappierender Entsprechung zur Seite stehen und durch ihre ganz unmittelbare Beziehung zur Geometrie eine leitbildhafte Bedeutung für die Theorie der algebraischen Zahlkörper erhalten.

Der Ring $\mathbb{Z}$ der ganzen Zahlen mit seinem Quotientenkörper $\mathbb{Q}$ steht in einer auffälligen Analogie zum Polynomring $\mathbb{F}_p[t]$ über dem Körper $\mathbb{F}_p$ von p Elementen mit seinem Quotientenkörper $\mathbb{F}_p(t)$. Wie $\mathbb{Z}$ ist auch $\mathbb{F}_p[t]$ ein Hauptidealring. Den Primzahlen entsprechen die normierten irreduziblen Polynome $p(t) \in \mathbb{F}_p[t]$, die wie die Primzahlen endliche Körper $\mathbb{F}_{p^d}$, $d = \mathrm{Grad}(p(t))$, als Restklassenringe haben, nur daß diese jetzt alle dieselbe Charakteristik besitzen. Der geometrische Charakter des Ringes $\mathbb{F}_p[t]$ tritt hier viel unmittelbarer hervor, denn für ein Element $f = f(t) \in \mathbb{F}_p[t]$ ist der Wert von f in einem Punkt $\mathfrak{p} = (p(t))$ des affinen Schemas $X = \mathrm{Spec}(\mathbb{F}_p[t])$ wirklich durch den Wert $f(a) \in \mathbb{F}_p$ gegeben, wenn $p(t) = t - a$ ist, oder allgemeiner durch $f(\alpha) \in \mathbb{F}_{p^d}$, wenn $\alpha \in \mathbb{F}_{p^d}$ eine Nullstelle von $p(t)$ ist. Dies beruht auf der Isomorphie

$$\mathbb{F}_p[t]/\mathfrak{p} \xrightarrow{\sim} \mathbb{F}_{p^d},$$

bei der die Restklasse $f(\mathfrak{p}) = f \bmod \mathfrak{p}$ in $f(\alpha)$ übergeht. In der Analogie des Fortschreitens der Primzahlen $2, 3, 5, 7, \ldots$ auf der einen Seite und des Wachsens der Mächtigkeiten $p, p^2, p^3, p^4, \ldots$ der Restklassenkörper $\mathbb{F}_{p^d}$ auf der anderen liegt eines der tiefsten Geheimnisse der Arithmetik.

Für die endlichen Erweiterungen K von $\mathbb{F}_p(t)$ erhält man nun die gleiche arithmetische Theorie wie für die algebraischen Zahlkörper, so wie wir sie ganz allgemein für beliebige eindimensionale noethersche Integritätsbereiche entwickelt haben. Der entscheidende Unterschied zum Zahlkörperfall liegt jedoch darin, daß der Funktionenkörper K abseits von den Primidealen von $\mathfrak{o}$ noch endlich viele weitere Primideale versteckt, die zur Entwicklung einer vollständigen Theorie unbedingt mit ins Auge gefaßt werden müssen.

Dieses Phänomen wird schon am Beispiel des rationalen Funktionenkörpers $\mathbb{F}_p(t)$ deutlich und beruht darauf, daß die Wahl der Unbestimmten t, die den Ganzheitsring $\mathbb{F}_p[t]$ festlegt, ganz willkürlich ist. Eine andere Wahl, etwa $t' = 1/t$, legt einen ganz anderen Ring $\mathbb{F}_p[1/t]$ fest und damit ganz andere Primideale. Es kommt daher darauf an, eine von solcher Wahl unabhängige Theorie zu entwickeln. Dies kann auf zwei Weisen geschehen, eine bewertungstheoretische und eine schematheoretische, also geometrische.

Wir erläutern zuerst die naivere, d.h. die bewertungstheoretische Methode. Sei K eine endliche Erweiterung von $\mathbb{F}_p(t)$ und $\mathcal{O}$ der ganze Abschluß von $\mathbb{F}_p[t]$ in K. Nach § 11 gehört zu jedem Primideal $\mathfrak{p} \neq 0$ von $\mathcal{O}$ eine normierte diskrete Bewertung, d.h. eine surjektive Funktion

$$v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$$

mit den Eigenschaften

(i) $v_\mathfrak{p}(0) = \infty$,

(ii) $v_\mathfrak{p}(ab) = v_\mathfrak{p}(a) + v_\mathfrak{p}(b)$,

(iii) $v_\mathfrak{p}(a+b) \geq \min\{v_\mathfrak{p}(a), v_\mathfrak{p}(b)\}$.

Mit der Primzerlegung im Dedekindring $\mathcal{O}$ stehen die Bewertungen in der Beziehung

$$(a) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(a)}.$$

Die Definition einer diskreten Bewertung von K bedarf nun nicht der Vorgabe eines Teilringes $\mathcal{O}$, und es kommen in der Tat außer den aus $\mathcal{O}$ entstehenden Bewertungen noch endlich viele weitere hinzu. Im Falle des Körpers $\mathbb{F}_p(t)$ gibt es außer den zu den Primidealen $\mathfrak{p} = (p(t))$ von $\mathbb{F}_p[t]$ gehörenden Bewertungen noch eine weitere, die **Gradbewertung** v_∞. Sie ist für $\frac{f}{g} \in \mathbb{F}_p(t)$, $f, g \in \mathbb{F}_p[t]$, durch

$$v_\infty(\frac{f}{g}) = \mathrm{Grad}(g) - \mathrm{Grad}(f)$$

gegeben und gehört zum Primideal $\mathfrak{p} = y\mathbb{F}_p[y]$ des Ringes $\mathbb{F}_p[y]$ mit $y = 1/t$. Man kann zeigen, daß hiermit alle normierten Bewertungen des Körpers $\mathbb{F}_p(t)$ erschöpft sind.

Für eine beliebige endliche Erweiterung K von $\mathbb{F}_p(t)$ betrachtet man nun anstelle der Primideale die sämtlichen normierten diskreten Bewertungen $v_\mathfrak{p}$ von K im obigen Sinne, wobei man den Buchstaben $\mathfrak{p}$ als Symbol beibehält. Als Analogon zur Idealgruppe bildet man die freie, durch diese Symbole erzeugte "Divisorengruppe"

$$Div(K) = \{\sum_\mathfrak{p} n_\mathfrak{p}\mathfrak{p} \mid n_\mathfrak{p} \in \mathbb{Z},\ n_\mathfrak{p} = 0 \quad \text{für fast alle } \mathfrak{p}\},$$

betrachtet die Abbildung

$$\operatorname{div} : K^* \to Div(K), \quad \operatorname{div}(f) = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(f)\mathfrak{p},$$

mit dem Bild $\mathcal{P}(K)$ und definiert die Divisorenklassengruppe von K durch

$$Cl(K) = Div(K)/\mathcal{P}(K).$$

Im Gegensatz zur Idealklassengruppe eines algebraischen Zahlkörpers ist diese Gruppe nicht endlich. Man hat vielmehr den kanonischen Homomorphismus

$$\deg : Cl(K) \to \mathbb{Z},$$

der der Klasse von $\mathfrak{p}$ den Grad $\deg(\mathfrak{p}) = [\kappa(\mathfrak{p}) : \mathbb{F}_p]$ des Restklassenkörpers des Bewertungsringes von $\mathfrak{p}$ zuordnet, und der Klasse eines beliebigen Divisors $\mathfrak{a} = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p}$ die Summe

$$\deg(\mathfrak{a}) = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \deg(\mathfrak{p}).$$

Für einen Hauptdivisor $\operatorname{div}(f)$, $f \in K^*$, ergibt sich durch eine leichte Rechnung $\deg(\operatorname{div}(f)) = 0$, so daß die Abbildung deg wohldefiniert ist. Als Analogon zur Endlichkeit der Klassenzahl bei den Zahlkörpern hat man hier die Tatsache, daß nicht $Cl(K)$ selbst, sondern der Kern $Cl^0(K)$ von deg endlich ist. Die Unendlichkeit der Klassengruppe darf man den Funktionenkörpern nicht als Nachteil anrechnen, sondern muß vielmehr die Endlichkeit bei den Zahlkörpern als einen Mangel ansehen, der nach Korrektur verlangt. Wie diese Situation zu beurteilen ist und wie sie bereinigt wird, werden wir in Kap. III, § 1 erläutern.

Der ideale und in jeder Hinsicht befriedigende Rahmen für die Theorie der Funktionenkörper wird durch den Begriff des **Schemas** gegeben. Im vorigen Paragraphen haben wir die affinen Schemata eingeführt als Paare $(X, \mathcal{O}_X)$, bestehend aus einem topologischen Raum $X = \operatorname{Spec}(\mathcal{O})$ und einer Garbe $\mathcal{O}_X$ von Ringen auf X. Ein Schema ist nun allgemeiner ein topologischer Raum X mit einer Ringgarbe $\mathcal{O}_X$, derart daß zu jedem Punkt von X eine Umgebung U existiert, so daß U zusammen mit der Einschränkung $\mathcal{O}_U$ der Garbe $\mathcal{O}_X$ auf U, also das Paar $(U, \mathcal{O}_U)$, isomorph zu einem affinen Schema im Sinne von § 13 ist. Diese Verallgemeinerung des affinen Schemas ist für die Funktionenkörper K der angemessene Begriff. Er zeigt alle Primideale auf einmal und versteckt keine.

Im Falle $K = \mathbb{F}_p(t)$ etwa erhält man das zugehörige Schema $(X, \mathcal{O}_X)$ durch einen Verklebungsprozeß aus den beiden Ringen $A = \mathbb{F}_p[u]$ und $B = \mathbb{F}_p[v]$, genauer aus den beiden affinen Schemata $U = \operatorname{Spec}(A)$ und $V = \operatorname{Spec}(B)$. Nimmt man aus U den Punkt $\mathfrak{p}_0 = (u)$ und aus

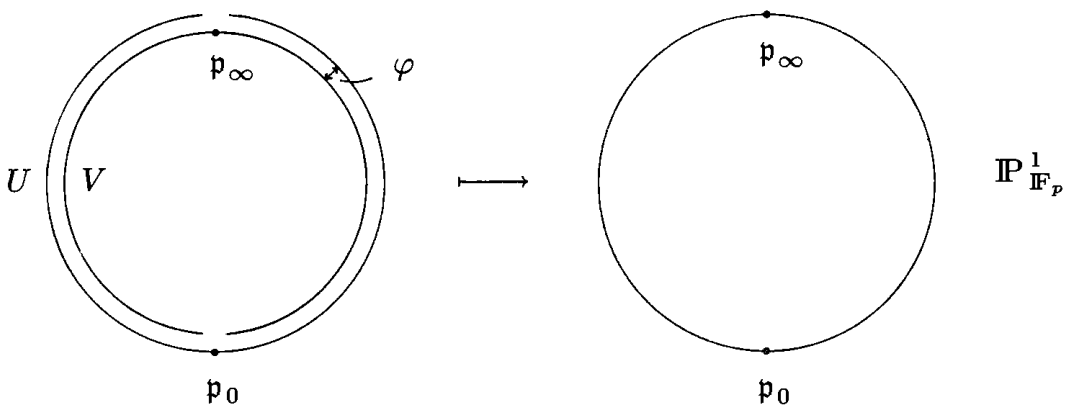
V den Punkt $\mathfrak{p}_\infty = (v)$ heraus, so wird $U - \{\mathfrak{p}_0\} = \mathrm{Spec}(\mathbb{F}_p[u, u^{-1}])$, $V - \{\mathfrak{p}_\infty\} = \mathrm{Spec}(\mathbb{F}_p[v, v^{-1}])$, und man erhält durch den Isomorphismus $f : \mathbb{F}_p[u, u^{-1}] \to \mathbb{F}_p[v, v^{-1}]$, $u \mapsto v^{-1}$, eine Bijektion

$$\varphi : V - \{\mathfrak{p}_\infty\} \to U - \{\mathfrak{p}_0\}, \quad \mathfrak{p} \mapsto f^{-1}(\mathfrak{p}).$$

In der Vereinigung $U \cup V$ werden nun die Punkte von $V - \{\mathfrak{p}_\infty\}$ und $U - \{\mathfrak{p}_0\}$ vermöge φ miteinander identifiziert, und es entsteht ein topologischer Raum X. In einer unmittelbar ersichtlichen Weise wird aus den beiden Garben $\mathcal{O}_U$ und $\mathcal{O}_V$ eine Ringgarbe $\mathcal{O}_X$ auf X. Nimmt man aus X den Punkt $\mathfrak{p}_\infty$ bzw. $\mathfrak{p}_0$ heraus, so erhält man kanonische Isomorphismen

$$(X - \{\mathfrak{p}_\infty\}, \mathcal{O}_{X-\{\mathfrak{p}_\infty\}}) \cong (U, \mathcal{O}_U), \quad (X - \{\mathfrak{p}_0\}, \mathcal{O}_{X-\{\mathfrak{p}_0\}}) \cong (V, \mathcal{O}_V).$$

Das Paar $(X, \mathcal{O}_X)$ ist das dem Körper $\mathbb{F}_p(t)$ zugeordnete Schema. Es heißt die **projektive Gerade** über $\mathbb{F}_p$ und wird mit $\mathbb{P}^1_{\mathbb{F}_p}$ bezeichnet.



Allgemeiner kann man auf ähnliche Weise einer beliebigen Erweiterung $K|\mathbb{F}_p(t)$ ein Schema $(X, \mathcal{O}_X)$ zuordnen. Für die genaue Ausführung dieser Bildung verweisen wir den Leser auf [51].