de Gruyter Lehrbuch

Stroth · Algebra

Gernot Stroth

Algebra

Einführung in die Galoistheorie

Walter de Gruyter
Berlin · New York 1998

Gernot Stroth
Fachbereich Mathematik und Informatik
Institut für Algebra und Geometrie
Universität Halle-Wittenberg
06099 Halle

1991 Mathematics Subject Classification:
12-01, 13-01, 20-01

∞ Gedruckt auf säurefreiem Papier, das die US-ANSI-Norm über Haltbarkeit erfüllt.

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Stroth, Gernot:
Algebra : Einführung in die Galoistheorie / Gernot Stroth. - Berlin; New York : de Gruyter, 1998
(De-Gruyter-Lehrbuch)
ISBN 3-11-015534-6 (Gb.)
ISBN 3-11-015533-8 (brosch.)

© Copyright 1998 by Walter de Gruyter GmbH & Co., D-10785 Berlin.

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Printed in Germany.
Konvertierung von LaTeX-Dateien des Autors: I. Zimmermann, Freiburg.
Druck und Bindung: WB-Druck GmbH & Co., Rieden/Allgäu.

Für Natascha, Kerstin und Nicole

Vorwort

Der vorliegende Text ist aus meiner Vorlesung Algebra I/II, die ich mehrmals an der Freien Universität Berlin und dann im akademischen Jahr 1994/95 an der Martin-Luther-Universität Halle-Wittenberg gehalten habe, hervorgegangen. Die Vorlesung richtete sich an Studenten im dritten Fachsemester. Vorausgegangen war eine Vorlesung „Lineare Algebra", etwa im Umfang meines Buches Lineare Algebra, Heldermann 1995, in der die Begriffe Ring, Körper und Gruppe einführend behandelt wurden, so daß hier bereits einige Kenntnisse vorausgesetzt werden konnten. Die relevanten Tatsachen werden jedoch (ohne Beweis) im vorliegenden Buch kurz angegeben. In der Vorlesung Algebra I wurde der Standardstoff, Kapitel 1–9 dieses Buches, behandelt. Im Gegensatz zu den meisten Büchern über Algebra, in denen die Begriffe Gruppe, Ring, Körper als eigenständige Gebiete vorgestellt werden, ist das Ziel dieses Buches, eine Darstellung der Galoistheorie von Polynomgleichungen zu geben. Alles ordnet sich diesem Ziel unter. So werden Ringe und Gruppen nur soweit behandelt, wie es für die Entwicklung der Galoistheorie notwendig ist.

Der Name Algebra ist arabischer Herkunft und bedeutet in etwa „Lösung von Gleichungen". Dies ist auch der Gegenstand dieses Buches. In der Schule lernt man, wie man die Lösungen von $3x^2 - 13x - 10 = 0$ findet. Die Gleichung $ax^2 + bx + c = 0$ hat die Wurzeln

$$r_1, r_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Das liefert dann für obige Gleichung $r_1, r_2 = 5, -2/3$.

Das Hauptanliegen dieses Buches ist die Beschäftigung mit Polynomgleichungen und ihren Lösungen. Schon die Babylonier (1600 v. Chr.) besaßen Methoden, quadratische Gleichungen zu lösen. Ca. 100 n. Chr. wurden die ersten algebraischen Formeln für quadratische Polynome gefunden. Geometrische Lösungen für die Gleichungen dritten Grades waren auch bekannt, algebraische Formeln aber bis 1500 völlig unbekannt. Die Mathematiker der Renaissance in Bologna teilten kubische Gleichungen in drei Grundtypen ein

$$x^3 + px = q, \quad x^3 = px + q, \quad x^3 + q = px.$$

Man beachte, daß die Existenz negativer Zahlen noch nicht akzeptiert wurde. Diese Gleichungen wurden von Ferro gelöst. Die heute übliche Formel stammt von Tartaglia (1535), der seine Methode in einem öffentlichen Wettkampf der Methode von Fior, einem Studenten von Ferro, gegenüber stellte und ihre Überlegenheit demonstrierte. Allerdings hielt er seine Methode, wie damals durchaus üblich, geheim, hat sie jedoch später Cardano mitgeteilt, wobei dieser versprechen mußte, sie nicht weiterzugeben. Dieser hielt sich nicht daran, sondern veröffentlichte 1545

ein Buch, in dem sich unter anderem auch die Lösungsformeln der Gleichungen dritten Grades befanden. Weiter enthielt das Buch die auf Ferrari, einen Schüler von Cardano, zurückgehende Methode, eine Gleichung vierten Grades zu lösen, indem man sie auf eine kubische Gleichung zurückführt. Alle Formeln hatten eine seltsame gemeinsame Eigenschaft. Man erhält z. B. für die Gleichung $x^3 + px = q$

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

Dieser Ausdruck ist aus den Koeffizienten der Gleichung aufgebaut, wobei nur Addition, Subtraktion, Multiplikation, Division und Wurzelziehen vorkommen.

Solche Ausdrücke nennt man Radikale. Da alle Gleichungen vom Grad höchstens vier nun durch Radikale gelöst waren, war es natürlich zu fragen, ob dies auch für die Gleichung 5. Grades möglich ist. Viele Mathematiker versuchten sich an diesem Problem. Euler fand z. B. viele neue Methoden. Um 1770 war es Lagrange, der einen wesentlichen Schritt vorwärts machte. Er untersuchte systematisch die verschiedenen Tricks, die zu den Formeln für die Gleichungen vom Grad ≤ 4 führten, und zeigte, daß diese alle im wesentlichen darauf beruhten, geeignete Funktionen in den Wurzeln zu finden, die unter gewissen Permutationen der Wurzeln invariant sind. Er zeigte weiter, daß dieses Verfahren für die Gleichung fünften Grades scheitern muß. Somit hatte man nach Lagrange die Vermutung, daß die Lösung der allgemeinen Gleichung 5. Grades durch Radikalausdrücke nicht möglich ist. Im Jahre 1813 lieferte Ruffini einen Beweis, der allerdings einige Lücken hatte. Dies lag hauptsächlich daran, daß Ruffini keine mathematisch strenge Definition der Lösbarkeit durch Radikalausdrücke hatte. Die Nichtlösbarkeit der allgemeinen Gleichung 5. Grades wurde schließlich von Abel 1824 bewiesen. Nun ergab sich natürlich die Frage, welche Gleichungen sind durch Radikale lösbar. Abel arbeitete hieran, starb aber 1829. Die Lösung dieses Problems durch Galois 1832 ist dann auch der Hauptgegenstand dieses Buches. Die eigentliche revolutionäre Idee Galois war die folgende: Sei f ein Polynom mit rationalen Koeffizienten und $x_1, \ldots, x_n$ die Nullstellen. Sei $K = \mathbb{Q}(x_1, \ldots, x_n)$ der kleinste Teilkörper von $\mathbb{C}$, der alle Nullstellen enthält, so muß man K untersuchen, wenn man etwas über f erfahren will. Dem Körper K wird eine gewisse Gruppe G von Automorphismen zugeordnet, die sogenannte Galoisgruppe. Wir betrachten z. B. die Gleichung $x^4 - 5x^2 + 6 = 0$. Die Nullstellen in $\mathbb{C}$ sind $\alpha = \sqrt{2}$, $\beta = -\sqrt{2}$, $\gamma = \sqrt{3}$ und $\delta = -\sqrt{3}$. Es gehören die Paare α, β und γ, δ jeweils irgendwie zusammen. Wir können α und β von γ und δ unterscheiden, indem wir nur Gleichungen mit rationalen Koeffizienten benutzen. Es sind α und β Nullstellen von $x^2 - 2$ aber γ und δ nicht. Zwar besteht auch ein Unterschied zwischen α und β, aber der Vorzeichenwechsel ist nicht mit rationalen Polynomen zu entdecken. Nun gibt es genau vier Anordnungen der Wurzeln, so daß alle in der ersten Anordnung richtigen rationalen Gleichungen in jeder

Anordnung richtig bleiben: $\alpha\beta\gamma\delta$ $|\alpha\beta\delta\gamma$ $|\beta\alpha\gamma\delta$ $|\beta\alpha\delta\gamma$. Die Permutationsgruppe dieser vier Anordnungen ist genau die Galoisgruppe. Galois zeigte, daß sich viele wesentliche Eigenschaften von f in der Gruppe G widerspiegeln, so z. B. die Frage nach der Lösbarkeit durch Radikale. Dabei entdeckte er, daß es in Gruppen G ausgezeichnete Untergruppen N gibt, die sogenannten Normalteiler. Zu diesen gehören dann Zwischenkörper $\mathbb{Q} \subseteq K_1 \subseteq K$, die genauso wie K gebildet sind. Damit ist die Tür zur Induktion aufgestoßen. Das Hauptresultat von Galois ist, daß f genau dann eine Radikalformel für die Wurzeln besitzt, falls es eine Kette $1 = N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_k = G$ gibt, so daß N_{i+1}/N_i kommutativ ist. Bedeutend ist hierbei, daß das Kriterium nicht irdendeine Formel in den Koeffizienten des Polynoms f ist. Um die Frage nach der Auflösbarkeit durch Radikalausdrücke beantworten zu können, muß eine neue Struktur, die Gruppe, eingeführt werden. Das Kriterium ist dann in der Sprache dieser neuen Theorie.

Galois Entdeckung des Normalteilers und die Entwicklung der Galoistheorie war der eigentliche Anfang der Algebra, deren Axiomatisierung bis in die 30er Jahre dieses Jahrhunderts reicht.

Der Weg zu diesem Resultat wird lang sein. Wir müssen uns zunächst in §1 mit Polynomen beschäftigen. Dazu werden wir etwas allgemeinere Strukturen, die Ringe, betrachten. Für eine gewisse Klasse, euklidische Ringe, Hauptidealringe, zu denen dann auch die Polynomringe gehören, werden wir eine Teilbarkeitstheorie entwickeln.

Als nächstes müssen wir uns die Körper näher ansehen. Das heißt, wir müssen uns mit der Frage beschäftigen, wie wir überhaupt zu obigem Körper K kommen (§2, §3). Wir werden algebraische Erweiterungen von Körpern und Zerfällungskörper von Polynomen betrachten. Weiter werden wir die Existenz algebraisch abgeschlossener Körper beweisen.

In §5 müssen wir die Gruppentheorie soweit entwickeln, daß wir unsere Probleme wirklich mit Hilfe dieser Theorie lösen können. Insbesondere werden wir uns mit auflösbaren Gruppen beschäftigen, und zeigen, daß die symmetrische Gruppe vom Grad mindestens 5 nicht auflösbar ist. Dies ist der eigentliche Grund für die Nichtexistenz von Auflösungsformeln obiger Art für Gleichungen vom Grad größer als vier. Darüber hinaus werden wir den wichtigsten Satz der endlichen Gruppentheorie, den Sylowsatz, beweisen.

In §6 werden wir dann die eigentliche Galoistheorie entwickeln, die den Zusammenhang zwischen den Zwischenkörpern und der Automorphismengruppe einer Körpererweiterung zum Gegenstand hat. Die Galoistheorie wird hier als Teilgebiet der Körpertheorie, also ohne Verbindung zu den Polynomen, vorgestellt. Diese Verbindung wird dann später in §7 und §8 hergestellt. Hier wird gezeigt, daß der Zerfällungskörper eines separablen Polynoms stets galoissch ist, d. h. hierauf ist die in §6 entwickelte Theorie anwendbar.

Das Ziel dieses Buches ist, zu zeigen, was hinter den klassischen Problemen, wie Lösbarkeit von Gleichungen (§9, §12) und Konstruktion mit Zirkel und Lineal steckt (§4, §10). Darüber hinaus kann man sehen wie verschiedene Zweige der Mathematik zusammenarbeiten, um ein Problem zu lösen. Wir werden die bis hierher entwickelte Theorie anwenden, um das eingangs angedeutete Kriterium zur Auflösbarkeit von Polynomgleichungen durch Radikalausdrücke herzuleiten. Weiter werden wir die klassischen Konstruktionsaufgaben, Dreiteilung des Winkels, Quadratur des Kreises, Verdoppelung des Würfels und Konstruktion des regelmäßigen n-Ecks behandeln.

Neben der reinen Entwicklung der Theorie wollen wir uns auch mit praktischen Fragen beschäftigen. Diese werden im zweiten Teil des Buches im Vordergrund stehen. So wollen wir uns in §11 mit einer interessanten Klasse von Polynomen, den Kreisteilungspolynomen beschäftigen. Neben der Frage nach Irreduzibilität wird hier auch die Frage nach Methoden zur Berechnung dieser Polynome beantwortet. Wir werden die Resultate über Kreisteilungspolynome anwenden, um drei klassische Sätze, den Satz von Zsigmondy über die Existenz von primitiven Primzahlen, den Satz von Dirichlet über Primzahlen in arithmetischer Progression und den Satz von Wedderburn über die Nichtexistenz endlicher Schiefkörper zu beweisen.

Viele praktische Fragen beruhen darauf, daß wir Polynome in irreduzible faktorisieren können, bzw. den größten gemeinsamen Teiler von Polynomen berechnen können. Hierzu werden in §15 und §16 Algorithmen entwickelt. Der notwendige theoretische Unterbau, der aus der Bewertungstheorie kommt, und mit dem Hensel'schen Lemma endet, wird in §14 bereitgestellt. Dabei ist auch hier wieder nicht an eine Einführung in die Bewertungstheorie gedacht. Es soll nur der später vorgestellte Hensel-Algorithmus motiviert werden.

Das Buch endet in §17 mit Methoden zur Berechnung von Galoisgruppen. Zunächst werden die bekannten Formeln für die Gleichung vom Grad höchstens 4 hergeleitet. Danach werden zwei Algorithmen zur Berechnung von Galoisgruppen von Polynomen mit ganzzahligen Koeffizienten vorgestellt. Da diese sehr viel Information über die symmetrischen Gruppen voraussetzten, ist klar, daß sie nur bis zu kleinen Graden eingesetzt werden können. Auf welchen Ideen allgemeine Algorithmen beruhen könnten, wird am Ende dieses Paragraphen kurz skizziert.

Auch das sog. Umkehrproblem der Galoistheorie wird kurz angesprochen. So werden in §13 die abelschen Gruppen und in §17 die symmetrischen Gruppen als Galoisgruppen über $\mathbb{Q}$ realisiert. Auch wird als Beispiel die Gruppe $AG(3, 2)$, eine Erweiterung einer Gruppe der Ordnung 8 mit $GL(3, 2)$, als Galoisgruppe eines Polynoms vom Grad 8 realisiert.

In einem Anhang haben wir zwei Gegenstände aufgenommen, die nicht für das Erreichen der in diesem Buch gestellten Ziele notwendig sind, aber doch in ein

Algebra Lehrbuch gehören, den Beweis der Transzendenz von e und π und den Beweis der algebraischen Abgeschlossenheit von $\mathbb{C}$.

Zum Ende noch ein paar Worte zu der Person Evariste Galois. Er wurde 1811 geboren und starb 1832 nach einem Duell. Mit 15 Jahren publizierte er bereits seine ersten Arbeiten. Genauso revolutionär wie im politischen war er auch im mathematischen Denken. Insofern hatte er es schwer von seinen Zeitgenossen verstanden zu werden. Seine erste Arbeit auf dem Gebiet der Auflösbarkeit von Polynomgleichungen reichte Galois 1829 bei der Akademie der Wissenschaften in Paris ein. Sein Referent war Cauchy, der sich damals auch mit der Auflösbarkeit von Polynomgleichungen befaßte. Cauchy lehnte diese Arbeit und eine acht Tage später zum gleichen Thema eingereichte Arbeit ab. Die Manuskripte sind nie gefunden worden. Auch eine 1830 anläßlich des Wettbewerbs „Großer Preis der Mathematik" eingereichte Arbeit ist verschollen. Im Jahre 1831 sandte Galois zum letzten Mal eine Arbeit an die Akademie. Da Cauchy nicht in Paris war, wurden Poisson und Lacroix zu Gutachtern bestellt. Beide waren allerdings mehr an Physik als an Algebra interessiert. So lehnten sie nach 5 Monaten die Arbeit mit der Begründung ab, daß sie sie nicht verstehen und ihre Bedeutung auch nicht sehen. Das Werk Galois wurde also von seinen Zeitgenossen weder verstanden noch gewürdigt. Es wäre wohl verlorengegangen, wenn er nicht am Vorabend seines Duells seine Resultate in einem Brief an seinen Freund Auguste Chevalier zusammengefaßt hätte. Es dauerte bis 1846 bis sein Nachlaß herausgegeben wurde. Äußerer Anlaß waren Arbeiten von Cauchy zur Gleichungstheorie, die sich aber im althergebrachten Rahmen bewegten. Liouville erkannte nun die wesentliche Bedeutung der Galois'schen Arbeiten und gab sie 1846 heraus. Für weitere Informationen zu diesem Themenkreis sei auf die Biographie „Evariste Galois 1811–1832" von Laura Toti Rigatelli, Birkhäuser 1996, verwiesen.

Abschließend danke ich noch allen, die das Entstehen dieses Buches über die Jahre kritisch begleitet haben. Mein besonderer Dank geht an die Studenten meiner Vorlesung 1996/97, die mich bei der Fehlersuche unterstützt haben, und an Herrn Dr. S. Heiss, der große Teile des Manuskripts gelesen und Verbesserungsvorschläge gemacht hat.

Halle, im Januar 1998 *Gernot Stroth*

Inhaltsverzeichnis

§1 Ringe 1

§2 Körpererweiterungen 37

§3 Algebraische Erweiterungen 43

§4 Konstruktionen mit Zirkel und Lineal 59

§5 Gruppen 66

§6 Galoistheorie 99

§7 Normale Erweiterungen 118

§8 Separable Erweiterungen 125

§9 Radikalerweiterungen 134

§10 Regelmäßige n-Ecke 143

§11 Kreisteilungsköper 154

§12 Norm und Spur 178

§13 Abelsche Erweiterungen von $\mathbb{Q}$ 184

§14 p-adische Zahlen 189

§15 Der größte gemeinsame Teiler 206

§16 Faktorisierung von Polynomen 217

§17 Galoisgruppen 236

Anhang

§A1 Der Körper der komplexen Zahlen 271

§A2 Transzendenz von e und π 276

Literatur 281

Index 283

§1 Ringe

Dieser Paragraph soll die Grundlagen für die späteren Untersuchungen im Rahmen der Galoistheorie legen. Wir werden uns deshalb im wesentlichen nur mit den Polynomringen beschäftigen. Für diese soll eine Teilbarkeitstheorie entwickelt werden, die parallel zu der Teilbarkeitstheorie in $\mathbb{Z}$ ist. Dabei werden wir sehen, daß beide Ringe nur Spezialfälle von größeren Klassen von Ringen, den euklidischen Ringen bzw. den Hauptidealringen, sind. Insbesondere die beiden letzten Klassen von Ringen spielen in der Zahlentheorie eine wichtige Rolle, auf die wir aber im Rahmen dieses Buches nicht eingehen können. Eine Andeutung dieses Zusammenhangs wird in (1.29) gegeben.

Wir setzen voraus, daß der Leser mit den einfachsten Definitionen und Resultaten der Ringtheorie vertraut ist, wiederholen aber noch einmal die notwendigen Definitionen.

(1.1) Definition. Sei $\mathcal{R}$ eine Menge mit zwei Verknüpfungen $+, \cdot$. Bezüglich $+$ sei $\mathcal{R}$ eine kommutative Gruppe. Weiter gelte:

(1) $a(bc) = (ab)c$ für alle $a, b, c \in \mathcal{R}$.

(2) $a(b + c) = ab + ac$ für alle $a, b, c \in \mathcal{R}$.

(3) $(a + b)c = ac + bc$ für alle $a, b, c \in \mathcal{R}$.

(4) Es gibt ein Element $1 \in \mathcal{R}$ mit $1a = a1 = a$ für alle $a \in \mathcal{R}$.

Dann nennen wir $\mathcal{R}$ einen Ring. Ist $ab = ba$ für alle $a, b \in \mathcal{R}$, so heißt $\mathcal{R}$ kommutativ. Ein kommutativer Ring, in dem $(\mathcal{R} \setminus \{0\}, \cdot)$ eine Gruppe ist, heißt Körper.

(1.2) Definition. Sei $\mathcal{R}$ ein Ring und $\mathfrak{i} \subseteq \mathcal{R}$. Es sei $(\mathfrak{i}, +)$ eine Untergruppe von $(\mathcal{R}, +)$ und $a\mathfrak{i} \in \mathfrak{i}$ für alle $a \in \mathcal{R}$ und $i \in \mathfrak{i}$. Dann heißt $\mathfrak{i}$ ein Linksideal in $\mathcal{R}$. Entsprechend wird Rechtsideal definiert. Ist $\mathfrak{i}$ Linksideal und Rechtsideal, so heißt $\mathfrak{i}$ 2-seitig.

Ist aus dem Zusammenhang klar, ob es sich um ein Links- oder Rechtsideal handelt, bzw. falls dies keine Rolle spielt, so werden wir einfach von einem Ideal sprechen.

(1.3) Beispiel. (a) Sei $\mathcal{R} = \mathbb{Z}$ und $\mathfrak{i} = 2\mathbb{Z} = \{n \mid n \in \mathbb{Z},\ n \text{ gerade}\}$. Dann ist $\mathfrak{i}$ ein Ideal. Wir werden später sehen, daß alle Ideale von $\mathbb{Z}$ ähnlich wie $\mathfrak{i}$ aussehen, also aus den Vielfachen eines festen Elementes aus $\mathbb{Z}$ bestehen.

(b) Sei $\mathcal{R} = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{R}\right\}$ der Ring der 2×2-Matrizen über $\mathbb{R}$. Setze

$$\mathfrak{i} = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R}\right\}.$$

Es ist $\left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right) = \left(\begin{smallmatrix} xa+zb & ya+tb \\ 0 & 0 \end{smallmatrix}\right) \in \mathfrak{i}$ für alle $\left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right) \in \mathcal{R}$.

Somit ist $\mathfrak{i}$ ein Rechtsideal. Es ist aber kein Linksideal, da

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \notin \mathfrak{i}$$

ist. Also sind die Begriffe Links- und Rechtsideal verschieden.

(1.4) Definition. Sei $\mathcal{R}$ ein Ring, und sei $\mathfrak{i}$ ein 2-seitiges Ideal in $\mathcal{R}$. Setze $\mathcal{R}/\mathfrak{i} = \{a + \mathfrak{i} \mid a \in \mathcal{R}\}$. Auf $\mathcal{R}/\mathfrak{i}$ definiere eine Addition und Multiplikation durch

$$\begin{aligned} (a + \mathfrak{i}) + (b + \mathfrak{i}) &= (a + b) + \mathfrak{i} \\ (a + \mathfrak{i})(b + \mathfrak{i}) &= ab + \mathfrak{i}. \end{aligned}$$

Wir nennen $\mathcal{R}/\mathfrak{i}$ mit dieser Addition und Multiplikation den Faktorring von $\mathcal{R}$ nach $\mathfrak{i}$.

Daß die Bezeichnung „Ring" für $\mathcal{R}/\mathfrak{i}$ gerechtfertigt ist, zeigt der folgende Satz, dessen Beweis wir dem Leser überlassen.

(1.5) Satz. *Sei $\mathcal{R}$ ein Ring, $\mathfrak{i}$ ein 2-seitiges Ideal in $\mathcal{R}$. Dann ist $\mathcal{R}/\mathfrak{i}$ ein Ring.*

(1.6) Definition. Seien $\mathcal{R}_1$ und $\mathcal{R}_2$ zwei Ringe.

(a) Eine Abbildung $f : \mathcal{R}_1 \to \mathcal{R}_2$ heißt (Ring) Homomorphismus, falls

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad \text{und} \quad \varphi(ab) = \varphi(a)\varphi(b)$$

für alle $a, b \in \mathcal{R}_1$ gilt.

Ein surjektiver, injektiver, bijektiver Homomorphismus heißt Epimorphismus, Monomorphismus bzw. Isomorphismus. Gibt es einen Isomorphismus zwischen $\mathcal{R}_1$ und $\mathcal{R}_2$, so schreibe

$$\mathcal{R}_1 \cong \mathcal{R}_2.$$

(b) Sei $\varphi : \mathcal{R}_1 \to \mathcal{R}_2$ ein Homomorphismus. Setze

$$\operatorname{Ker} \varphi = \{a \mid a \in \mathcal{R}_1, \varphi(a) = 0\}.$$

Wir nennen $\operatorname{Ker} \varphi$ den Kern von φ.

(1.7) Satz. *Seien $\mathcal{R}_1$ und $\mathcal{R}_2$ zwei Ringe und $\varphi : \mathcal{R}_1 \to \mathcal{R}_2$ ein Homomorphismus. Dann ist* $\operatorname{Ker}\varphi$ *ein 2-seitiges Ideal in $\mathcal{R}_1$ und*

$$\mathcal{R}_1/\operatorname{Ker}\varphi \cong \operatorname{Bild}\varphi.$$

Beweis. Offenbar ist $\operatorname{Ker}\varphi$ eine Untergruppe von $\mathcal{R}_1$ bezüglich $+$. Sei nun $a \in \mathcal{R}_1$ und $b \in \operatorname{Ker}\varphi$. Dann ist

$$\varphi(ab) = \varphi(a)\varphi(b) = 0 = \varphi(b)\varphi(a) = \varphi(ba).$$

Also sind ab und ba in $\operatorname{Ker}\varphi$, d. h. $\operatorname{Ker}\varphi$ ist ein 2-seitiges Ideal.

Definiere $\psi : \operatorname{Bild}\varphi \to \mathcal{R}_1/\operatorname{Ker}\varphi$ durch

$$\psi(\varphi(a)) = a + \operatorname{Ker}\varphi.$$

Da ψ durch die Wahl eines Urbildes von $\varphi(a)$ definiert wurde, ist zunächst zu zeigen, daß ψ wohldefiniert ist. Sei dazu $\varphi(a) = \varphi(b)$. Dann ist $a - b \in \operatorname{Ker}\varphi$, also ist $a + \operatorname{Ker}\varphi = b + \operatorname{Ker}\varphi$. Somit ist ψ wohldefiniert.

Wir zeigen nun zuerst, daß ψ ein Homomorphismus ist. Wir wählen dazu Elemente $\varphi(a), \varphi(b) \in \operatorname{Bild}\varphi$. Dann ist

$$\begin{aligned}\psi(\varphi(a) + \varphi(b)) &= \psi(\varphi(a+b)) = (a+b) + \operatorname{Ker}\varphi = (a + \operatorname{Ker}\varphi) + (b + \operatorname{Ker}\varphi)\\ &= \psi(\varphi(a)) + \psi(\varphi(b))\end{aligned}$$

und

$$\begin{aligned}\psi(\varphi(a)\varphi(b)) &= \psi(\varphi(ab)) = (ab) + \operatorname{Ker}\varphi = (a + \operatorname{Ker}\varphi)(b + \operatorname{Ker}\varphi)\\ &= \psi(\varphi(a))\psi(\varphi(b)).\end{aligned}$$

Also ist ψ ein Homomorphismus.

Sei $a \in \mathcal{R}_1$. Dann ist $\psi(\varphi(a)) = a + \operatorname{Ker}\varphi$, also ist ψ ein Epimorphismus.

Sei $\psi(\varphi(a)) = \operatorname{Ker}\varphi$. Dann ist $a \in \operatorname{Ker}\varphi$, also $\varphi(a) = 0$. Somit ist ψ ein Monomorphismus. □

Eine wichtige Folgerung aus (1.7), die wir häufig benutzen werden, ist, daß für ein 2-seitiges Ideal $\mathfrak{i}$ jedes Ideal von $\mathcal{R}/\mathfrak{i}$ Bild eines Ideales von $\mathcal{R}$, das oberhalb von $\mathfrak{i}$ liegt, ist, und umgekehrt.

Der folgende Satz gibt eine idealtheoretische Kennzeichnung der Körper in der Klasse der Ringe.

(1.8) Satz. *Ein kommutativer Ring $\mathcal{R}$ mit mindestens zwei Elementen ist genau dann ein Körper, wenn er keine Ideale ungleich* $\{0\}$ *und $\mathcal{R}$ enthält.*

Beweis. Es habe $\mathcal{R}$ nur die Ideale $\{0\}$ und $\mathcal{R}$. Wir zeigen zunächst, daß jedes Element von $\mathcal{R} \setminus \{0\}$ invertierbar ist.

Sei $0 \neq a \in \mathcal{R}$. Betrachte die Menge

$$a\mathcal{R} = \{ar \mid r \in \mathcal{R}\}.$$

Wir zeigen, daß $a\mathcal{R}$ ein Ideal ist.

Sind $ar_1, ar_2 \in a\mathcal{R}$, so ist $ar_1 + ar_2 = a(r_1 + r_2) \in a\mathcal{R}$. Ist $b \in \mathcal{R}$ und $ar \in a\mathcal{R}$, so ist $(ar)b = a(rb) \in a\mathcal{R}$. Damit ist $a\mathcal{R}$ ein Ideal.

Da $a = a \cdot 1 \in a\mathcal{R}$ ist, ist $a\mathcal{R} \neq \{0\}$. Nach Annahme ist somit $a\mathcal{R} = \mathcal{R}$. Dann ist aber $1 \in a\mathcal{R}$, d. h. es gibt ein $b \in \mathcal{R}$ mit $1 = ab$, was liefert, daß a invertierbar ist.

Um zu zeigen, daß $\mathcal{R} \setminus \{0\}$ eine Gruppe ist, müssen wir noch zeigen, daß $\mathcal{R} \setminus \{0\}$ multiplikativ abgeschlossen ist. Seien $a, b \in \mathcal{R} \setminus \{0\}$ mit $ab = 0$. Wie bereits bewiesen gibt es ein $c \in \mathcal{R}$ mit $bc = 1$. Somit ist

$$a = a \cdot 1 = a(bc) = (ab)c = 0 \cdot c = 0.$$

Dies ist ein Widerspruch. Da $|\mathcal{R}| \geq 2$ ist, ist $\mathcal{R} \setminus \{0\} \neq \emptyset$ und somit eine Gruppe. Insbesondere haben wir, daß $\mathcal{R}$ ein Körper ist.

Sei nun umgekehrt $\mathcal{R}$ ein Körper und $\mathfrak{i}$ ein Ideal, $\mathfrak{i} \neq \{0\}$. Wähle ein Element $a \neq 0$ in $\mathfrak{i}$. Dann gibt es ein $b \in \mathcal{R}$ mit $ab = 1$. Also ist $1 \in \mathfrak{i}$. Sei nun $r \in \mathcal{R}$ beliebig. Dann ist $r = 1 \cdot r \in \mathfrak{i}$, d. h. $\mathcal{R} = \mathfrak{i}$. □

(1.9) Bemerkung. (1) $|\mathcal{R}| \geq 2$ ist notwendig in (1.8), da in einem Körper $0 \neq 1$ gilt, in einem Ring nicht. Der Ring $\mathcal{R} = \{0\}$ erfüllt alle Voraussetzungen, ist aber kein Körper!

(2) Eine wichtige Anwendung von (1.8), die wir später häufig benutzen werden, ist die folgende.

Seien K_1, K_2 zwei Körper und $\varphi : K_1 \to K_2$ ein Homomorphismus. Da nach (1.7) $\operatorname{Ker} \varphi$ ein Ideal in K_1 ist, ist nach (1.8) entweder $\operatorname{Ker} \varphi = K_1$ oder $\operatorname{Ker} \varphi = 0$. Also ist φ entweder die Nullabbildung oder ein Monomorphismus.

Wir wollen das Wesentliche der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$ herausarbeiten, um es dann auf eine größere Klasse von Ringen verallgemeinern zu können. Eine der wesentlichen Eigenschaften von $\mathbb{Z}$ ist, daß aus $a \neq 0 \neq b$ stets $ab \neq 0$ folgt, was z. B. in $\mathbb{Z}/6\mathbb{Z}$ nicht mehr richtig ist. Dies führt zunächst zu folgender Definition.

(1.10) Definition. Sei $\mathcal{R}$ ein kommutativer Ring.

(a) Ein Element $0 \neq a \in \mathcal{R}$ heißt Nullteiler, falls es ein $0 \neq b \in \mathcal{R}$ mit $ab = 0$ gibt.

(b) Enthält $\mathcal{R}$ keine Nullteiler, so heißt $\mathcal{R}$ ein Integritätsbereich.

(c) Ein Ideal $\mathfrak{p} \neq \mathcal{R}$ von $\mathcal{R}$ heißt Primideal, falls $\mathcal{R}/\mathfrak{p}$ ein Integritätsbereich ist.

(1.11) Beispiele. (1) $\mathbb{Z}$ ist Integritätsbereich.

(2) Ist p Primzahl, so ist $p\mathbb{Z}$ Primideal in $\mathbb{Z}$. Dies motiviert die Bezeichnung Primideal nachträglich. Sei $(a + p\mathbb{Z})(b + p\mathbb{Z}) = 0 + p\mathbb{Z}$, so ist $ab \in p\mathbb{Z}$. Also ist $ab = pr$ mit geeignetem $r \in \mathbb{Z}$. Da p Primzahl ist, ist p ein Teiler von a oder b. Wir können annehmen, daß a von p geteilt wird. Dann ist $a = pt \in p\mathbb{Z}$. Also ist $a + p\mathbb{Z} = pt + p\mathbb{Z} = p\mathbb{Z}$.

(3) Sei $\mathcal{R} = \mathbb{Z}/4\mathbb{Z} = \{1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}, 4\mathbb{Z}\}$.

Es ist $2 + 4\mathbb{Z} \neq 4\mathbb{Z}$ aber $(2 + 4\mathbb{Z})(2 + 4\mathbb{Z}) = 4 + 4\mathbb{Z} = 4\mathbb{Z}$. Also ist $4\mathbb{Z}$ kein Primideal in $\mathbb{Z}$.

(4) Wir wollen zeigen, daß $n\mathbb{Z}$, $n > 0$, genau dann ein Primideal ist, falls n eine Primzahl ist. Ist n eine Primzahl, so folgt die Behauptung mit (2).

Sei nun n keine Primzahl. Dann gibt es $a > 1 < b$ mit $n = ab$. Also ist

$$n\mathbb{Z} = (a + n\mathbb{Z})(b + n\mathbb{Z}) \quad \text{mit } a + n\mathbb{Z} \neq n\mathbb{Z} \neq b + n\mathbb{Z}.$$

Damit ist $n\mathbb{Z}$ kein Primideal. Wir werden später sehen, daß die $n\mathbb{Z}$ und $\{0\}$ sämtliche Ideale von $\mathbb{Z}$ sind. Die Primideale $\neq 0$, sind somit genau die Ideale $p\mathbb{Z}$ mit p Primzahl.

Die Eigenschaft von Primzahlen p in $\mathbb{Z}$, daß, wenn p ein Produkt teilt, es auch einen der Faktoren teilen muß, überträgt sich auf Primideale, wie der folgende Satz zeigt.

(1.12) Satz. *Sei $\mathcal{R}$ ein kommutativer Ring, $\mathfrak{i} \neq \mathcal{R}$ ein Ideal. Dann ist $\mathfrak{i}$ genau dann ein Primideal, falls aus $ab \in \mathfrak{i}$ mit $a, b \in \mathcal{R}$ stets $a \in \mathfrak{i}$ oder $b \in \mathfrak{i}$ folgt.*

Beweis. (a) Sei $\mathfrak{i}$ Primideal und $ab \in \mathfrak{i}$. Dann ist $\mathfrak{i} = ab + \mathfrak{i} = (a + \mathfrak{i})(b + \mathfrak{i})$. Da $\mathcal{R}/\mathfrak{i}$ ein Integritätsbereich ist, folgt $a + \mathfrak{i} = \mathfrak{i}$ oder $b + \mathfrak{i} = \mathfrak{i}$, d. h. $a \in \mathfrak{i}$ oder $b \in \mathfrak{i}$.

(b) Sei $(a + \mathfrak{i})(b + \mathfrak{i}) = \mathfrak{i}$. So ist $ab \in \mathfrak{i}$, und nach Voraussetzung ist $a \in \mathfrak{i}$ oder $b \in \mathfrak{i}$. Also ist $a + \mathfrak{i} = \mathfrak{i}$ oder $b + \mathfrak{i} = \mathfrak{i}$, und $\mathcal{R}/\mathfrak{i}$ ist ein Integritätsbereich. □

(1.13) Definition. Sei $\mathcal{R}$ ein Ring. Ein (Rechts-, Links-)Ideal $\mathfrak{m} \neq \mathcal{R}$ nennen wir maximal, falls für jedes (Rechts-, Links-)Ideal $\mathfrak{n}$ von $\mathcal{R}$ mit $\mathfrak{m} \subseteq \mathfrak{n} \neq \mathcal{R}$ stets $\mathfrak{m} = \mathfrak{n}$ folgt.

Um die Existenz maximaler Ideale in Ringen zu zeigen, benötigen wir ein mengentheoretisches Hilfsmittel, das wir auch an späterer Stelle noch einsetzen werden.

Sei $\mathcal{M}$ eine Menge mit einer Halbordnung $\sqsubset$. Eine Teilmenge $\mathcal{K}$ von $\mathcal{M}$ heißt eine Kette, falls für $a, b \in \mathcal{K}$ stets $a \sqsubset b$ oder $b \sqsubset a$ gilt. Eine Kette $\mathcal{K}$ besitzt eine obere Schranke $m \in \mathcal{M}$, falls $k \sqsubset m$ für alle $k \in \mathcal{K}$ ist. Ein Element $m_0 \in \mathcal{M}$ heißt maximal in $\mathcal{M}$, falls aus $m \in \mathcal{M}$ und $m_0 \sqsubset m$ stets $m = m_0$ folgt. Das angesprochene Hilfsmittel lautet nun wie folgt:

(Lemma von Zorn[1]): *Sei $\mathcal{M}$ eine nicht leere halbgeordnete Menge. Hat jede Kette $\mathcal{K}$ von $\mathcal{M}$ eine obere Schranke in $\mathcal{M}$, so gibt es wenigstens ein maximales Element in $\mathcal{M}$.*[2]

(1.14) Satz. *Sei $\mathcal{R}$ ein Ring.*

(a) *Jedes (Rechts-, Links-) Ideal $\mathfrak{i}$ von $\mathcal{R}$, $\mathfrak{i} \neq \mathcal{R}$, liegt in einem maximalen Ideal.*

(b) *Ist $\mathcal{R}$ kommutativ, so ist jedes maximale Ideal ein Primideal.*

Beweis. (a) Sei $\mathfrak{i}$ ein Ideal. Setze

$$\mathfrak{S} = \{\mathfrak{j} \mid \mathfrak{i} \subseteq \mathfrak{j},\ \mathfrak{j} \neq \mathcal{R},\ \mathfrak{j} \text{ Ideal}\}$$

Da $\mathfrak{i} \in \mathfrak{S}$ ist, ist $\mathfrak{S} \neq \varnothing$. Wir ordnen $\mathfrak{S}$ per Inklusion. Sei $\mathfrak{K}$ eine Kette in $\mathfrak{S}$, d. h. eine vollständig geordnete Teilmenge. Setze

$$\mathfrak{j} = \bigcup_{\mathfrak{k} \in \mathfrak{K}} \mathfrak{k}.$$

Dann ist $\mathfrak{j}$ ein Ideal.

Wir zeigen $\mathfrak{j} \in \mathfrak{S}$. Da $\mathfrak{i} \subseteq \mathfrak{j}$ ist, müssen wir nur $\mathfrak{j} \neq \mathcal{R}$ zeigen. Sei somit $\mathfrak{j} = \mathcal{R}$. Dann ist $1 \in \mathfrak{j}$. Also gibt es ein $\mathfrak{k} \in \mathfrak{K}$ mit $1 \in \mathfrak{k}$, was aber $\mathcal{R} = \mathfrak{k}$ liefert, ein Widerspruch. Somit hat jede Kette in $\mathfrak{S}$ eine obere Schranke. Mit dem Lemma von Zorn folgt nun, daß es ein maximales Element $\mathfrak{m}$ in $\mathfrak{S}$ gibt.

(b) Da $\mathfrak{m}$ ein maximales Ideal ist, ist nach (1.8) $\mathcal{R}/\mathfrak{m}$ ein Körper. Insbesondere ist $\mathcal{R}/\mathfrak{m}$ ein Integritätsbereich und dann $\mathfrak{m}$ ein Primideal. □

Wir wollen die eindeutige Primfaktorzerlegung von $\mathbb{Z}$ in einer größeren Klasse von Ringen beweisen. Dazu müssen wir zunächst den Begriff der Primzahl verallgemeinern. Es gibt zwei Möglichkeiten. Eine Primzahl $p \in \mathbb{Z}$ hat die Eigenschaft,

[1] M. Zorn, *6.6.1906 Hamburg, †9.3.1993 Bloomington, emigrierte 1933 in die USA, Professor in Yale und Indiana University, Bloomington, Arbeitsgebiete Gruppentheorie, Mengenlehre, besondere Berühmtheit erlangte er durch das Zorn'sche Lemma, das sich in „A remark on methods in transfinite algebra", Bull. Amer. Math. Soc. 41 (1935), 667–670 befindet.

[2] Für weitere Informationen bzw. Äquivalenzen zu Axiomen der Mengenlehre siehe P. Halmos, Naive Mengenlehre. Dort kann man in §16 mehr über das Lemma von Zorn erfahren.

daß, wenn sie ein Produkt teilt, sie einen der Faktoren teilt. Sie hat aber auch die Eigenschaft, daß p außer $\pm p$ und ± 1 keine weiteren Teiler hat. Diese letzte Eigenschaft werden wir zur Verallgemeinerung benutzen. Da diese Elemente offenbar nicht mehr zerlegbar sind, wollen wir sie irreduzibel nennen. Die Elemente, die die erste Eigenschaft haben, werden wir prim nennen. In den uns hauptsächlich interessierenden Ringen, den Hauptidealringen, werden wir sehen, daß die irreduziblen Elemente genau die Primelemente sind.

Unsere Definition von irreduzibel hat z. B. in $\mathbb{Z}$ zur Folge, daß mit 2 auch -2 irreduzibel ist. Die besondere Rolle von -1 in $\mathbb{Z}$ soll zunächst herausgearbeitet werden. Es sind offenbar 1 und -1 die beiden einzigen invertierbaren Elemente in $\mathbb{Z}$. In allgemeinen Ringen kann es durchaus mehr invertierbare Elemente e geben. Wir nennen diese Einheiten. Ist dann p irreduzibel, so auch ep. In $\mathbb{Z}$ ist $10 = 2 \cdot 5$ aber auch $10 = (-2) \cdot (-5)$. Dies zeigt, daß wir eine Eindeutigkeit der Primfaktorzerlegung nur modulo Einheiten haben können und führt zu folgender Definition:

(1.15) Definition. Sei $\mathcal{R}$ ein Integritätsbereich.

(a) Sind $a, b \in \mathcal{R}$, so nennen wir a einen Teiler von b, falls es ein $c \in \mathcal{R}$ gibt, so daß $b = ac$ ist. Wir schreiben dann $a \mid b$.

(b) Ein Element $e \in \mathcal{R}$ heißt Einheit, falls $e \mid 1$.

(c) Ein Element $p \in \mathcal{R}$ heißt irreduzibel, falls aus $ab = p$ mit $a, b \in \mathcal{R}$, stets a Einheit oder b Einheit folgt und p selbst keine Einheit ist.

(d) $\mathcal{R}$ heißt ZPE-Ring (Ring mit eindeutiger Primfaktorzerlegung), falls sich jedes $0 \neq a \in \mathcal{R}$ in der Gestalt $ep_1 \dots p_n$ mit einer Einheit e und bis auf Einheiten eindeutig bestimmten irreduziblen Elementen p_i schreiben läßt.

(e) Ein Element $0 \neq p \in \mathcal{R}$, das keine Einheit ist, heißt Primelement, falls aus $p \cdot r = ab$ (d. h. p teilt ab) mit $a, b, r \in \mathcal{R}$, stets $a = p \cdot s$ oder $b = p \cdot s$ ($s \in \mathcal{R}$ geeignet) folgt.

Die Primelemente sind immer auch irreduzibel, wie wir jetzt zeigen werden.

(1.16) Lemma. *Sei $\mathcal{R}$ ein Integritätsbereich und p ein Primelement. Dann ist p irreduzibel.*

Beweis. Sei $p = ab$ mit $a, b \in \mathcal{R}$. Dann können wir $a = ps$ für geeignetes $s \in \mathcal{R}$ annehmen. Also ist $p = psb$. Das liefert $p(1-sb) = 0$. Da $\mathcal{R}$ ein Integritätsbereich ist, folgt $sb = 1$, d. h. b ist eine Einheit. Somit ist p irreduzibel. □

Irreduzible Elemente müssen im allgemeinen nicht prim sein, wie wir in (1.18) sehen werden. In den uns interessierenden Ringen wird das allerdings so sein.

(1.17) Lemma. *Sei $\mathcal{R}$ ein Integritätsbereich und $0 \neq p\mathcal{R}$ ein Primideal in $\mathcal{R}$. Dann ist p irreduzibel.*

Beweis. Sei $ab = p$ mit $a, b \in \mathcal{R}$. Dann ist $ab \in p\mathcal{R}$. Nach (1.12) ist $a \in p\mathcal{R}$ oder $b \in p\mathcal{R}$. Sei ohne Beschränkung $a \in p\mathcal{R}$. Dann ist $a = px$ mit $x \in \mathcal{R}$, was $p = pxb$ und dann $p(1 - xb) = 0$ liefert. Da $p \neq 0$ ist, folgt $1 = xb$, womit b eine Einheit ist. Da $p\mathcal{R} \neq \mathcal{R}$ ist nach Definition des Primideals, ist p keine Einheit. □

(1.18) Beispiel. (a) Die Umkehrung von (1.17) ist i. a. falsch. Sei

$$\mathcal{R} = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

Dann ist $\mathcal{R}$ ein Integritätsbereich, da $\mathcal{R} \subseteq \mathbb{C}$ ist. Wir zeigen, daß das Element $3 \in \mathcal{R}$ irreduzibel ist. Sei dazu $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Also gilt auch

$$3 = \bar{3} = (a - b\sqrt{-5})(c - d\sqrt{-5}),$$

wobei $^-$ das Bilden des konjugiert Komplexen ist. Das ergibt

$$\begin{aligned} 9 &= 3 \cdot 3 = (a + b\sqrt{-5})(a - b\sqrt{-5})(c + d\sqrt{-5})(c - d\sqrt{-5}) \\ &= (a^2 + 5b^2)(c^2 + 5d^2). \end{aligned}$$

Die eindeutige Primfaktorzerlegung in $\mathbb{Z}$ liefert $a^2 + 5b^2 = 3$ oder 9. Das geht nur mit $a = \pm 2$, $b = \pm 1$ und $a^2 + 5b^2 = 9$. Dann ist aber $c^2 + 5d^2 = 1$, was $c = \pm 1$, $d = 0$ liefert. Damit ist $c + d\sqrt{-5} = \pm 1$, d. h., $c + d\sqrt{-5}$ ist eine Einheit. Wir haben somit gezeigt, daß 3 irreduzibel ist.

Wir zeigen nun, daß 3 kein Primelement ist. Es ist

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Aber $2 + \sqrt{-5} \neq 3(a + b\sqrt{-5})$ mit $a, b \in \mathbb{Z}$, da 3 nicht 2 teilt. Somit haben wir ein Beispiel eines irreduziblen Elementes, das kein Primelement ist.

Auch ist $3\mathcal{R}$ kein Primideal. Es ist $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 \in 3\mathcal{R}$, aber weder $(2 + \sqrt{-5})$ noch $(2 - \sqrt{-5})$ ist in $3\mathcal{R}$ enthalten.

(b) Wir wollen die Ideale in $\mathbb{Z}$ bestimmen. Sei $\mathfrak{i} \subseteq \mathbb{Z}$ ein Ideal, $\mathfrak{i} \neq 0, \mathbb{Z}$. Mit $x \in \mathfrak{i}$ ist auch $-x \in \mathfrak{i}$. Wähle nun $x \in \mathfrak{i}$ minimal mit $x > 0$.

Sei $y \in \mathfrak{i}$. Indem wir notfalls y durch $-y$ ersetzen, können wir $y \geq x$ annehmen. Also gibt es ein $n \in \mathbb{N}$ mit $nx \leq y < (n + 1)x$. Nun ist $y - nx < x$. Da $\mathfrak{i}$ ein Ideal

ist, ist $y - nx \in \mathfrak{i}$. Die minimale Wahl von x liefert $y - nx = 0$, d. h. $y = nx$. Somit ist

$$\mathfrak{i} = x\mathbb{Z} = \{xa \mid a \in \mathbb{Z}\}.$$

Beispiel (1.18)(b) führt uns zu der folgenden Definition:

(1.19) Definition. Sei $\mathcal{R}$ ein Integritätsbereich. $\mathcal{R}$ heißt ein Hauptidealring (HIR), falls jedes Ideal $\mathfrak{i}$ von $\mathcal{R}$ die Gestalt $a\mathcal{R}$ mit geeignetem $a \in \mathcal{R}$ hat.

Es besagt (1.18)(b), daß $\mathbb{Z}$ ein Hauptidealring ist. Wir hatten in (1.11)(4) gesehen, daß die Primideale $\neq 0$ in $\mathbb{Z}$ genau die Ideale der Form $p\mathbb{Z}$ mit p Primzahl sind. Dies wollen wir nun auf die Klasse der Hauptidealringe verallgemeinern.

(1.20) Lemma. *Sei $\mathcal{R}$ ein* HIR. *Dann sind* 0 *und $p\mathcal{R}$ mit irreduziblem p die sämtlichen Primideale von $\mathcal{R}$. Jedes von* 0 *verschiedene Primideal ist maximal.*

Beweis. Sei $\mathfrak{p}$ ein Primideal, $\mathfrak{p} \neq 0$. Dann ist $\mathfrak{p} = p\mathcal{R}$ mit geeignetem $p \in \mathcal{R}$. Nach (1.17) ist p irreduzibel.

Sei umgekehrt p irreduzibel. Wir zeigen, daß $p\mathcal{R}$ maximal ist. Es folgt mit (1.14)(b) dann, daß $p\mathcal{R}$ ein Primideal ist.

Sei also $p\mathcal{R} \subset a\mathcal{R} \subset \mathcal{R}$. Dann ist $p = ab$ mit $b \in \mathcal{R}$. Ist a eine Einheit, so ist $1 \in a\mathcal{R}$, ein Widerspruch. Also ist a keine Einheit und somit ist b eine Einheit, d. h. es gibt ein $c \in \mathcal{R}$ mit $bc = 1$. Das liefert $pc = abc = a \in p\mathcal{R}$. Also ist $a\mathcal{R} \subseteq p\mathcal{R}$, ein Widerspruch. □

Ein sehr wichtiger Begriff in der Arithmetik von $\mathbb{Z}$ ist der des größten gemeinsamen Teilers. Auch diesen wollen wir nun verallgemeinern.

(1.21) Definition. Sei $\mathcal{R}$ ein Integritätsbereich und $a_1, \ldots, a_n \in \mathcal{R}$. Wir nennen d einen größten gemeinsamen Teiler der a_i und schreiben

$$\mathrm{ggT}(a_1, \ldots, a_n) = d,$$

falls d alle a_i teilt, und für jedes $c \in \mathcal{R}$, das alle a_i teilt, stets d durch c geteilt wird.

Es ist also d maximal bezüglich der Teilerrelation. Obwohl durch die Bezeichnung $d = \mathrm{ggT}(a, b)$ suggeriert, ist d nicht eindeutig bestimmt. In $\mathbb{Z}$ ist z. B. $2 = \mathrm{ggT}(2, 4)$, aber auch $-2 = \mathrm{ggT}(2, 4)$.

Die obige Definition zeigt: Ist $d_1 = \mathrm{ggT}(a, b)$ und $d_2 = \mathrm{ggT}(a, b)$, so ist $d_1 \mid d_2$ und $d_2 \mid d_1$, was $d_1 = d_2 e$ mit einer Einheit e liefert. Der größte gemeinsame Teiler ist also nur bis auf Einheiten eindeutig bestimmt. Trotzdem werden wir im

folgenden stets von dem größten gemeinsamen Teiler sprechen und je nach Bedarf den geeigneten wählen.

Als erstes zeigen wir, daß es in einem Hauptidealring für endlich viele Elemente stets einen größten gemeinsamen Teiler gibt.

(1.22) Satz. *Sei $\mathcal{R}$ ein* HIR *und $a_1, \ldots, a_n \in \mathcal{R}$. Dann existiert ein größter gemeinsamer Teiler d der a_i, $i = 1, \ldots, n$, in $\mathcal{R}$ und es gibt $b_1, \ldots, b_n \in \mathcal{R}$ mit $a_1b_1 + a_2b_2 + \cdots + a_nb_n = d$.*

Beweis. Da $\mathcal{R}$ ein HIR ist, gilt

$$a_1\mathcal{R} + \cdots + a_n\mathcal{R} = d\mathcal{R} \quad \text{mit } d \in \mathcal{R} \text{ geeignet.}$$

Also ist $a_i = dr_i$, $i = 1, \ldots, n$. Insbesondere teilt d dann alle a_i. Weiter gilt $d = a_1b_1 + \cdots + a_nb_n$ mit geeigneten $b_i \in \mathcal{R}$. Sei nun $t \in \mathcal{R}$ ein Teiler von a_i für alle i. Dann wird d wegen der Summendarstellung von t geteilt. Also ist d ein größter gemeinsamer Teiler der a_i, $i = 1, \ldots, n$. □

Daß in einem Integritätsbereich nicht unbedingt ein größter gemeinsamer Teiler zweier Elemente existieren muß, kann man in Aufgabe 17 sehen.

Die obige Darstellung des größten gemeinsamen Teilers werden wir noch häufig benutzen.

(1.23) Satz. *Ist $\mathcal{R}$ ein* HIR, *so ist jedes irreduzible Element prim.*

Beweis. Sei $p \mid ab$, d. h. $ab = pr$ und $c = \mathrm{ggT}(a, p)$. Da $c \mid p$, ist c eine Einheit oder $c = ep$ mit einer Einheit e. Da $c \mid a$, können wir $c = 1$ annehmen. Nach (1.22) gibt es $u, v \in \mathcal{R}$ mit $1 = up + va$. Durch Multiplikation mit b erhalten wir $b = upb + vab = (ub + vr)p$, und somit ist p ein Teiler von b. □

In Hauptidealringen sind also die Begriffe irreduzibel und prim gleich.

Unser Ziel ist es, zu zeigen, daß Hauptidealringe eine eindeutige Primfaktorzerlegung haben. Dazu sehen wir uns zunächst an, wie wir gezeigt haben, daß $\mathbb{Z}$ ein HIR ist. Dazu hatten wir in (1.18)(b) benutzt, daß es in $\mathbb{Z}$ eine Division mit Rest gibt. Dies wollen wir nun verallgemeinern.

(1.24) Definition. Ein Integritätsbereich $\mathcal{R}$ heißt ein euklidischer[3] Ring, falls es eine Abbildung $\varphi : \mathcal{R} \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ mit folgenden Eigenschaften gibt:

[3] Euklid von Alexandria, *um 365 v. Chr., †um 300 v. Chr., wirkte in Alexandria, Verfasser der „Elemente".

(1) Für $a, b \in \mathcal{R}$ mit $ab \neq 0$ gilt $\varphi(ab) \geq \varphi(a)$,

(2) Zu jedem Paar $a, b \in \mathcal{R}$ mit $a \neq 0$, gibt es Elemente $q, r \in \mathcal{R}$ mit $b = qa + r$, wobei $r = 0$ oder $\varphi(r) < \varphi(a)$ ist (Division mit Rest).

Nun können wir genauso wie in (1.18)(b) vorgehen und zeigen:

(1.25) Satz. *Jeder euklidische Ring ist Hauptidealring.*

Beweis. Sei $0 \neq \mathfrak{i}$ ein Ideal in $\mathcal{R}$. Wähle $0 \neq a \in \mathfrak{i}$ mit $\varphi(a)$ minimal. Sei $b \in \mathfrak{i}$ und $b = aq + r$ mit $\varphi(r) < \varphi(a)$ oder $r = 0$. Dann ist $r = b - aq \in \mathfrak{i}$. Wegen der minimalen Wahl von a ist $r = 0$. Also ist $b = aq$, d. h. $\mathfrak{i} = a\mathcal{R}$. □

(1.26) Beispiele. (a) $\mathcal{R} = \mathbb{Z}$. Setze $\varphi(a) = |a|$. Es sei $ab \neq 0$. Dann ist $\varphi(ab) = |ab| = |a||b| \geq |a| = \varphi(a)$. Es gibt $q \in \mathbb{Z}$ mit $qa \leq b < (q+1)a$. Ist $b = qa + r$, so ist $r = 0$, oder $\varphi(r) = |r| < |a| = \varphi(a)$.

(b) Der nun folgende Ring ist nur ein Spezialfall einer wesentlich größeren Klasse von Ringen, mit denen wir uns in (1.29) beschäftigen werden. Man nennt ihn den Ring der Gauß'schen Zahlen[4]:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Da $\mathbb{Z}[i] \subseteq \mathbb{C}$ ist, ist $\mathbb{Z}[i]$ ein Integritätsbereich. Setze nun

$$\varphi(a + ib) = a^2 + b^2 = (a + ib)(a - ib) = |a + ib|^2.$$

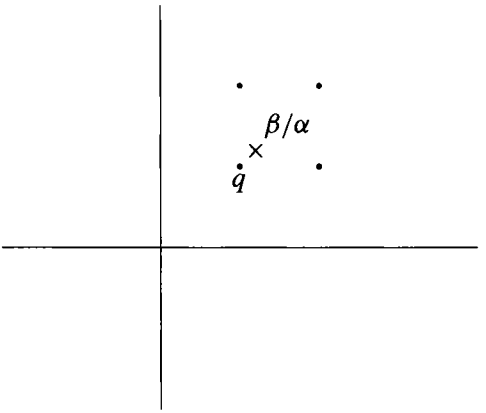
Für $c + ib \neq 0$ gilt

$$\begin{aligned}\varphi((a + ib)(c + id)) &= |(a + ib)(c + id)|^2 = |a + ib|^2|c + id|^2 \geq |a + ib|^2 \\ &= \varphi(a + ib).\end{aligned}$$

Seien $a + ib$, $c + id$ gegeben, $c + id \neq 0$. Wir wollen $\beta = a + ib$ durch $\alpha = c + id$ mit Rest teilen. Es ist

$$\frac{\beta}{\alpha} = \frac{a + ib}{c + id} = \frac{(a + ib)(c - id)}{(c + id)(c - id)} = \frac{(a + ib)(c - id)}{c^2 + d^2} = s + it \quad \text{mit } s, t \in \mathbb{Q}.$$

[4] C. F. Gauß, *30.4.1777 Braunschweig, †23.2.1855 Göttingen, Professor in Göttingen, wird als der größte Mathematiker der Neuzeit bezeichnet. In seiner Doktorarbeit bewies er den Fundamentalsatz der Algebra (jedes nicht konstante Polynom mit komplexen Koeffizienten hat eine Nullstelle in den komplexen Zahlen), mit 19 Jahren bewies er die Konstruierbarkeit mit Zirkel und Lineal des regelmäßigen 17-Ecks, ein Problem, das bis auf Euklid zurück geht. Mit 24 Jahren schrieb er die „Disquisitiones Arithmeticae", eines der bedeutendsten Werke der Mathematik. Hier wurden die Grundlagen der Zahlentheorie, die bis daher aus vereinzelten Problemen bestand, gelegt. Er arbeitete auf vielen verschiedenen Gebieten (Geometrie, Algebra, Astronomie, Physik) und führte grundlegende Begiffe ein, z. B. die Gauß'sche Glockenkurve und die erste geometrische Interpretation der komplexen Zahlen mittels der Gauß'schen Zahlenebene.



Wähle $x, y \in \mathbb{Z}$ mit $|s - x| \leq \frac{1}{2}$ und $|t - y| \leq \frac{1}{2}$ und setze $q = x + iy$. Dann ist

$$(a + ib) = (x + iy)(c + id) + r \quad \text{mit } r = (c + id)[(s + it) - (x + iy)].$$

Somit ist

$$\varphi(r) = \varphi(c + id)\varphi((s - x) + i(t - y)) \leq \varphi(c + id)\frac{1}{2} < \varphi(c + id).$$

(c) In euklidischen Ringen kann man mit dem sogenannten euklidischen Algorithmus sehr leicht einen größten gemeinsamen Teiler von $a \neq 0$ und b berechnen:

Setze $r_{-1} = b$, $r_0 = a$.

$$r_{-1} = q_1 r_0 + r_1 \quad \text{mit } \varphi(r_1) < \varphi(r_0)$$

Nun wende die Division mit Rest auf das Paar r_0, r_1 an:

$$r_0 = q_2 r_1 + r_2, \quad \varphi(r_2) < \varphi(r_1)$$

usw.

$$r_i = q_{i+2} r_{i+1} + r_{i+2}, \quad \varphi(r_{i+2}) < \varphi(r_{i+1})$$

Dies wird solange fortgesetzt, bis der Rest Null wird, also

$$r_s = q_{s+2} r_{s+1}$$

Dann ist r_{s+1} ein größter gemeinsamer Teiler von a und b.

Offenbar ist r_{s+1} ein Teiler von r_s. Da

$$r_{s-1} = q_{s+1} r_s + r_{s+1}$$

ist, ist r_{s+1} auch ein Teiler von r_{s-1}. Sei allgemein r_{s+1} ein Teiler von r_{i+2} und r_{i+1}, so auch von $r_i = q_{i+2}r_{i+1} + r_{i+2}$. Per Induktion erhalten wir, daß r_{s+1} sowohl a als auch b teilt.

Ist nun d ein Teiler von a und b, so auch von r_2. Sei allgemein schon gezeigt, daß d sowohl r_i als auch r_{i+1} teilt, so wird auch $r_{i+2} = r_i - q_{i+2}r_{i+1}$ von d geteilt. Per Induktion erhalten wir, daß d dann r_{s+1} teilt. Somit ist r_{s+1} ein größter gemeinsamer Teiler von a und b. Sei z. B. $b = 60$, $a = 35$. Dann ist

$$\begin{aligned} 60 &= 35 + 25 \\ 35 &= 25 + 10 \\ 25 &= 2 \cdot 10 + 5 \\ 10 &= 2 \cdot 5. \end{aligned}$$

Also ist

$$5 = \mathrm{ggT}(60, 35).$$

Wir wollen jetzt zeigen, daß jeder Hauptidealring eine eindeutige Primfaktorzerlegung besitzt.

(1.27) Lemma. *Sei $\mathcal{R}$ ein* HIR. *Dann besitzt jede nicht leere Teilmenge $\mathfrak{S}$ von Idealen von $\mathcal{R}$ ein maximales Element.*

Beweis. Sei $\mathfrak{K}$ eine Kette in $\mathfrak{S}$. Dann ist $\mathfrak{j} = \bigcup_{\mathfrak{i} \in \mathfrak{K}} \mathfrak{i}$ ein Ideal. Da $\mathcal{R}$ ein Hauptidealring ist, ist $\mathfrak{j} = c\mathcal{R}$ mit geeignetem $c \in \mathcal{R}$. Somit gibt es ein $\mathfrak{i} \in \mathfrak{K}$ mit $c \in \mathfrak{i}$. Da $\mathfrak{i}$ ein Ideal ist, ist $\mathfrak{j} = c\mathcal{R} \subseteq \mathfrak{i} \subseteq \mathfrak{j}$. Also ist $\mathfrak{j} \in \mathfrak{K}$ und somit $\mathfrak{j} \in \mathfrak{S}$, d. h. jede Kette in $\mathfrak{S}$ hat eine obere Schranke. Nun folgt mit dem Lemma von Zorn die Behauptung. □

(1.28) Hauptsatz. *Sei $\mathcal{R}$ ein* HIR. *Dann ist $\mathcal{R}$ ein* ZPE-*Ring.*

Beweis. Wir zeigen zunächst, daß sich jedes Element $a \in \mathcal{R}$, $a \neq 0$, als $ep_1 \dots p_k$ mit einer Einheit e und irreduziblen p_i schreiben läßt. Sei

$$\mathfrak{S} = \{b\mathcal{R} \mid a = bp_1 \dots p_n \text{ mit endlich vielen irreduziblen } p_i\}.$$

Da $a\mathcal{R} \in \mathfrak{S}$ ist, ist $\mathfrak{S} \neq \varnothing$. Nach (1.27) gibt es ein maximales Element $c\mathcal{R}$ in $\mathfrak{S}$. Nach Definition von $\mathfrak{S}$ ist

$$a = cp_1 \dots p_k.$$

Wir zeigen zunächst, daß c eine Einheit ist. Sei dazu $c\mathcal{R} \neq \mathcal{R}$. Nach (1.14) ist $c\mathcal{R} \subseteq \mathfrak{m} \subset \mathcal{R}$ mit maximalem Ideal $\mathfrak{m}$ in $\mathcal{R}$. Sei $\mathfrak{m} = p\mathcal{R}$. Nach (1.14)(b) ist $\mathfrak{m}$ ein Primideal. Nach (1.17) ist p irreduzibel. Nun ist $c = pd$ mit geeignetem d.

Also ist $c\mathcal{R} \subseteq d\mathcal{R}$. Da $a = dpp_1 \dots p_n$ ist, ist $d\mathcal{R} \in \mathfrak{S}$. Die Maximalität von $c\mathcal{R}$ liefert nun $d\mathcal{R} = c\mathcal{R}$. Dann ist $d = rc$ mit geeignetem $r \in \mathcal{R}$, was $c = dp = crp$ ergibt. Somit ist $rp = 1$, ein Widerspruch. Wir haben nun $c\mathcal{R} = \mathcal{R}$, d. h. c ist Einheit. Damit haben wir die Existenz der Zerlegung gezeigt.

Wir zeigen nun die Eindeutigkeit der Zerlegung. Sei

$$a = ep_1 \dots p_k = \tilde{e}\tilde{p}_1 \dots \tilde{p}_r$$

mit Einheiten e, $\tilde{e}$ und irreduziblen Elementen $p_1, \dots, p_k$, $\tilde{p}_1, \dots, \tilde{p}_r$. Seien $p_t, \dots, p_k$ die irreduziblen Elemente, die auch unter den $\tilde{p}_i$ vorkommen, d. h. $p_t = \tilde{f}_j \tilde{p}_j$ für geeignetes j, $\tilde{f}_j$ eine Einheit. Dann ist

$$a = ep_1 \dots p_{t-1} p_t \dots p_k = \tilde{\tilde{e}}\, \tilde{p}_1 \dots \tilde{p}_{r-k+t}\, p_t \dots p_k, \quad \tilde{\tilde{e}} \text{ Einheit.}$$

Da $\mathcal{R}$ ein Integritätsbereich ist, folgt

$$ep_1 \dots p_{t-1} = \tilde{\tilde{e}}\, \tilde{p}_1 \dots \tilde{p}_{r-k+t}.$$

Also können wir annehmen, daß es kein Paar $\tilde{p}_i$, p_j gibt, so daß für eine geeignete Einheit d wir $\tilde{p}_i = p_j d$ haben.

Nun ist $\tilde{e}\tilde{p}_1 \dots \tilde{p}_r \in p_1\mathcal{R}$. Nach (1.20) ist $p_1\mathcal{R}$ ein Primideal und maximales Ideal. Somit ist nach (1.8) $\mathcal{R}/p_1\mathcal{R}$ ein Körper. Es ist

$$(\tilde{e} + p_1\mathcal{R})(\tilde{p}_1 + p_1\mathcal{R}) \dots (\tilde{p}_r + p_1\mathcal{R}) = ((\tilde{e}\tilde{p}_1 \dots \tilde{p}_r) + p_1\mathcal{R}) = p_1\mathcal{R}$$

Also gibt es ein i mit $\tilde{p}_i + p_1\mathcal{R} = p_1\mathcal{R}_1$ d. h., $\tilde{p}_i \in p_1\mathcal{R}$. Dann ist $\tilde{p}_i = p_1 d$. Da $\tilde{p}_i$ irreduzibel ist, folgt, daß d eine Einheit ist, ein Widerspruch. □

Wir haben bisher gezeigt, daß jeder euklidische Ring ein Hauptidealring und jeder Hauptidealring ein ZPE-Ring ist. Ein Beispiel eines ZPE-Ringes, der kein Hauptidealring ist, werden wir in (1.47) kennenlernen. Wir wollen nun zeigen, daß es Hauptidealringe gibt, die nicht euklidisch sind.

(1.29) Beispiel. Beispiele von Integritätsbereichen kommen häufig aus der Zahlentheorie.

Sei $m \in \mathbb{Z}$, m quadratfrei. Setze

$$R_m = \{r + s\sqrt{m} \mid r, s \in \mathbb{Z}\} \quad \text{für } m \equiv 2, 3 \pmod 4$$
$$R_m = \{(r + s\sqrt{m})/2) \mid r, s \in \mathbb{Z},\ r,\ s \text{ haben gleiche Parität}\} \quad \text{sonst.}$$

Da R_m in $\mathbb{C}$ enthalten ist, ist R_m ein Integritätsbereich. Weiter ist sogar R_m in $\{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\} = M$ enthalten. Wir werden später sehen, daß M ein Körper

ist, den wir mit $\mathbb{Q}(\sqrt{m})$ bezeichnen werden. Wir können für R_m auch die folgende Definition geben

$$R_m = \{u \mid u \in M,\ u \text{ ist Nullstelle eines Polynoms } x^2 + cx + d \text{ mit } c, d \in \mathbb{Z}\}.$$

Hier ist die Asymmetrie zwischen $m \equiv 1 \pmod 4$ und $m \not\equiv 1 \pmod 4$ aufgehoben.

Für $u = a + b\sqrt{m} \in M$ definiere jetzt

$$N(u) = a^2 - mb^2 = (a + b\sqrt{m})(a - b\sqrt{m}).$$

Aus der zweiten Gleichung kann man sofort ablesen:

$$N(u_1 u_2) = N(u_1)N(u_2)$$

(vgl. mit dem φ aus (1.26)(b)!).

Wir wollen R_m auf seine Hauptidealeigenschaft hin untersuchen. Nicht jeder Ring R_m ist Hauptidealring. Betrachten wir z. B. R_{-5}. Wie wir in (1.18) gesehen haben, gibt es irreduzible Elemente in R_{-5}, die keine Primelemente sind. Dies geht aber nach (1.23) in einem HIR nicht. Also haben wir, daß R_{-5} kein Hauptidealring ist. Auf der anderen Seite ist R_{-1} nach (1.26)(b) mit der Abbildung $\varphi(r) = N(r)$ sogar euklidisch.

Ist $m < 0$, so ist R_m allerdings selten euklidisch, wie wir jetzt zeigen werden.

(1) *Ist $m < 0$, m quadratfrei, $m \neq -1, -2, -3, -7, -11$, so ist R_m nicht euklidisch. Ist $m = -1, -2, -3, -7, -11$, so ist R_m euklidisch, wobei $\varphi(r) = N(r)$ ist.*

Beweis. Sei R_m euklidisch. Es ist $m = -6, -10$ oder $m \leq -13$. Sei $b \in R_m \setminus \{0\}$ keine Einheit mit $\varphi(b)$ minimal. Sei weiter $a \in R_m$ beliebig. Da R_m euklidisch ist, gibt es $q, r \in R_m$ mit

$$a = bq + r \quad \text{und} \quad r = 0 \quad \text{oder} \quad \varphi(r) < \varphi(b).$$

Die minimale Wahl von b liefert, daß $r = 0$ oder eine Einheit ist.

Sei r eine Einheit. Dann ist $rr' = 1$ für geeignetes r'. Also ist

$$1 = N(rr') = N(r)N(r')$$

und dann

$$N(r) = \pm 1.$$

Sei $r = m_1 + m_2\sqrt{m}$. Dann ist

$$\pm 1 = m_1^2 - m_2^2 m.$$

Da $m < -1$ ist, folgt $m_2 = 0$ und $m_1 = \pm 1$. Sei $r = (m_1 + m_2\sqrt{m})/2$. Dann ist

$$\pm 4 = m_1^2 - m_2^2 m.$$

Wieder gilt $m_2 = 0$ und $m_1 = \pm 2$. Also ist stets $r = \pm 1$. Damit haben wir

$$a = bq \quad \text{oder} \quad a = bq \pm 1.$$

Somit teilt b entweder a, $a + 1$ oder $a - 1$. Wähle nun speziell $a = 2$. Dann gilt, b teilt 2 oder 3, da b keine Einheit ist. Wir zeigen, daß 2 und 3 beide irreduzibel sind.

Sei $3 = [(u + v\sqrt{m})/2][(x + y\sqrt{m})/2]$ mit $u, v, x, y \in \mathbb{Z}$. Dann ist

$$3^2 = N(3) = [(u^2 - mv^2)/4][(x^2 - my^2)/4].$$

Da kein Faktor eine Einheit ist, folgt mit (1.25) und (1.28)

$$3 = (u^2 - mv^2)/4 = (x^2 - my^2)/4.$$

Das liefert $u^2 - mv^2 = 12$, was offenbar keine Lösung hat.

Sei $2 = [(u + v\sqrt{m})/2][(x + y\sqrt{m})/2]$ mit $u, v, x, y \in \mathbb{Z}$. Dann ist

$$4 = [(u^2 - v^2 m)/4][(x^2 - y^2 m)/4].$$

Somit ist $8 = u^2 - v^2 m$, was auch keine Lösung hat.

Da b aber 2 bzw. 3 teilt, folgt nun, daß $b = \pm 2$ oder ± 3 ist. Die Einheiten sind ± 1, wie bereits gezeigt.

Sei nun $m \equiv 1 \pmod 4$. Dann wählen wir $a = (1 + \sqrt{m})/2$. Wir erhalten nun $a + 1 = (3 + \sqrt{m})/2$ und $a - 1 = (-1 + \sqrt{m})/2$.

Damit gilt, daß 2 oder 3 eine der Zahlen a, $a + 1$, $a - 1$ teilt. Ist nun entweder $(x + y\sqrt{m})/4 \in R_m$ oder $(x + y\sqrt{m})/6 \in R_m$, so muß 2 bzw. 3 die Koeffizienten x und y teilen. Dies ist aber weder bei a, $a + 1$ noch bei $a - 1$ der Fall.

Sei $m \equiv 2, 3 \pmod 4$, so wähle $a = 1 + \sqrt{m}$. Dann ist $a + 1 = 2 + \sqrt{m}$ und $a - 1 = \sqrt{m}$. Wieder teilt weder 2 noch 3 eine der Zahlen a, $a + 1$, $a - 1$.

Daß R_m für die angegebenen Werte euklidisch ist, kann man wie in (1.26)(b) zeigen. □

Wir haben gerade gezeigt, daß z. B. R_{-19} kein euklidischer Ring ist. Wir wollen zeigen, daß R_{-19} ein HIR ist. Damit haben wir dann ein Beispiel eines Hauptidealringes, der nicht euklidisch ist.

(2) *Sei m quadratfrei, $m \neq 1, 0$. Für $x, y \in R_m$, wobei x nicht von y geteilt wird und $|N(x)| \geq |N(y)|$ ist, gebe es stets $u, v \in R_m$ mit*

(a) $xu \neq yv$ *und*

(b) $|N(xu - yv)| < |N(y)|$

Dann ist R_m ein Hauptidealring.

Beweis. Sei $0 \neq \mathfrak{i} \subseteq R_m$ ein Ideal. Wähle $y \in \mathfrak{i}$ mit $y \neq 0$ und $|N(y)|$ minimal. Sei $x \in \mathfrak{i}$. Angenommen y teilt nicht x. Nach Annahme gibt es dann $u, v \in R_m$ mit $xu - yv \neq 0$ und $|N(xu - yv)| < |N(y)|$. Da $xu - yv \in \mathfrak{i}$ ist, geht das nicht. Somit ist $x = yt$, d. h. $\mathfrak{i} = yR_m$. □

Dieses Kriterium wenden wir nun mit $m = -19$ an und zeigen

(3) R_{-19} *ist ein* HIR.

Beweis. Da $-19 \equiv 1 \pmod 4$ ist, ist

$$R_{-19} = \{(a + b\sqrt{-19})/2 \mid a, b \in \mathbb{Z}, a \text{ und } b \text{ haben die gleiche Parität}\}$$

Da $m < 0$ ist, ist $N(u) \geq 0$ für alle $u \in R_{-19}$. Wir wollen (2) nachprüfen.

Seien $x, y \in R_{-19}$, y kein Teiler von x und $N(x) \geq N(y)$. Gesucht sind $u, v \in R_m$ mit $xu - yv \neq 0$ und $N(xu - yv) < N(y)$ bzw. $N((x/y)u - v) < 1$.

Es ist $x/y \in M$, also ist $x/y = (a + b\sqrt{-19})/c$ mit geeigneten $a, b, c \in \mathbb{Z}$ und $\mathrm{ggT}(a, b, c) = 1$. Da $x/y \notin R_{-19}$ ist, folgt $c > 1$.

Sei $c = 2$. Da $x/y \notin R_{-19}$ ist, folgt nun, daß a und b entgegengesetzte Parität haben. Setze $u = 1$ und

$$v = \big((a - 1) + b\sqrt{-19}\big)/2 \in R_{-19}.$$

Dann ist

$$\left(\frac{x}{y}\right)u - v = \frac{1}{2} \quad \text{und} \quad 0 < N\left(\frac{1}{2}\right) = \frac{1}{4} < 1.$$

Sei $c = 3$. Dann ist 3 kein Teiler von a oder 3 kein Teiler von b. Insbesondere ist $a^2 + b^2 \not\equiv 0 \pmod 3$. Nun ist

$$a^2 + 19b^2 \equiv a^2 + b^2 \pmod 3.$$

Also ist

$$a^2 + 19b^2 = 3q + r \quad \text{mit } r = 1 \text{ oder } 2.$$

Setze $u = a - b\sqrt{-19}$ und $v = q$. Dann ist

$$\left(\frac{x}{y}\right)u - v = (a + b\sqrt{-19})(a - b\sqrt{-19})/3 - q = (a^2 + 19b^2)/3 - q = \frac{r}{3}$$