MASTERARBEIT | MASTER'S THESIS

Titel | Title

Binäre quadratische Formen und die Arithmetik des Ringes der Eisensteinzahlen

verfasst von | submitted by

Astrid Mosgöller BEd

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Education (MEd)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 199 504 520 02
Studienrichtung lt. Studienblatt | Degree programme as it appears on the student record sheet:	Masterstudium Lehramt Sek (AB) Unterrichtsfach Chemie Unterrichtsfach Mathematik
Betreut von | Supervisor:	ao. Univ.-Prof. Dr. Joachim Mahnkopf

Zusammenfassung

Die vorliegende Arbeit beschäftigt sich mit einem Unterring der komplexen Zahlen, den sogenannten Eisensteinzahlen. Mithilfe zahlentheoretischer Grundlagen und Herleitungen wird die Arithmetik des Rings der Eisensteinzahlen, insbesondere die Teilbarkeit, Primelemente und eine eindeutige Faktorisierung erarbeitet. Genauer wird in dieser Masterarbeit gezeigt, dass die Eisensteinzahlen $\mathbb{Z}[\omega]$ einen euklidischen Ring bilden, weswegen eine Division mit Rest und ein euklidischer Algorithmus durchgeführt werden können. Aus mehreren Ansätzen wird dann als zentrales Ergebnis ein Zerlegungsgesetz für Primzahlen $p \in \mathbb{P}$ in $\mathbb{Z}[\omega]$ aufgestellt und vollständig mittels Reduktionstheorie von binären quadratischen Formen bewiesen. Unter Zuhilfenahme der Normabbildung $\delta : \mathbb{Z}[\omega] \to \mathbb{N}$ und des Zerlegungsgesetzes können anschließend die Primelemente in $\mathbb{Z}[\omega]$ bestimmt und eine Primfaktorzerlegung berechnet werden.

Abstract

The present thesis deals with a subring of the complex numbers, the so-called Eisenstein integers. Using number-theoretic basics and derivations the arithmetic of the ring of Eisenstein integers, particularly divisibility, prime elements, and unique factorization, is developed. More precisely, this master thesis shows that the Eisenstein integers $\mathbb{Z}[\omega]$ form a Euclidean ring so that division with remainder and the application of a Euclidean algorithm can be carried out. Using several approaches a decomposition law for prime numbers $p \in \mathbb{P}$ in $\mathbb{Z}[\omega]$ is then derived as a central result and completely proven by means of the reduction theory of binary quadratic forms. With the help of the norm mapping $\delta : \mathbb{Z}[\omega] \to \mathbb{N}$ and the decomposition law the prime elements in $\mathbb{Z}[\omega]$ can then be determined and a prime factorization can be calculated.

Inhaltsverzeichnis

1 Einleitung **1**

2 Algebraische und zahlentheoretische Grundlagen **3**
2.1 Gruppe . . . 3
2.2 Ring . . . 7
2.2.1 Körper . . . 9
2.2.2 Teilbarkeit in Integritätsbereichen . . . 10
2.2.3 Ideale . . . 14
2.3 Zusammenhang: Hauptidealringe - faktorielle Ringe - euklidische Ringe . . 20
2.3.1 Beispiel: Der euklidische Ring $\mathbb{Z}$ . . . 24
2.4 Zusammenfassung . . . 27

3 Quadratische Zahlkörper und Ganzheitsringe **28**
3.1 Quadratische Zahlkörper . . . 28
3.2 Ganzheitsringe in quadratischen Zahlkörpern . . . 30
3.2.1 Einheiten in quadratischen Zahlringen . . . 33
3.3 Imaginär-quadratische, euklidische Ganzheitsringe . . . 34
3.3.1 Bestimmung der imaginär-quadratischen, euklidischen Ganzheitsringe . . . 34
3.3.2 Teilbarkeit in imaginär-quadratischen, euklidischen Ganzheitsringen 39
3.3.3 Zerlegungsverhalten von Primelementen $p \in \mathbb{Z}$ im Ganzheitsring $\mathcal{O}_d$ 41
3.3.4 Teilbarkeit in euklidischen Ganzheitsringen . . . 43
3.3.5 Teilbarkeit in allgemeinen quadratischen Zahlkörpern mit nicht notwendig faktoriellem Ganzheitsring $\mathcal{O}_d$ . . . 46
3.4 Zusammenfassung . . . 48

4 Arithmetik im Ring der Eisensteinzahlen $\mathbb{Z}[\omega]$ **49**
4.1 $\mathbb{Z}[\omega]$ ist euklidisch . . . 49
4.2 Primelemente in $\mathbb{Z}[\omega]$ . . . 54
4.2.1 Zusammenhang der Arithmetik von $\mathbb{Z}$ und $\mathbb{Z}[\omega]$: Zerlegungsgesetz . 55
4.2.2 Primzahltest in $\mathbb{Z}[\omega]$ . . . 60
4.3 Beispiele und Anwendung . . . 61
4.3.1 Anwendungen der Division mit Rest . . . 61
4.3.2 Anwendungen zur Primzerlegung . . . 64

5 Binäre quadratische Formen **69**
5.1 Grundlagen . . . 69
5.2 Reduktionstheorie positiv definiter, quadratischer Formen . . . 71

6 Fazit **75**

7 Abbildungs- und Literaturverzeichnis **76**

1 Einleitung

Mit ihren Wurzeln in der Antike hat sich die Zahlentheorie zu einem modernen Forschungsgebiet entwickelt, das grundlegende Fragen der Arithmetik mit aktuellen Problemstellungen und Anwendungen verknüpft. Dabei sind gerade die algebraischen Strukturen wie Ringe ein zentrales Thema. Ebenso relevant sind die mit Hilfe ebendieser Ringe formulierten Eigenschaften der Teilbarkeit, Primzahlen und Faktorisierung, die zum Beispiel in der Kryptografie Anwendung finden. Genau diese Merkmale werden in dieser Arbeit in Bezug auf die Eisensteinzahlen untersucht.
Die Eisensteinzahlen gehen auf den Mathematiker Gotthold Eisenstein (*1823 - 1852*) zurück. Dieser ist vor allem für seine Arbeit *"teils in der höheren Arithmetik, teils in der Theorie der [...] Funktionen, teils in der Verknüpfung dieser beiden großen Gebiete",* [1] bekannt und wurde von vielen namhaften Wissenschaftlern und Mathematikern bereits zu Lebzeiten unterstützt, unter anderem von Humboldt, Gauß und Dirichlet [1][13, S. 420f]. Die Eisensteinzahlen bilden einen speziellen Ring innerhalb eines Erweiterungskörpers von $\mathbb{Q}$. Sie werden unter Zuhilfenahme der dritten Einheitswurzel $\omega^3 = 1; \quad \omega = e^{\frac{2\pi i}{3}}$ dargestellt und bilden den euklidischen Ring $\mathbb{Z}[\omega]$, dessen Arithmetik entsprechend der ganzen Zahlen $\mathbb{Z}$ ergründbar ist.
Ziel dieser Masterarbeit ist es, die grundlegenden arithmetischen Eigenschaften im Ring der Eisensteinzahlen zu erörtern. Insbesondere sollen dabei die Teilbarkeit, die primen Elemente und eine eindeutige Faktorisierung erarbeitet und schließlich die Arithmetik mit der Arithemtik der ganzen Zahlen verglichen werden, indem das Zerlegungsgesetz im Ring der Eisensteinzahlen bewiesen wird. Um dieses Ziel erreichen zu können, werden theoretische Aspekte mit konkreten Beispielen und geometrischen Darstellungen verdeutlicht, um ein ganzheitliches Bild der Eisensteinzahlen zu erhalten.
Dazu werden im zweiten Kapitel ein zahlentheoretischer Grundstein gelegt und algebraische Strukturen definiert. Dabei nehmen die Teilbarkeit und die Primzahlen einen großen Teil ein. Anhand des Rings der ganzen Zahlen $\mathbb{Z}$ werden diese Strukturen verdeutlicht und erste Beispiele gegeben. Besondere Beachtung erhalten dabei unter anderem die Division mit Rest und die Existenz des euklidischen Algorithmus, sowie die Primzahlen mit ihren Eigenschaften, beispielsweise die Existenz und Eindeutigkeit der Primfaktorzerlegung in allgemeinen Ringen R.
Daran anknüpfend werden die quadratischen Erweiterungskörper über $\mathbb{Q}$, die sogenannten quadratischen Zahlkörper sowie deren Ganzheitsringe vorgestellt. Das Hauptaugenmerk liegt dabei auf den sogenannten imaginär-quadratischen Zahlkörpern $\mathbb{Q}(\sqrt{d})$ mit $d < 0$. Die in Abschnitt 1 dargestellten Grundlagen zu primen Elementen werden anschließend mithilfe einer Normabbildung, die die Elemente aus quadratischen Zahlkörpern auf den Integritätsbereich der ganzen Zahlen abbildet, im Fall der Ganzheitsringe in $\mathbb{Q}(\sqrt{d})$ genauer analysiert.
Das vierte Kapitel widmet sich den Eisensteinzahlen, das heißt dem Ring der ganzen Zahlen in $\mathbb{Q}(\sqrt{-3})$. Dazu werden verschiedene Herangehensweisen zur Erarbeitung eines konkreten Zerlegungsgesetzes nach Forster [5][7] und Weissman [16] auf das Beispiel des

[1] Gauß, 1847. In einer Vorrede zum Sammelband Eisensteins Werke "Math. Abh."

Rings der Eisensteinzahlen angewendet. Zur Erarbeitung dieses Zerlegungsgesetztes für die Elemente im Ring $\mathbb{Z}[\omega]$ wird dabei einerseits mit dem Verfahren des "Lifting und Lowering" von Primelementen, andererseits mit quadratischen Resten und der Zuhilfenahme des Legendre-Symbols gearbeitet. Anschließend werden die zugrundeliegenden theoretischen Ergebnisse anhand konkreter Berechnungen zur Anwendung gebracht. Der vollständige Beweis des Zerlegungsgesetzes im Ring $\mathbb{Z}[\omega]$ erfolgt abschließend durch die im fünften Kapitel besprochene Reduktionstheorie für binäre quadratische Formen.

2 Algebraische und zahlentheoretische Grundlagen

Der Einstieg in diese Arbeit erfolgt mit der Definition algebraischer Strukturen. Ausgehend von Gruppen und ihren Morphismen wird im Anschluss die Struktur der Ringe betrachtet, die den Grundstein der Zahlentheorie legt und damit für die Analyse der Eisensteinzahlen von hoher Bedeutung ist.

2.1 Gruppe

Definition 1. Eine Menge G zusammen mit einer Verknüpfung

$$\circ : G \times G \to G, (a, b) \mapsto a \circ b,$$

heißt ***Gruppe*** $(G, \circ)$, wenn die folgenden Bedingungen erfüllt werden:

(G1) Die Verknüpfung $\circ$ ist ***assoziativ***, also für alle $a, b, c \in G$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$.

(G2) Es gibt ein eindeutig bestimmtes $e \in G$ für das gilt:
$e \circ a = a \circ e = a$ für alle $a \in G$
e heißt ***neutrales Element*** von G.

(G3) Zu jedem $a \in G$ gibt es ein eindeutig bestimmtes $a^{-1} \in G$ für das gilt:
$a^{-1} \circ a = a \circ a^{-1} = e$
a^{-1} heißt ***Inverses*** von a.
Für die Inversion gilt außerdem $(a^{-1})^{-1} = a$.

G heißt ***kommutativ***, wenn für alle Elemente $a, b \in G$ gilt $a \circ b = b \circ a$.

Ist die Verknpüfung abelsch, so wird sie mit dem Symbol "+" geschrieben und als ***Addition*** bezeichnet. Das neutrale Element e der Addition wird auch ***Nullelement*** genannt, man schreibt 0. Ist die Verknüpfung nicht abelsch, so wird sie als ***Multiplikation*** bezeichnet mit dem neutralen Element oder ***Einselement***, geschrieben 1. Die kürzere Schreibweise für multiplikativ verknüpfte Elemente erfolgt mit einem zentralen Punkt $a \cdot b$ oder kurz mit ab.

In jeder Gruppe $(G, \circ)$ mit $a, x, y \in G$ gelten die ***Kürzungsregeln***:

$$ax = ay \Rightarrow x = y \qquad xa = ya \Rightarrow x = y.$$

Daraus folgt, dass die Gleichungen $ax = b$ und $ya = b$ für jedes $a \in G$ und $b \in G$ eindeutig lösbar sind durch

$$x = a^{-1}b \qquad y = ba^{-1}.$$

Definition 2. Seien $(G, \circ)$ und $(H, \bullet)$ Gruppen. Eine Abbildung $\varphi : G \to H$ heißt ***Gruppenhomomorphismus***, wenn für alle Elemente $a, b \in G$ gilt:

$$f(a \circ b) = f(a) \bullet f(b).$$

Ist die Abbildung φ bijektiv, so heißt sie Gruppen**isomorphismus** und die Gruppen heißen isomorph: $G \cong H$.
Surjektive Homomorphismen heißen Epimorphismen, injektive heißen Monomorphismen. Ein Gruppenhomomorphismus von G nach G heißt Endomorphismus. Ist ein solcher Endomorphismus bijektiv, so heißt er Automorphismus.
Der ***Kern*** von φ ist die Menge aller Elemente von G, die auf das neutrale Element e_H von H abgebildet werden, also

$$Kern\,\varphi := \{a \in G : \varphi(a) = e_H\}.$$

Definition 3. Für die Gruppe G und die Teilmenge U von G ($U \subset G$) heißt U ***Untergruppe*** von G, wenn gilt:

(UG1) U ist abgeschlossen bezüglich der Multiplikation, also für $a, b \in U$ ist $a \circ b \in U$.

(UG2) U ist mit der von G vererbten Verknüpfung $\circ$ wieder eine Gruppe.

Man schreibt $U < G$.

Für die Untersuchung in der Praxis verwenden wir die folgende

Bemerkung 4. Eine Teilmenge U einer Gruppe G ist genau dann eine Untergruppe, wenn gilt:

(1) $U \neq \emptyset$

(2) $a, b \in U \Rightarrow ab^{-1} \in U$

Beweis. Wenn G eine Gruppe ist gilt das Assoziativgesetz, das dann auch für jede Untergruppe U gelten muss. Durch $U \neq \emptyset$ gibt es ein $a \in U$ für das $aa^{-1} = e \in U$. Zu $b \in U$ ist $b^{-1} = eb^{-1} \in U$.
Mit $a, b \in U$ und $ab = a(b^{-1})^{-1} \in U$ ist U abgeschlossen bezüglich der Multiplikation. □

In jeder Gruppe G gibt es die ***trivialen Untergruppen*** $\{e\}$ und G.

Beispiel 5.

- $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$.
- $(\mathbb{Q}, +)$ ist eine Untergruppe von $(\mathbb{R}, +)$.
- $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{C}, +)$.

Lemma 6. *Seien $(G, \circ), (H, \bullet)$ Gruppen mit neutralem Element e_G bzw. e_H und $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann gilt für alle $a \in G$:*

a) $\varphi(e_G) = e_H$

b) $\varphi(a^n) = \varphi(a)^n$ *für alle* $n \in \mathbb{Z}$

c) *Das Bild einer Untergruppe von G ist eine Untergruppe von H: $U_G < G \Rightarrow \varphi(U_G) < H$.*

d) *Das Urbild einer Untergruppe von H ist eine Untergruppe von G: $U_H < H \Rightarrow \varphi^{-1}(U_H) < G$.*

e) *Der Gruppenhomomorphismus φ ist injektiv genau dann, wenn $\ker\varphi = \{e_G\}$.*

Beweis. [4, S.21][11, S. 25]

a) Aus $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$ folgt durch kürzen sofort $e_H = \varphi(e_G)$.

b) Die Behauptung ist für $n \geq 0$ klar. Wir zeigen die Behauptung für $n = -1$. Nach a) gilt $e_H = \varphi(e_G) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) \Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$. Damit gilt für alle $m \in \mathbb{N}$: $\varphi(a^{-m}) = \varphi(a^m)^{-1} = (\varphi(a)^m)^{-1} = \varphi(a)^{-m}$.

c) Seien $a, b \in U_G$ mit $a' = \varphi(a), b' = \varphi(b) \in \varphi(U_G)$. Es gilt sicher $ab^{-1} \in U_G$ und aus $a'(b')^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) \in \varphi(U_G)$ folgt die Behauptung.

d) Seien $a, b \in \varphi^{-1}(U_H)$ und daher $\varphi(a), \varphi(b) \in U_H$. Dann folgt die Behauptung direkt aus $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} \in U_H \Rightarrow ab^{-1} \in \varphi(H)$.

e) "$\Rightarrow$" $\varphi(e_G) = e_H$ und $\varphi(a) = e_H \Rightarrow a = e$
"$\Leftarrow$" Seien $a, b \in G$ und $\varphi(a) = \varphi(b)$. Dann ist $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H$, also $ab^{-1} \in \ker\varphi = \{e_G\}$, also muss $a = b$ gelten.

□

Definition 7. Eine Untergruppe $N < G$ heißt ***Normalteiler*** (in Zeichen $N \lhd G$), wenn für alle $a \in G$ gilt: $aH = Ha$.

Satz 8. *Sei G eine Gruppe und $N \lhd G$ ein Normalteiler. Dann gibt es genau eine Verknüpfung $\circ$ auf der Menge G/N mit den Eigenschaften:*

a) *$(G/N, \circ)$ ist eine kommutative Gruppe.*

b) *Die Abbildung $\pi : G \to G/N, a \mapsto aN$ ist ein Gruppenepimorphismus mit Kern N und heißt der **kanonische Morphismus** zu N.*

Beweis. [11, S. 48], [4, S. 35]

a) Seien $a, b \in G$ und $N \lhd G$ ein Normalteiler. Wir definieren die Verknüpfung $\circ$ durch $(aN) \circ (bN) := (ab)N$ und müssen zeigen, dass sie unabhängig von der Wahl der Repräsentanten ist. Seien $a', b' \in G$ mit $aN = a'N, bN = b'N$, also $a^{-1}a', b^{-1}b' \in N$. Dann gibt es $x, y \in N$, sodass $xb' = b'y$. Wir setzen $x = a^{-1}a'$, sodass gilt

$$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = b^{-1}xb' = b^{-1}b'y \in N.$$

Damit haben wir die Wohldefiniertheit gezeigt. Die Verknüpfung ist assoziativ, da

$$((aN) \circ (bN)) \circ (cN) = ((ab)N) \circ (cN) = ((ab)c) \circ N.$$

b) Die Abbildung ist ein Homomorphismus, da für $a, b \in G$ gilt

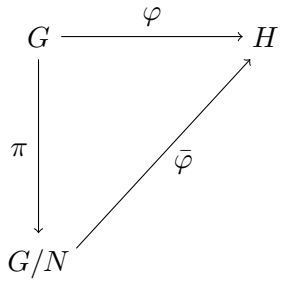
$$\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b)$$

und daher ist die Verknüpfung eindeutig bestimmt. Jedes $aN \in G/N$ ist ein Bild von $\pi(a)$ und deswegen ist die Abbildung auch surjektiv und es gilt wegen $a \in \ker\pi \Leftrightarrow N = \pi(a) = aN \Leftrightarrow a \in N$ auch $\ker\pi = N$.

□

Das neutrale Element von G/N ist N und das Inverse von aN ist $a^{-1}N$.
G/N heißt die ***Faktorgruppe von G nach N***.
Die Verknüpfung in G/N wird häufig genauso genannt wie in G. So wird die Addition beispielsweise beschrieben durch $(a+N)+(b+N) = (a+b)+N$.

Satz 9 (Homomorphiesatz)**.** *Sei $\varphi : G \to H$ ein Gruppenhomomorphismus, $N \lhd G$ ein Normalteiler mit $N \subset \ker\varphi$. Sei weiter $\pi : G \to G/N$ der kanonische Gruppenepimorphismus. Dann gibt es genau eine Abbildung $\bar{\varphi} : G/N \to H$ mit $\varphi = \bar{\varphi} \circ \pi$, die das folgende Diagramm erfüllt:*



$\bar{\varphi}$ ist ein Gruppenhomomorphismus und es gilt: $\bar{\varphi}(G/N) = \varphi(G)$, $\ker\bar{\varphi} = \pi(\ker\varphi)$.

Beweis. $\bar{\varphi}$ ist eindeutig bestimmt, da aus $\bar{\varphi} = \varphi \circ \pi$ für alle $a \in G$ folgt $\bar{\varphi}(aN) = \bar{\varphi}(\pi(a)) = \varphi(a)$.
$\bar{\varphi}$ ist wohldefiniert, weil aus $\bar{\varphi}(aN) = \varphi(a)$ für alle Elemente $a, b \in G$ mit $aN = bN$ folgt $b^{-1}a \in N \subset \ker\varphi$. Also ist $e_H = \varphi(b^{-1}a) = \varphi(b)^{-1} \cdot \varphi(a)$ und daher $\varphi(a) = \varphi(b)$.
Die Abbildung ist ein Homomorphismus wegen

$$\bar{\varphi}((aN)(bN) = \bar{\varphi}((ab)N) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(aN)\bar{\varphi}(bN).$$

Die Behauptungen $\bar{\varphi}(G/N) = \varphi(G)$ und $\ker\bar{\varphi} = \pi(\ker\varphi)$ folgen aus der Definition von $\bar{\varphi}$ und der Surjektivität von π. □

Aus dem Homomorphiesatz folgt

Korollar 10 (1. Isomorphiesatz)**.** *Seien $\varphi, \pi, \bar{\varphi}$ definiert wie im Homomorphiesatz 9, dann gilt:*

- *$\bar{\varphi}$ ist bijektiv genau dann, wenn $N = \ker \varphi$.*
- *Ist φ surjektiv, dann gilt $H \cong G/\ker \varphi$.*

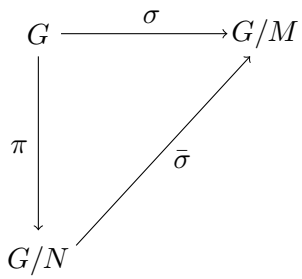
Beweis. Aus $N = \ker \varphi$ folgt, dass $\bar{\varphi}$ injektiv ist. Die Surjektivität folgt aus $\bar{\varphi}(G/N) = \varphi(G)$, damit ist $\bar{\varphi}$ ein Gruppenisomorphismus. □

Der zweite Isomorphiesatz ist für diese Arbeit nicht relevant, daher springen wir direkt zu

Satz 11 (3. Isomorphiesatz)**.** *Sei G Gruppe und $N \lhd G, M \lhd G$ Normalteiler mit $N \subset M$. Dann gilt:*

- *$N \lhd M \lhd G$ und $M/N \lhd G/N$*
- *Der Gruppenhomomorphismus $\varphi : (G/N)/(M/N) \to G/M, (aN)(M/N) \mapsto aM$ ist ein Isomorphismus.*

Beweis. Wir stellen den Zusammenhang erneut mit einem Diagramm dar, wobei π bzw. σ die kanonischen Gruppenepimorphismen zu N bzw. M sind:



Nach dem Homomorphiesatz ist $\bar{\sigma}(aN) = aM$ und wegen der Surjektivität der beiden Abbildungen gilt $\ker \pi = N$ und $\ker \sigma = M \supset N$. Aus $\ker \bar{\sigma} = (\ker \sigma)/N = M/N$ folgt daher sofort $M/N \lhd G/N$. Wenden wir nun erneut den Homomorphisatz gemeinsam mit dem 1. Isomorphisatz an erhalten wir den behaupteten Isomorphismus $(G/N)/(M/N) \to G/M$. □

2.2 Ring

Definition 12. Ein ***Ring*** $(R, +, \cdot)$ ist eine Menge R zusammen mit zwei Verknüpfungen $+$ und $\cdot$, die folgende Bedingungen erfüllen:

(R1) $(R, +, 0)$ ist eine kommutative Gruppe.

(R2) $(R, \cdot)$ ist assoziativ, man sagt auch $(R, \cdot)$ ist Halbgruppe und hat ein Einselement 1.

(R3) Es gelten die ***Distributivgesetze***, d.h. für alle $a, b, c \in R$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(b + c) \cdot a = b \cdot a + c \cdot a$.

Ein Ring heißt ***kommutativ***, wenn die Multiplikation die Regel
$a \cdot b = b \cdot a$ für alle $a, b \in R$ erfüllt.
Ist das Einselement des Rings R zusätzlich ungleich 0, so heißt R ***kommutativer Ring mit Einselement***.

In einem Ring mit Einselement gilt für alle Elemente $a \in R$:

$$(-1)a = a(-1) = -a.$$

Weitere algebraische Eigenschaften von Ringen sind:

Bemerkung 13. Sei R ein Ring mit Nullelement 0, dann gilt für alle $a, b \in R$:

- $a0 = 0a = 0$
- $(-a)b = a(-b) = -(ab)$
- $(-a)(-b) = ab$

Beweis.

- $a0 = a(0 + 0) = a0 + a0 \quad | - a0$
  $0 = a0$
  analog für $0a = 0$
- $ab + (-a)b = (a + (-a))b = 0b = 0$
  Aus der Eindeutigkeit des Inversen folgt wegen $ab + -(ab) = 0$ sofort $(ab) = (-a)b$.
  analog für $-(ab) = a(-b)$
- $ab = -(-(ab) = -(a(-b)) = (-a)(-b)$

□

Analog zu Abbildungen in Gruppen gibt es in Ringen **Ringhomomorphismen** und alle weiteren in Definition 2 gegebenen Bezeichnungen, wie Monomorphismus, Epimorphismus, Isomorphismus und Kern, die von den Eigenschaften der jeweiligen Abbildung abhängen.

Definition 14. Seien R ein Ring und S eine Teilmenge von R ($S \subset R$). Dann heißt S ***Unterring*** von R, wenn gilt:

(UR1) S ist abgeschlossen bezüglich der Addition und der Multiplikation, also für $a, b \in S$ ist auch $a + b \in S$ und $a \cdot b \in S$.

(UR2) S mit den von R vererbten Verknüpfungen $+$ und $\cdot$ ist wieder ein Ring.

Für die Untersuchung in der Praxis wird analog zur Untersuchung von Untergruppen eine Bemerkung verwendet:

Bemerkung 15. Eine Teilmenge $S \subset R$ ist genau dann Unterring, wenn folgendes gilt:

(a) $S \neq \emptyset$

(b) $a, b \in S \Rightarrow a - b \in S$ und $a \cdot b \in S$

Beweis. Aus dem analogen Kriterium für Untergruppen, siehe Bemerkung 4, folgt der Beweis sofort. □

Beispiel 16.

- $(\mathbb{Z}, +, \cdot)$ ist ein Unterring von $(\mathbb{Q}, +, \cdot)$.
- $(\mathbb{Q}, +, \cdot)$ ist ein Unterring von $(\mathbb{C}, +, \cdot)$.

Definition 17. Sei $(R, +, \cdot)$ ein kommutativer Ring.

- Die Elemente des Rings a, b heißen ***Nullteiler***, wenn gilt $ab = 0$.
  R heißt ***nullteilerfrei***, wenn es keine Nullteiler außer 0 gibt, also wenn aus $ab = 0$ sofort $a = 0$ oder $b = 0$ folgt.
- Besitzt der Ring R ein Einselement ungleich 0 und ist zusätzlich nullteilerfrei, so heißt R ***Integritätsbereich***.

2.2.1 Körper

Definition 18. Eine Menge K zusammen mit den beiden Verknüpfungen + und $\cdot$ heißt ***Körper*** $(K, +, \cdot)$, wenn folgende Bedingungen für alle Elemente $a, b, c \in K$ erfüllt werden:

(K1) $(K, +, \cdot)$ ist ein Ring mit Einselement.

(K2) $(K \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe.

(K3) Es gilt das Distributivgesetz: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Anders gesagt müssen $(K, +, 0)$ und $(K \setminus \{0\}, \cdot, 1)$ kommutative Gruppen mit Null- bzw. Einselement sein und zusätzlich das Distributivgesetz für die Kombination der beiden Operationen erfüllt werden.
Ein Integritätsbereich ist genau dann ein Körper, wenn ein inverses Element der Multiplikation existiert.
Ein Körper, in dem die Multiplikation nicht kommutativ ist, heißt **Schiefkörper**.

In einem Körper gelten die folgenden algebraischen Gesetze:

Bemerkung 19. Sei K ein Körper und enthält $a, b \in K$, dann gilt:

- $(ab)^{-1} = a^{-1}b^{-1}$
- $(-a)^{-1} = -a^{-1}$

Beweis.

- $(ab) \cdot (a^{-1}b^{-1}) = aba^{-1}b^{-1} = aa^{-1}bb^{-1} = 1 \cdot 1 = 1$
  Aus der Eindeutigkeit des Inversen folgt aus $(ab) \cdot (ab)^{-1} = 1$ sofort $(ab)^{-1} = a^{-1}b^{-1}$.
- $(-a)^{-1} = ((-1) \cdot a)^{-1} = (-1)^{-1} \cdot a^{-1}$
  Da $(-1)^{-1} \cdot (-1) = 1$ und daher $(-1)^{-1} = -1$, folgt $(-a)^{-1} = -a^{-1}$.

□

Auch für Abbildungen zwischen Körpern gelten die in Definition 2 gegebenen Bezeichnungen.

Definition 20. Für den Körper $(K, +, \cdot)$ und die in K enthaltene Teilmenge J ($J \subset K$) heißt J genau dann ***Unterkörper*** von K, wenn J mit den vererbten Verknüpfungen $+$ und $\cdot$ selbst ein Körper ist.

Beispiel 21.

- $(\mathbb{R}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{C}, +, \cdot)$.
- $\mathbb{Q}[\mathrm{i}] := \{a + \mathrm{i}b : a, b \in \mathbb{Q}\}$ ist ein Unterkörper von $\mathbb{C}$ mit dem inversen Element $\mathbb{C} \ni (a + \mathrm{i}b)^{-1} = \frac{a}{a^2-b^2} - \mathrm{i}\frac{b}{a^2-b2} \in \mathbb{Q}[\mathrm{i}]$.
- $\mathbb{Q}[\omega] := \{a + \omega b : a, b \in \mathbb{Q}\}$ ist ein Unterkörper von $\mathbb{C}$ mit dem inversen Element $\mathbb{C} \ni (a + \omega b)^{-1} = \frac{a-b}{a^2-ab+b^2} - \omega\frac{b}{a^2-ab+b^2} \in \mathbb{Q}[\omega]$. [2]

2.2.2 Teilbarkeit in Integritätsbereichen

Ein wesentlicher Teil dieser Arbeit wird dem Erarbeiten der Teilbarkeit im Ring der Eisensteinzahlen gewidmet. Daher ist eine genaue Betrachtung der Teilbarkeit in Integritätsbereichen notwendig, um die darin kennengelernten Grundsätze und Begriffe auf den Ring der Eisensteinzahlen übertragen zu können.

Sei für die folgenden Behauptungen R immer ein Integritätsbereich, also ein nullteilerfreier, kommutativer Ring mit Einselement.

Definition 22. Seien $a, b, e \in R$.

- a heißt ***Teiler*** von b, falls es ein $c \in R$ gibt, sodass $a \cdot c = b$. Man schreibt $a \mid b$. b heißt ***Vielfaches*** von a.
- e heißt ***Einheit*** von R, falls es ein Inverses bezüglich der Multiplikation besitzt, also falls gilt: $ee^{-1} = e^{-1}e = 1$. Analog gilt: $e \mid 1$
- Die Elemente a, b heißen ***assoziiert***, wenn gilt $a \mid b$ und $b \mid a$. Man schreibt $a \sim b$.

[2] ω bezeichnet die primitive, dritte Einheitswurzel mit $\omega = \mathrm{e}^{\frac{2\pi\mathrm{i}}{3}}$.

Es ist schnell gezeigt, dass die Relation $\sim$ eine Äquivalenzrelation ist [9].

Bemerkung 23. Die Menge R^* aller Einheiten in einem Ring R mit Einselement bildet eine kommutative Gruppe bezüglich der Multiplikation, die ***Einheitengruppe*** von R.

Beweis. Für $a, b \in R^*$ gibt es $a^{-1}, b^{-1} \in R$, sodass $aa^{-1} = a^{-1}a = 1 \in R^*$ also ist das Inverse $a^{-1} \in R^*$ und wegen $(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab)$ mit $(ab)^{-1} = b^{-1}a^{-1}$ ist auch das Produkt $a \cdot b \in R^*$. □

Lemma 24 (Rechenregeln für Teilerbarkeit)**.** *Für alle Elemente $a_i, b_i, c_i \in R, e \in R^*$ gilt:*

(i) $a \mid a, a \mid 0, 1 \mid a$

(ii) $0 \mid a \Leftrightarrow a = 0$

(iii) $a \mid b \wedge b \mid c \Rightarrow a \mid c$ *("$\mid$" ist transitiv.)*

(iv) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$

(v) Es ist $e \in R^*$ genau dann, wenn e alle $a \in R \setminus \{0\}$ teilt.

(vi) Falls $c \in R \setminus \{0\}$, dann gilt: $a \mid b \Leftrightarrow ac \mid bc$.

(vii) a ist genau dann assoziiert zu b, wenn $a = eb$ mit $e \in R^*$.

(viii) Falls $a \mid b_1$, $a \mid b_2$ ... $a \mid b_n$, dann gilt für alle $c_1, c_2, ..., c_n \in R : a \mid (c_1b_1 + c_2b_2 + ... + c_nb_n)$.

Beweis. [4, S. 206f],[S. 5f][9],[S. 86f][10]

(i) R ist Integritätsbereich und hat daher ein Einselement 1. Aus $1 \cdot a = a \cdot 1 = a$ folgt sofort $1 \mid a$ und $a \mid a$. Aus $0 \cdot a = 0$ folgt sofort $a \mid 0$.

(ii) Gilt $0 \mid a$, so ist $0 \cdot x = a$. Aus $0 \cdot x = 0$ folgt sofort $a = 0$.

(iii) Sei $a \cdot x = b$ und $b \cdot y = c$. Dann folgt aus $a \cdot x \cdot y = c$ sofort $a \mid c$.

(iv) Sei $a \cdot x = b$ und $c \cdot y = d$. Dann folgt aus $b \cdot d = ax \cdot cy = ac \cdot (xy)$ sofort $ac \mid bd$.

(v) "$\Leftarrow$:" Wenn e alle $a \in R \setminus \{0\}$ teilt, dann gilt auch $e \mid 1$ und damit ist nach Definition der Einheiten $e \in R^*$.
"$\Rightarrow$:" Ist e eine Einheit, so gilt $ee^{-1} = 1$ und daher $e \mid 1$. Nach (i) gilt auch $1 \mid e$ und daher ist $e \sim 1$. Für alle $a \in R \setminus \{0\}$ gilt wegen (i) $1 \mid a$ und daraus folgt $e \mid a$.

(vi) "$\Rightarrow$:" Sei $a \cdot x = b$. Dann folgt aus $a \cdot x \cdot c = a \cdot c \cdot x = b \cdot c$ sofort $ac \mid bc$.
"$\Leftarrow$:" Sei $ac \cdot x = bc$. Dann folgt aus $ac \cdot x \cdot c^{-1} = a \cdot x \cdot cc^{-1} = a \cdot x \cdot 1 = bc \cdot c^{-1} = b$ sofort $a \mid b$.

(vii) Aus $a = eb$ folgt $b \mid a$. Aus $a = 1 \cdot a = ee^{-1}a = eb$ folgt mithilfe der Kürzungsregel sofort $a \mid b$ und daher $a \sim b$.

(viii) Sei für alle $b_i = a \cdot x_i$. Dann ist $b_i \cdot c_i = a \cdot x_i \cdot c_i$. Aus

$$ax_1c_1 + ax_2c_2 + ... + ax_nc_n = b_1c_1 + b_2c_2 + ... + b_nc_n$$
$$a \cdot (x_1c_1 + x_2c_2 + ... + x_nc_n) = b_1c_1 + b_2c_2 + ... + b_nc_n$$

folgt $a(b_1c_1 + b_2c_2 + ... + b_nc_n)$.

□

Definition 25. Seien $a, b, c, e \in R$ mit $a \notin R^*, a \neq 0, e \in R^*$.

- Das Element a heißt ***echter Teiler*** von b, falls $a \mid b$ und $a \neq e \cdot b$ für alle $e \in R^*$. Die Elemente a und $e \in R^*$ heißen die trivialen Teiler von a.
- a heißt ***unzerlegbar*** oder ***irreduzibel***, falls a keinen echten Teiler besitzt, also wenn gilt: $a = b \cdot c \Rightarrow b \in R^* \vee c \in R^*$.
- Das Element a heißt ***prim***, falls gilt: $a \mid bc \Rightarrow a \mid b \vee a \mid c$.

Bemerkung 26. Jedes Primelement in R ist irreduzibel.

Beweis. Sei p prim und $p = ab$.
Aus der Definition folgt sofort $p \mid a \vee p \mid b$.
Gelte o.B.d.A. $p \mid a$, sodass $a = c \cdot p$ mit $c \in R$.
Dann gilt weiter: $p = a \cdot b = c \cdot p \cdot b = (c \cdot b) \cdot p$ und somit muss $b \in R^*$ gelten.

□

Diese Bemerkung hat im späteren Verlauf eine zentrale Relevanz. Einerseits werden Ringe besprochen, in denen auch die Umkehrung: "Jedes irreduzible Element ist ein Primelement," gilt. Andererseits wird die Bedeutung des Unterschieds der Begriffe *irreduzibel* und *prim* in Bezug auf alle Unterkörper der Menge der komplexen Zahlen $\mathbb{C}$ näher untersucht.

Definition 27. Ein Element $x \in R$ heißt ***gemeinsamer Teiler*** von a und b, $a, b \in R$, wenn gilt: $x \mid a$ und $x \mid b$.
a und b heißen ***teilerfremd***, wenn sie keine gemeinsamen, echten Teiler besitzen.

Definition 28. Ein Element $d \in R$ heißt ***größter gemeinsamer Teiler*** (oder kurz ***ggT***) einer Teilmenge $M \subseteq R, M \neq \emptyset$, wenn gilt:

- $d \mid a$ für jedes $a \in M$
- $d' \mid a$ für jedes $a \in M \Rightarrow d' \mid d$

Übliche Notationen für den größten gemeinsamen Teiler sind $ggT(a, b) = d$ oder noch kürzer $(a, b) = d$.

Bemerkung 29. Der ggT ist bis auf Assoziiertheit eindeutig bestimmt.

Beweis. Sei $d \in R$ der größte gemeinsame Teiler der Teilmenge $M \subseteq R, M \neq \emptyset$ und $d' \in R$ ein weiterer ggT dieser Menge M. Dann gilt wegen obiger Definition $d' \mid d$ und $d \mid d'$ und daher ist $d \sim d'$. □

Einige wichtige Eigenschaften des größten gemeinsamen Teilers werden notiert im folgenden

Lemma 30. *Seien alle $a_i, b_i, c_i \in R$ und keine Einheiten. Dann gelten die folgenden Bedingungen:*

(i) Haben je zwei Elemente einer endlichen Menge $M = \{a_1, ..., a_n\}$ einen ggT, so hat hat die Menge M einen $ggT = d$, das heißt $d \mid a_i$ für $1 \leq i \leq n$ und $d' \mid a \Rightarrow d' \mid d$.

(ii) $((a, b), c) \sim (a, (b, c))$

(iii) $c(a, b) \sim (ca, cb)$

(iv) Aus $(a, b) = 1$ *und* $(a, c) = 1$ *folgt* $(a, bc) = 1$.

Beweis. [10, S. 144f]

(i) Sei $d_1 = (a_1, a_2), d_2 = (d_1, a_3), ..., d = d_r = (d_{r-1}, a_r)$. Dann folgt aus der Definition sofort, dass d der größte gemeinsame Teiler aller a_i ist.

(ii) Beide Ausdrücke entsprechen dem $ggT(a, b, c)$.

(iii) Seien $(a, b) = d$ und $(ca, cb) = f$. Dann gilt sicher $cd \mid f$. Deshalb ist $f = cd \cdot e, e \in R^*$. Daraus folgt auch, dass $a = d \cdot e \cdot x, x \in R$ mit $x \cdot f = c$. Aus der analogen Ausführung für b ergibt sich: $de \mid a, de \mid b, de \mid d$, also $(ca, cb) \sim cd \sim c(a, b)$.

(iv) Aus $(a, b) = 1$, $(a, ac) \sim a$ und (iii) folgt, dass $(ac, bc) \sim c$. Daraus ergibt sich weiter:

$$1 \sim (a, c) \sim (a, (ac, bc)) \sim ((a, ac), bc) \sim (a, bc).$$

□

Definition 31. Sei R ein Integritätsbereich und seien alle $d_i \in R$. Dann heißt die Folge $(d_1, ..., d_n, ...), n \in \mathbb{N}$ ***Teilerkette***, wenn für alle d_i gilt:

$$d_{i+1} \mid d_i.$$

In einem Integritätsbereich R gilt der ***Teilerkettensatz***, wenn jede Teilerkette ***stationär*** wird, das heißt es gibt ein letztes Element der Teilerkette $n_0 \in \mathbb{N}$, sodass $d_n \sim d_{n+1}$ für alle $n \geq n_0$ [4, S. 209].
In manchen Lehrbüchern ist eine etwas andere Formulierung des Teilerkettensatzes zu finden, indem es heißt: In R gilt der Teilerkettensatz, wenn es keine aufsteigende Kette von Teilern für alle Elemente $a \in R$ gibt.

2.2.3 Ideale

Die Entwicklung von Mengen mit "idealen Zahlen" war der Anreiz der Entstehung der Ideale. Sie sollen innerhalb der Ringtheorie die Anwendung der Teilbarkeit vereinfachen. Dabei sind Ideale in der Ringtheorie das Analogon zu Normalteilern und ebenfalls zu Faktorgruppen in der Gruppentheorie.

Definition 32. Sei R ein Ring und $I \subset R$ eine Teilmenge von R.

(I1) Eine additive Untergruppe I von R, also $I < (R, +0)$, heißt genau dann ein ***Ideal*** von R, wenn $a + b \in I$ und $ra \in I$ für alle $a, b \in I$ und $r \in R$.

(I2) Das Ideal I eines Rings R heißt das von a erzeugte ***Hauptideal***, falls es ein $a \in R$ gibt, sodass: $I = (a) := Ra := \{ra : r \in R\}$.

(I3) $I \neq R$ heißt außerdem ***Primideal*** von R, falls aus $a \cdot b \in I$ folgt: $a \in I$ oder $b \in I$.

(I4) I heißt ***maximales Ideal*** von R, wenn für jedes Ideal $A \subseteq R$ mit $I \subseteq A$ sofort $I = A$ oder $A = R$ folgt.

Die Ideale (0) und $(1) = R$ heißen ***triviale Ideale*** von R.
Jedes Ideal ist nach dieser Definition auch ein Unterring von R, aber nicht umgekehrt.

Beispiel 33.

- Die geraden Zahlen bilden ein Ideal von $\mathbb{Z}$. Sie sind sogar ein Hauptideal, da sie aus der Ziffer 2 gebildet werden können: $(2) = \{2x : x \in \mathbb{Z}\}$.
- Jedes von einer Primzahl erzeugte Hauptideal in $\mathbb{Z}$ ist ein Primideal und sogar ein maximales Ideal.

Lemma 34 (Rechenregeln für Ideale)**.** *Sei R ein Ring und seien I, J, K Ideale von R, dann gilt:*

(i) Sei (M) die Schnittmenge aller Ideale von R, die die Teilmenge $M \subseteq R$ enthalten. Dann ist (M) ebenfalls ein Ideal von R und heißt das von M erzeugte Ideal. Ist M selbst ein Ideal von R, so gilt $M = (M)$.

(ii) Sei $K = (I \cup J) =: I + J$, das heißt für jedes Element $k \in K$ gilt $k = a + b$ für gewisse $a \in I$ und $b \in J$. Dann ist K ein Ideal von R und ist das kleinste Ideal, das I und J enthält.

(iii) Sei $K = IJ =: (ab)$ mit $a \in I, b \in J$. Dann ist K ein Ideal von R.

(iv) "Aufsteigende Kette von Idealen": Seien $I_1, I_2, ...$ Ideale von R mit $I_1 \subset I_2 \subset \cdots$, dann gilt: $\bigcup I_j$ mit $j \in \mathbb{N}$ ist ein Ideal von R.

(v) Seien $a, b \in R$. Dann teilt a das Element b genau dann, wenn $(b) \subseteq (a)$. Es gilt $(a) = (b)$ genau dann, wenn $a \sim b$.

(vi) Es ist $e \in R^*$ genau dann, wenn $(e) = R$ gilt.

Beweis. [4, S. 184, S. 192][10, S. 101f][11, S. 203]

(i) Sofort aus der Definition folgt der erste Teil der Aussage: Die Schnittmenge von Idealen ist wieder ein Ideal in R.
Sei $M = \{a_1, a_2, ..., a_n\}, n \in \mathbb{N}$ und (M) eben jene Schnittmenge, also

$$(M) := \bigcap_{M \subset I \subset R} I,$$

wobei I ein Ideal von R ist, also es gilt $a + b \in I, ra \in I$ für alle $a, b \in I, r \in R$.
Wir wollen zeigen, dass gilt

$$x \in (M) \Leftrightarrow x = \sum_{a \in M, r \in R} ra.$$

Das heißt (M) ist die Menge aller endlicher Linearkombinationen von Elementen aus M und weiter das kleinste M enthaltende Ideal.

"$\Rightarrow$" Nach Definition 32 muss gelten

$$\begin{aligned}(M) &= (a_1, ..., a_n)\\ &\supseteq \sum_{a_i \in M, r_i \in R} r_i a_i\\ &\Rightarrow \text{ jedes } M \ni x_i = \sum_{a_i \in M} ra_i : r \in R.\end{aligned}$$

"$\Leftarrow$"

$$x = \sum_{a_i \in M, r_i \in R} r_i a_i \Rightarrow x \in (M),$$

$$\text{da } a_i \in M \subseteq (M) \Rightarrow r_i a_i \in (M) \Rightarrow \sum_{a_i \in M, r_i \in R} r_i a_i \in (M)$$

(ii) folgt direkt aus (i)

(iii) Aus der Definition folgt direkt, dass K ein Ideal von R ist, das gleichzusetzen ist mit der Menge aller Elemente der Form $a_1b_1 + a_2b_2 + ... + a_mb_m$ mit $a_i \in I$ und $b_i \in J$.

(iv) Zu zeigen ist, dass die Vereinigung dieser aufsteigenden Kette von Idealen selbst ein Ideal ist. Dazu genügt es zu zeigen, dass $\bigcup I_J$ abgeschlossen bezüglich der Subtraktion und der beidseitigen Multiplikation mit beliebigen Elementen von R ist.
Subtraktion: Sei $a, b \in \bigcup I_j$. Dann ist $a \in I_j$ für ein j und $b \in I_k$ für ein k. Sei o.B.d.A. $k > j$, dann muss a ebenfalls in I_k liegen, da $I_j \subset I_k$. Daher gilt $a - b \in I_k$.
Multiplikation: Es gilt sicher auch ra und $ar \in I_j$ für ein $r \in R$. Somit muss $a - b \in \bigcup I_j$ und $ra, ar \in \bigcup I_j$ für alle $a, b \in \bigcup I_j, r \in R$ gelten.

(v) Da $a \mid b$ gilt $b \in Ra$. Wegen $(b) = Rb$ folgt daher sofort $Rb \subseteq Ra = (a)$.

(vi) Aus 24 und (v) folgt die Behauptung sofort.

□

Satz 35. *Sei R kommutativer Ring $\neq \emptyset$. R ist ein Körper genau dann, wenn die einzigen Ideale in R die trivialen Ideale* (1) *und* (0) *sind.*

Beweis. [10, S. 102]

"$\Rightarrow$": Sei R kommutativer Ring $\neq 0$. Seien (0) und R die einzigen Ideale in R. Für ein Element $0 \neq a \in R$ ist das Ideal $(a) \neq (0)$ und daher $(a) = R$. Dann existiert ein $r \in R$, sodass $1 \in (a) = ar$ und damit muss R ein Körper sein, indem ein zu a inverses Element $r \in R$ existiert, sodass $ar = 1$.

"$\Leftarrow$": Sei R ein Schiefkörper, also ein Körper ohne Kommutativität der Multiplikation. Sei I ein Ideal in R. Wenn I ein Element $a \neq 0$ enthält, dann enthält das Ideal auch $R \ni aa^{-1} = 1$. Das einzige Ideal, das 1 enthält ist R und damit ist $I = R$.

□

Lemma 36. *Seien R, S Ringe und $\varphi : R \to S$ ein Ringhomomorphismus. Dann gilt:*

a) Ist $J \subset S$ ein Ideal, dann ist $\varphi^{-1}(J)$ ein Ideal von R.

b) Ist φ surjektiv und ist $I \subset R$ ein Ideal, dann ist $\varphi(I)$ ein Ideal von S.

Beweis. [4, S. 177]

a) Nach dem Kriterium für Gruppen, Lemma 6 ist $\varphi^{-1}(J)$ eine Untergruppe von R. Sei $a \in \varphi^{-1}(J)$ und $r \in R$ und damit $\varphi(a) \in J$, so folgen

$$\varphi(ra) = \varphi(r)\varphi(a) \in J \Rightarrow ra \in \varphi^{-1}(J) \quad \text{und} \quad \varphi(ar) = \varphi(a)\varphi(r) \in J \Rightarrow ar \in \varphi^{-1}(J),$$

also ist J ein Ideal von R.

b) $\varphi(I)$ ist nach Lemma 6 eine Untergruppe. Sei $b \in \varphi(I)$ und $s \in S$, dann gibt es ein $a \in I$ und ein $r \in R$, sodass $b = \varphi(a)$ und $s = \varphi(r)$. Daher ist $sb = \varphi(ra) \in \varphi(I)$ und ebenso $bs \in \varphi(I)$.

□

Definition 37. Ein Integritätsbereich R, in dem jedes Ideal ein Hauptideal ist, heißt ***Hauptidealring***.

Nach dieser Definition gilt jedenfalls: Jeder Körper ist ein Hauptidealring [11, S. 213]. Für jeden kommutativen Integritätsbereich R kann mithilfe dieser Rechenregeln zu Idealen noch einiges über die Teilbarkeit in R formuliert werden:

Beispiel 38 (Teilbarkeit und Ideale)**.** Die Menge R^* ist multiplikative Gruppe von R und damit gilt die Kürzungsregel. Für die Elemente $a, b, c \in R$ mit den von ihnen erzeugten Hauptidealen $(a), (b)$ gilt:
$b \mid a \Leftrightarrow (b) \supset (a)$, weil
$(b) \subset (a) \Leftrightarrow a \in (b) \Leftrightarrow a = bc$.
Die Elemente a und b sind in R^* assoziiert genau dann, wenn $b \mid a$ und $a \mid b$ gilt. Dies gilt wiederum nur, wenn $(b) \supset (a)$ und $(a) \supset (b)$, also nur wenn $(a) = (b)$.
a kann also nur dann ein echtes Vielfaches von b sein, wenn $(a) \supsetneq (b)$

Dieses Beispiel führt uns direkt zur folgenden wichtigen Feststellung. Aus Definition 31 und dem Teilerkettensatz in Integritätsbereichen lässt sich für Hauptideale festhalten:

Satz 39 (Teilerkettensatz für Hauptidealringe)**.** *In jedem Hauptidealring gilt der Teilerkettensatz.*

Beweis. Sei R Hauptidealring und alle $(a_i), i \in \mathbb{N}$ Ideale von R.
Angenommen es gibt eine Teilerkette in R, sodass:

$$(a_0) \subset (a_1) \subset (a_2) \subset ...,$$

dann ist ihre Vereinigungsmenge $\bigcup(a_i)$ nach (i), Satz 34 ein Ideal in R, mit $\bigcup(a_i) = (d)$ für manche $d \in R$. Es ist auch $d \in (a_i)$ für ein i und daher $(d) \subset (a_i)$. Für $m, n \in \mathbb{N}$ und $i \leq m \leq n$ muss daher gelten $(a_m) \supset (a_n) \supset \bigcup(a_i) = (d) \supset (a_m)$ und dies führt zu $(a_n) \sim (a_{n+1})$ für alle $n \geq i$. □

Eine äquivalente Formulierung für den Teilerkettensatz in Hauptidealen ist: Der Integritätsbereich R enthält keine unendlich aufsteigende Kette von Hauptidealen [4, S. 210][10, S. 142].

Definition 40. Sei R Ring und I ein Ideal in R. Dann heißt $r \in R$ kongruent zu $r', (r \equiv r')$, wenn $r - r' \in I$.
Weiter heißt $R/I = \{r + I : r \in R\}$ der ***Faktorring*** oder ***Restklassenring*** von R modulo I, wobei Addition und Multiplikation für $x, y \in R$ wie folgt definiert sind:

(1) $(x + I) + (y + I) := (x + y) + I$ und

(2) $(x + I) \cdot (y + I) := xy + I$,

wobei $(x + I) := \{x + a : a \in I\}$.

Die Wohldefiniertheit der Addition folgt direkt aus dem bereits gezeigten Kriterium für Faktorgruppen 8. Um die Wohldefiniertheit der Multiplikation zu beweisen, müssen wir zeigen, dass sie unabhängig von der Wahl der Repräsentanten ist:

Beweis. Seien $x, y, x', y' \in R$ und I ein Ideal von R. Gelte $x + I = x' + I, y + I = y' + I$, also $x' = x + a$ und $y' = y + b$ für $a, b \in I$. Dann folgt aus

$$x'y' - xy = (x + a)(y + b) - xy = ay + xb + ab \in Ix'y' + I = xy + I$$

die Wohldefiniertheit. □

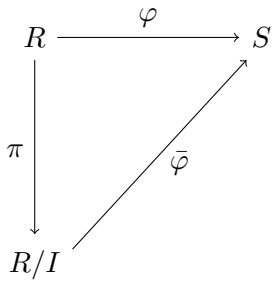
Wir übertragen das Assoziativgesetz und das Distributivgesetz direkt von R auf R/I und haben damit gezeigt, dass R/I ein Ring ist.
Für den Faktorring R/I gilt: I ist das neutrale Element der Addition und $(1+I)$ das Einselement.
Ist der Restklassenring R/I ein Körper, so heißt er ***Restklassenkörper***.

Lemma 41. *Sei R Ring und I ein Ideal von R. Die Abbildung $\pi : R \to R/I, r \mapsto r+I$ mit $r \in R$ ist ein Ringepimorphismus mit $\ker \pi = I$ und heißt der kanonische Morphismus zu I.*

Beweis. Wir haben bereits gezeigt, dass R/I ein Ring ist. Wie für die Faktorgruppen, Lemma 8, folgt die Behauptung. □

Direkt aus der Gruppentheorie lassen sich der Homomorphiesatz und die Isomorphiesätze übertragen, wobei wir den Begriff des Normalteilers durch jenen des Ideals ersetzen.

Satz 42 (Homomorphiesatz)**.** *Sei $\varphi : R \to S$ ein Ringhomomorphismus, $I \subset R$ ein Ideal von R mit $I \subset \ker \varphi$. Sei weiter $\pi : R \to R/I$ der kanonische Ringepimorphismus. Dann gibt es genau eine Abbildung $\bar{\varphi} : R/I \to S$ mit $\varphi = \bar{\varphi} \circ \pi$, das heißt die das folgende Diagramm erfüllt:*



$\bar{\varphi}$ ist ein Ringhomomorphismus und es gilt: $\bar{\varphi}(R/I) = \varphi(R)$, $\ker \bar{\varphi} = \pi(\ker \varphi)$.

Korollar 43 (1. Isomorphiesatz)**.** *Seien $\varphi, \pi, \bar{\varphi}$ definiert wie im Homomorphiesatz 42, dann gilt:*

- *$\bar{\varphi}$ ist bijektiv genau dann, wenn $I = \ker \varphi$.*
- *Ist φ surjektiv, dann gilt $S \cong R/\ker \varphi$.*

Satz 44 (3. Isomorphiesatz)**.** *Sei R Ring und $I \subset R, J \subset R$ Ideale mit $I \subset J$. Dann gilt:*

- *J/I ist ein Ideal von R/I.*
- *Der Ringhomomorphismus $\varphi : (R/I)/(J/I) \to R/J, (r+I)(J/I) \mapsto r+J$ ist ein Isomorphismus.*

An dieser Stelle wollen wir einige interessante Zusammenhänge aus dem Vorangegangenen festhalten und halten uns dabei an die Quellen [2, S.37f][4, S. 198f][10, S. 104][11, S. 193f]:

Proposition 45. *Seien R ein kommutativer Ring mit Einselement und I ein Ideal von R. Es gelten:*

(i) I ist ein Primideal. $\Leftrightarrow$ R/I ist ein Integritätsbereich.

(ii) I ist maximal. $\Leftrightarrow$ R/I ist ein (Restklassen-) Körper.

(iii) I ist maximal. $\Rightarrow$ I ist Primideal.

Beweis.

(i) "$\Rightarrow$" Sei I Primideal von R und $a, b \in R$. Dann gilt im Restklassenring R/I: $(a+I)(b+I) = ab + I = I$. Aus $ab \in I$ folgt, dass a oder b ein Element von I sein müssen. Daraus folgt sofort $a + I = I$ oder $b + I = I$.

"$\Leftarrow$" Sei R/I nullteilerfrei und sei $ab \in I$. Dann gilt wegen $(a+I)(b+I) = 0 + I$ sofort $a \in I$ oder $b \in I$.

(ii) Sei I ein maximales Ideal. Dann gilt für jedes weitere Ideal $J \in R$ mit $I \subset J \subset R$ sofort $J = I$ oder $J = R$. Aus dem 3. Isomorphiesatz 44 folgt sofort, dass es in R/I nur die trivialen Ideale gibt und damit ist nach Satz 35 R/I ein Körper.

(iii) Sei I maximal. Dann ist R/I ein Körper und daher nullteilerfrei. Daraus folgt sofort I ist ein Primideal von R.

□

Mithilfe der Idealtheorie die Begriffe *irreduzibel* und *prim* aus Definition 25 ebenfalls unterschieden werden [4, S. 207][11, S. 203]:

Proposition 46. *Sei R ein Integritätsbereich und $0 \neq p \in R$, $p \notin R^*$. Dann gilt:*

- *p ist irreduzibel genau dann, wenn $(p) \subset R$ maximal unter allen Hauptidealen ist.*
- *p ist prim genau dann, wenn $(p) \subset R$ ein Primideal ist.*

Beweis. Für den Beweis dieser Aussage erinnern wir uns an die Rechenregeln für Ideale (v) und (vi) aus Lemma 34.

- "$\Rightarrow$": Sei p irreduzibel und $(p) \subset (a) \subsetneq R$ für ein $a \in R$, also $p = ar$ mit $r \in R$. Da p irreduzibel und $a \notin R^*$ sind, muss $r \in R^*$ gelten und daher $a \sim p$, also $(a) = (p)$. "$\Leftarrow$": Sei (p) ein maximales Hauptideal und $p = ab$ mit $a \notin R^*$. Dann folgt $(p) = (a)$, also $a = cp$ für ein $c \in R$. Aus $p = ab = (cp)b = (cb)p$ folgt $b \in R^*$, also ist p irreduzibel.

- "⇒": Sei p prim und $ab \in (p) = Rp$. Dann gilt $p \mid ab$, also $p \mid a$ oder $p \mid b$. Daher gilt $a \in (p)$ oder $b \in (p)$. Weil $(p) \neq R$ ist (p) ein Primideal.
  "⇐": Sei (p) ein Primideal und $p \mid ab$. Dann ist $ab \in (p)$, also $a \in (p)$ oder $b \in (p)$. Daher gilt $p \mid a$ oder $p \mid b$ und daher ist p prim.

□

Lemma 47 (Lemma von Bezout)**.** *Für alle Elemente a, b eines Hauptidealrings R gibt es $x, y \in R$, sodass $ggT(a, b) = xa + yb$.*

Beweis. Sei $I = (a, b)$ das von den Elementen erzeugte Ideal. Da R ein Hauptidealring ist, ist I ein Hauptideal. Daher gibt es ein Element $d \in R$ mit $I = (d)$. Aus $(a) \subseteq I = (d)$ bzw. $(b) \subseteq I = (d)$ folgt, dass d ein gemeinsamer Teiler von a und b ist. Sei nun d' ein weiterer gemeinsamer Teiler von a und b. Dann gilt $(d) = I \subseteq (e)$ und daher $e \mid d$. Daher ist $d = ggT(a, b)$ und wegen $d \in I = (a, b)$ kann der ggT mithilfe von $x, y \in R$ dargestellt werden. □

Ein Spezialfalls des Lemmas von Bézout liegt für teilerfremde a, b mit $ggT(a, b) = 1$ vor, da hieraus sofort die Gleichung $1 = xa + yb$ folgt. Insbesondere gilt auch die Umkehrung: Gibt es $x, y \in R$ für teilerfremde $a, b \in R$, sodass $1 = xa + yb$, dann gilt $ggT(a, b) = 1$. Der Beweis für teilerfremde a, b folgt aus $I = (a, b) = R$.

Aus den vorangegangenen Zusammenhängen ergeben sich zwei äußerst bedeutende Resultate, nämlich

Korollar 48. *In einem Hauptidealring ist jedes irreduzible Element prim.*

Beweis. Nach Bemerkung 26 gilt, dass jedes irreduzible Element prim ist. In Hauptidealen ist jedes Ideal ein Hauptideal, daher gilt nach Proposition 46 für ein Element $0 \neq p \in \mathbb{R}, p \notin R^*$: p ist irreduzibel $\Leftrightarrow$ (p) ist maximal $\Leftrightarrow$ (p) ist prim $\Leftrightarrow$ p ist prim. □

Ein Beweis für dieselbe Behauptung ohne Zuhilfenahme der Idealtheorie kann beispielsweise bei Scheid und Frommer [14, S. 90f] nachgelesen werden.

Korollar 49. *Je zwei irreduzible Elemente sind assoziiert oder teilerfremd.*

Beweis. Sei R Hauptidealring, $a \in R$ und $p \in R$ irreduzibel. Wir wollen zeigen, dass gilt: $p \mid a$ oder p und a sind teilerfremd.
Angenommen p und a sind nicht teilerfremd, dann gibt es einen gemeinsamen Teiler $x \in R$, sodass $x \mid p$ und $x \mid a$. Aus $x \mid p$ und $x \notin R^*$ folgt $x \simeq p$, also auch $p \mid a$. □

2.3 Zusammenhang: Hauptidealringe - faktorielle Ringe - euklidische Ringe

Es wurden nun die wichtigsten Grundlagen der Zahlentheorie erläutert. Im Weiteren werden die Strukturen Hauptidealring und faktorieller Ring mit einer weiteren wichtigen Ringdefinition, dem euklidischen Ring, in Zusammenhang gebracht.

Definition 50. Ein Integritätsbereich R heißt ***euklidisch***, falls eine Abbildung $\delta : R \to \mathbb{N}$ existiert, sodass gilt:

(i) $\delta(0) = 0$

(ii) $\delta(xy) \geq \delta(x)$ für $0 \neq x, y \in R$

(iii) Für $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$, sodass $a = qb + r$ und $\delta(r) < \delta(b)$.

Nachfolgend werden die anschaulichen Darstellungen der Zusammenhänge von Fischer [4, S. 214f] und Jacobson [10, S. 140f] berücksichtigt.

Definition 51. Ein Integritätsbereich R heißt ***faktoriell***, wenn jedes Element $0 \neq a \in R, a \notin R^*$ eine multiplikative Zerlegung in irreduzible Elemente besitzt und diese Zerlegung ist bis auf die Reihenfolge und die Multiplikation mit Einheiten eindeutig.
Das heißt es gibt zu jedem $a \in R, a \neq 0, a \notin R^*$ die irreduziblen Elemente $q_1, ..., q_r \in R$, sodass

$$a = q_1 \cdot q_2 \cdots q_r$$

und diese Darstellung ist eindeutig.

Für die Untersuchung auf Faktorisierung in der Praxis wird die folgende Proposition verwendet, die zugleich die Existenz der Primfaktorzerlegung in faktoriellen Ringen beweist:

Proposition 52 (Primfaktorzerlegung in faktoriellen Ringen)**.** *R ist faktoriell genau dann, wenn die beiden folgenden Bedingungen (F1) und (F2) erfüllt sind:*

(F1) - Teilerkettenbedingung *In R gilt der Teilerkettensatz.*

(F2) - Primzahlbedingung *Jedes irreduzible Element von R ist prim.*

Beweis.

"$\Leftarrow$" Wir zeigen, dass R faktoriell ist:

Existenz der Zerlegung

Die Existenz einer solchen Zerlegung in irreduzible Faktoren folgt aus der Teilerkettenbedingung. Sei $a \notin R^*$.
Falls a selbst irreduzibel ist, ist die Behauptung klar. Andernfalls sei $a = a_1 b_1$ und a_1 ein echter Teiler von a. Dann ist a_1 entweder selbst irreduzibel oder $a_1 = a_2 b_2$ und a_2 ein echter Teiler von a_1. Wir erhalten eine Kette von echten Teilern, bei der jedes Element ein echter Teiler des vorangegangenen ist. Nach der Teilerkettenbedingung endet dieser Prozess nach endlich vielen Schritten mit einem irreduziblen Faktor a_n von a.
Damit können wir $a_n = p_1$ setzen und schreiben $a = p_1 c_1$. Nun folgt dieselbe Argumentation für eine Teilerkette von c_1, wobei wir wieder nach endlich vielen

Schritten einen irreduziblen Faktor c_m von a erhalten. Wir setzen $c_m = p_s$ und erhalten eine Zerlegung von a in irreduzible Faktoren:

$$a = p_1 c_1 = p_1 p_2 c_2 = \cdots = p_1 p_2 \cdots p_s$$

und erhalten damit auch eine Teilerkette, da $c_1 \mid a, ...c_{i+1} \mid c_i$ und diese bricht ab.

Eindeutigkeit der Zerlegung

Die Eindeutigkeit der Zerlegung folgt aus der Primzahlbedingung mithilfe von Induktion. Angenommen zu a gibt es zwei verschiedene Zerlegungen in irreduzible Faktoren, sodass

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \tag{1}$$

Falls $s = 1$, so ist $a = p_1$ und damit $t = 1$ und $a = q_1$, also $p_1 = q_1$.
Falls $s \neq 1$, so ist nach der Primzahlbedingung das Element p_1 aus der Darstellung (1) prim. Dadurch folgt aus $p \mid q_1 q_2 \cdots q_t$ sofort, dass p ein q_j teilt. Durch Änderung der Anordnung können wir aus $p_1 \mid q_1$ schließen, dass p_1 assoziiert zu q_1 sein muss, also $q_1 = p_1 e_1$, wobei e_1 eine Einheit ist.
Wir folgern aus (1):

$$b = p_2 \cdots p_s = e_1 q_2 \cdots q_t = q_2' \cdots q_t'$$

Alle q_j' mit $i > 2$ sind irreduzibel. Nach Induktionsvoraussetzung gilt $s - 1 = t - 1$ und bis auf Unterschiede in der Anordnung der einzelnen Faktoren ist die Darstellung der p_i für $i = 2, ..., s$ gezeigt. Nach dieser Voraussetzung muss auch $s = t$ gelten und $p_i \sim q_i$ mit $1 \leq i \leq s$.

"⇒" Wir zeigen, dass die Bedingungen (F1) und (F2) gelten:

(F1) Sei $a \in R$ mit $a = p_1 p_2 \cdots p_s$, wobei die Elemente p_i irreduzibel sind. Wir bezeichnen mit Länge$(a) := s$ die Länge von a. Die Wohldefiniertheit der Länge ist durch die Eindeutigkeit der Primfaktorzerlegung gegeben.
Gibt es für $b, c \in M$ und $b, c \notin R^*$ ebenfalls eine solche Darstellung aus irreduziblen Elementen

$$b = \prod_{j=1}^{t} p_j', c = \prod_{k=1}^{u} p_k''$$

mit Länge$(b) = t$, Länge$(c) = u$ und gilt weiter $a = bc$, so ist

$$\begin{aligned} a &= p_1 p_2 \cdots p_s \\ &= p_1' p_2' \cdots p_t' p_1'' p_2'' \cdots p_u''. \end{aligned}$$

Da die Zerlegung von a nach Definition eindeutig sein soll, kann dies nur erfüllt sein, wenn jedes p_i zu genau einem der p_j', p_k'' assoziiert ist. Daher gilt $s = t + u \Rightarrow$ Länge$(a) =$ Länge$(b) +$ Länge(c). Es gilt sicher Länge$(a) > 0$, da b und c keine Einheiten sind. Insbesondere ist b ein echter Teiler von a und daher gilt Länge$(b) <$ Länge(a). Ist die Folge $(a_1, ...a_n)$ eine Teilerkette, das heißt für alle a_i gilt $a_{i+1} \mid a_i$, dann ist die Länge der Kette sicher kleiner als Länge(a_n) und endet daher nach spätestens n Schritten.

(F2) Erinnerung: $p \notin R^*$ heißt prim, wenn aus $p \mid ab$ sofort $p \mid a \vee p \mid b$ folgt, beziehungsweise wenn aus $p \nmid a \wedge p \nmid b$ sofort $p \nmid ab$ folgt.
Sei p irreduzibel und $p \mid ab$.
Dann ist p keine Einheit. Falls o.B.d.A. a eine Einheit ist, dann ist ab assoziiert zu b und $p \mid b$.
Falls a und b keine Einheiten sind, müssen beide analog zu (1) dargestellt werden können, sodass $ab = p_1 p_2 \cdots p_s p'_1 p'_2 \cdots p'_t$. Da $p \mid ab$ ist p assoziiert zu einem p_i oder einem p'_j. Damit gilt wieder $p \mid a \vee p \mid b$.

□

Bemerkung 53. Die Primzahlbedingung (F2) lässt sich durch die sogenannte **ggT-Bedingung** ersetzen [10, S. 144-146]:

(F2a) - ggT-Bedingung Je zwei Elemente von R haben einen größten gemeinsamen Teiler.

Beweis. Um das Behauptete zu beweisen, benötigen wir die Definition 28. Wir müssen zuerst beweisen, dass zwei Elemente eines faktoriellen Rings einen ggT haben, (der bis auf Assoziiertheit eindeutig ist (1)). Im Anschluss müssen wir zeigen, dass die ggT-Bedingung die Primzahlbedingung bedingt und daher ersetzen kann (2).

(1) Seien $a, b \in R$. Ist $a \in R^*$, dann ist a der ggT von a und b. Analoges gilt für $b \in R^*$. Sind $a, b \notin R^*$, dann haben beide Elemente a und b nach 51 eine Zelegung in irreduzible, nicht zueinander assoziierte Elemente $p_i \in R$, sodass

$$a = e_a p_1^{k_1} \cdots p_r^{k_r} b = e_b p_1^{l_1} \cdots p_r^{l_r}$$

mit $e_i \in R^*, k_i, l_i \in \mathbb{N}$.
Wir bilden aus $m_i = max\{k_i, l_i\}$ das Element $d := p_1^{m_1} \cdots p_r^{m_r}$. d ist sicher ein gemeinsamer Teiler von a und b.
Sei c ein weiterer gemeinsamer Teiler von a und b mit $c = e_c p_1^{s_1} \cdots p_r^{s_r}$, wobei $0 \leq s_i \leq k_i, l_i$. Dann sind die $s_i \leq m_i$ und $c \mid d$. Aus der Definition 51 und der Eindeutigkeit der Zerlegungen von a und b ergibt sich die Eindeutigkeit der k_i, l_i und damit die Eindeutigkeit von d, dem größten gemeinsamen Teiler von a und b.

(2) Sei $p \in R$ irreduzibel. Angenommen $p \nmid a$ und $p \nmid b$. Dann ist nach den Eigenschaften des ggT, Lemma 30, $(p, a) = 1 = (p, b)$, woraus sofort $(p, ab) = 1$ folgt.
Es gilt also $p \nmid ab$.
Aus $p \mid ab$ muss daher $p \mid a$ oder $p \mid b$ folgen und p ist daher ein primes Element von R.

□

Satz 54. *Jeder Hauptidealring ist faktoriell.*

Beweis. Nach Satz 39 gilt der Teilerkettensatz in jedem Hauptidealring und damit ist die Bedingung **(F1)** erfüllt. Nach Korollar 48 gilt auch die Primzahlbedingung **(F2)** in jedem Hauptidealring. □

Satz 55. *Alle euklidischen Ringe sind Hauptidealringe.*

Beweis. Sei I ein Ideal des euklidischen Rings R mit der (Norm-) Abbildung $\delta : R \to \mathbb{N}$. Für $I = (0)$ ist die Behauptung trivial.
Für $I \neq 0$ gilt: Es gibt ein Element $b \neq 0, b \in I$ mit $\delta(b)$ minimal. Weiter gibt es für jedes $a \in I$ die Elemente $d, r \in R$, sodass $a = db + r$ mit $\delta(r) < \delta(b)$.
Aus $r = a - bd \in I$ und $\delta(r) < \delta(b)$ folgt direkt $r = 0$, bzw. $a = db$, also $a \in I$, das heißt $I = (b)$. □

Daraus folgt vor allem auch:

Korollar 56. *Jeder euklidische Ring ist faktoriell.*

Für diese Arbeit sind die algebraischen und zahlentheoretischen Grundlagen ausreichend erörtert. Andere Zusammenhänge werden in weiterer Folge nicht benötigt, können aber bei darüber hinaus bestehendem Interesse unter anderem in Frey [9], Karpfinger und Meyberg [11] oder bei Scheid und Frommer [14] nachgelesen werden.

2.3.1 Beispiel: Der euklidische Ring $\mathbb{Z}$

Um das Vorangegangene etwas besser verdeutlichen zu können, wird die Arithmetik des Rings der ganzen Zahlen, die das zentrale Untersuchungsobjekt der Zahlentheorie bilden, näher betrachtet. Zuerst halten wir fest: $\mathbb{Z}$ ist ein euklidischer Ring mit der Betragsfunktion: $|\quad| : \mathbb{Z} \to \mathbb{N}$ und daher auch ein Hauptidealring und faktoriell. [3]
Die zuvor erwähnten Begriffe können in $\mathbb{Z}$ sehr kompakt zusammengefasst werden:
Die Einheiten in $\mathbb{Z}$ sind ± 1.
Für alle Elemente $a \in \mathbb{Z}$ gilt daher $a \sim -a$.
Die Primelemente in $\mathbb{N}$ haben eine besondere Bedeutung. Sie werden als Primzahlen bezeichnet und bilden die Menge der Primzahlen $\mathbb{P}$. Eine Primzahl, die eine ganze Zahl n teilt, heißt ***Primteiler*** von n.

Behauptung 57. *Jede ganze Zahl $n \in \mathbb{Z}, |n| \geq 2$ hat einen Primteiler.*

Beweis. Sei $T_n := \{d \in \mathbb{N}, d \geq 2 : d \mid n\}$ die Menge aller Teiler ≥ 2 von n. Da $|n| \geq 2$ ist $n \notin \mathbb{Z}^* = \{-1, 1\}$ und hat einen echten Teiler, also $T_n \neq \emptyset$. Die Menge T_n enthält sicher ein kleinstes Element q.
Wenn $q \in \mathbb{P}$, dann ist q ein Primteiler von n. Wäre $q \notin \mathbb{P}$, dann hätte q einen echten Teiler m mit

$$m \mid q \mid n \quad \text{also} \quad m \mid n.$$

Dann wäre $m \in T_n$ und durch $m < q$ entsteht ein Widerspruch.
Das kleinste Element der Teilermenge von n muss also eine Primzahl sein. □

[3] Für einen kurzen Beweis ist nach Definition 50 lediglich zu zeigen (i) $|0| = 0$ und (ii) $|xy| \geq |x|$. (iii) wird auf Seite 25 gezeigt.

Mithilfe der Primzahlen lassen sich alle Elemente der ganzen Zahlen in Faktoren zerlegen:

Satz 58. *Sei $a \in \mathbb{Z}, a \geq 2$. Dann lässt sich a als Produkt von Primzahlen darstellen, also*

$$a = p_1 \cdot p_2 \cdots p_k \quad \textit{für} \quad p_i \in \mathbb{P}, 1 \leq i \leq k.$$

*Eine solche Darstellung heißt **Primfaktorzerlegung** (PFZ) von a. Die Primfaktorzerlegung ist bis auf die Anordnung der Primfaktoren und die Multiplikation der Faktoren mit -1 eindeutig.*

Beweis. Der Ring der ganzen Zahlen $\mathbb{Z}$ ist euklidisch und daher ein Hauptidealring, in dem die Begriffe prim und irreduzibel gleichbedeutend sind. Die Existenz und Eindeutigkeit der Primfaktorzerlegung in dem faktoriellen Ring $\mathbb{Z}$ ergibt sich aus der Definition 51 von faktoriellen Ringen und Proposition 52. □

Beispiel 59. Einige Beispiele für Primfaktorzerlegungen in $\mathbb{Z}$ sind:

$$\begin{aligned} 27 &= 3^3 = -3^2 \cdot 3 \\ 41 &= 41 \\ -60 &= 2^2 \cdot 3 \cdot -5 = -2 \cdot 2 \cdot 3 \cdot 5 = \ldots \\ 1234 &= 2 \cdot 617 \end{aligned}$$

Für sehr große Zahlen lässt sich auf den ersten Blick nicht sagen, ob eine Primzahl vorliegt. Daher werden in solchen Fällen sogenannte Primzahltests angewendet. Leider gibt es bis heute noch keinen praktikablen Primzahltest mit einer 100%-igen Sicherheit. Der Fermat'sche Primzahltest wird in dieser Arbeit für die Untersuchung der primen Elemente im Ring der Eisensteinzahlen noch eine Rolle spielen (siehe Seite 60).

Aus dem bisher gezeigten kann in den ganzen Zahlen die ***Division mit Rest*** definiert werden (vgl. 50(iii)).

Definition 60 (Division mit Rest)**.** Seien $a, b \in \mathbb{Z}$. Dann gibt es in $\mathbb{Z}$ eindeutig bestimmte $q, r \in \mathbb{Z}$, sodass gilt:

$$a = q \cdot b + r, \quad \text{sodass} \quad 0 \leq r < |b|.$$

Für den Fall $b \mid a$ ist $r = 0$. r heißt Rest. Das heißt Z ist ein euklidischer Ring.

Beispiel 61. Einige Beispiele für eine Division mit Rest in $\mathbb{Z}$ sind:

$$\begin{aligned} 52 &= 6 \cdot 8 + 4 \\ -76 &= -19 \cdot 4 + 0 \\ 49 &= -5 \cdot -9 + 4 \end{aligned}$$

Wir können anhand der Division mit Rest sofort die zugehörige Restklasse erkennen. Mithilfe der Division mit Rest kann außerdem der folgende Algorithmus definiert werden:

Algorithmus 62 (Euklidischer Algorithmus)**.** Seien $a, b \in \mathbb{Z}$. Wir führen wiederholt eine Division mit Rest durch, sodass wir eine Folge von Zahlen $g_i, 1 \leq i \leq m+1$ erhalten. Die rekursive Darstellung der Folge lautet

$$\begin{aligned} g_0 &= a \\ g_1 &= b \\ g_{n-1} &= q_n \cdot g_n + g_{n+1} \end{aligned}$$

Der Algorithmus bricht nach endlich vielen Schritten ab mit $g_{m+1} = 0$.

Beweis. Es gilt für alle g_i, dass $g_{n+1} < g_n$. Da bei der Division mit Rest nur positive Werte für den Rest r möglich sind, gibt es auch nur endlich viele mögliche Schritte bis wir bei $g_{n+1} = 0$ ankommen. □

Behauptung 63. *Der letzte Wert $\neq 0$ im Euklidischen Algorithmus g_m ist der größte gemeinsame Teiler der beiden ganzen Zahlen a und b.*

Beweis. Sei wie behauptet $g_{m+1} = 0$. Dann ist aufgrund des Algorithmus g_m ein gemeinsamer Teiler von g_m und g_{m-1}. g_m ist größtmöglicher gemeinsamer Teiler, da für alle weiteren gemeinsamen Teiler d gilt: dg_m.
Wir müssen nun noch zeigen: g_m ist gemeinsamer Teiler für alle g_n, insbesondere für a und b.
Aus $g_m \mid g_{m-1}$ mit $g_{m-1} = q_m g_m$ folgt sofort:

$$g_{m-2} = q_m g_m q_{m-1} + g_m = g_m(q_m g_{m-1} + 1), \quad \text{also} \quad g_m \mid g_{m-2}.$$

Diese Argumentation können wir bis $g_0 = a$ und $g_1 = b$ fortsetzen und damit ist gezeigt: $ggT(a, b) = g_m$. [15, S. 253] □

Um den euklidischen Algorithmus etwas anschaulicher zu machen, rechnen wir einige kurze Beispiele:

Beispiel 64.
Finde den größten gemeinsamen Teiler von 675 und 51.

$$\begin{aligned} 675 &= 13 \cdot 51 + 12 \\ 51 &= 4 \cdot 12 + 3 \\ 12 &= 4 \cdot 3 + 0 \\ ggT(675, 51) &= 3 \end{aligned}$$

Finde den größten gemeinsamen Teiler von 363 und -278.

$$
\begin{aligned}
363 &= -1 \cdot -278 + 85 \\
-278 &= -4 \cdot 85 + 62 \\
85 &= 1 \cdot 62 + 23 \\
62 &= 2 \cdot 23 + 16 \\
23 &= 1 \cdot 16 + 7 \\
16 &= 2 \cdot 7 + 2 \\
7 &= 3 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0 \\
ggT(363, -278) &= 1
\end{aligned}
$$

Der euklidische Algorithmus 62 und die damit einhergehende Behauptung 63 über den ggT gelten in allen euklidischen Ringen. Die Beweise für den euklidischen Algorithmus können äquivalent geführt werden mit $|g_{n+1}| < |g_n|$ [15, S. 258f].

2.4 Zusammenfassung

Für eine bessere Übersicht in den nachfolgenden Kapiteln fassen wir die wichtigsten, in den verschiedenen Ringen geltenden Kriterien zusammen:

In faktoriellen Ringen gilt:

- Es gibt eine eindeutige Zerlegung in irreduzible Faktoren für alle Elemente des Rings, die keine Einheit sind. (siehe 52)
- Je zwei Elemente haben einen größten gemeinsamen Teiler. (53)

In Hauptidealringen gilt zusätzlich:

- Lemma von Bézout: Für $a, b \in R$ gibt es $x, y \in R$, sodass $ggT(a, b) = xa + yb$. (47)
- Ein Element ist prim. $\Leftrightarrow$ Ein Element ist irreduzibel. (26, 48)
- Jedes Element des Rings hat eine eindeutige Zerlegung in irreduzible Elemente. (58)

In euklidischen Ringen gilt zusätzlich:

- Es gibt eine Division mit Rest. (50, 60)
- Es gibt einen euklidischen Algorithmus. Dessen letzter Wert $\neq 0$ liefert den größten gemeinsamen Teiler zweier Elemente. (62, 63)

3 Quadratische Zahlkörper und Ganzheitsringe

Der einfachste Zahlkörper ist die Menge der rationalen Zahlen $\mathbb{Q}$. Für die Untersuchung von Gleichungen über $\mathbb{Q}$ werden algebraische Zahlkörper herangezogen. Das sind endliche Erweiterungen über dem Körper $\mathbb{Q}$, in dem sich insbesondere die Ringe von ganzen Elementen untersuchen lassen - die Ganzheitsringe. Diese Ganzheitsringe haben eine Ringstruktur, die jenen der ganzen Zahlen ähnelt und dadurch eine Analyse ihrer Arithmetik erlaubt. Für die Untersuchung von quadratischen Gleichungen, insbesondere für die Untersuchung von binären quadratischen Formen eignen sich die quadratischen Zahlkörper, die der Ausgangspunkt für alle folgenden Überlegungen sind.

3.1 Quadratische Zahlkörper

Zu Beginn werden einige Begriffe festgehalten:

Bemerkung 65. Sei $d \in \mathbb{N}, d \geq 2$. Die Zahl d heißt ***quadratfrei***, wenn es kein $a \in \mathbb{N}, a \geq 2$ gibt, sodass gilt $a^2 \mid d$.
Es gilt: $\sqrt{d}$ ist irrational.

Beweis. Angenommen d sei rational, sodass $d = \frac{m}{n}$ mit teilerfremden $m, n \in \mathbb{N} \setminus \{0\}$.
Dann gilt auch

$$m^2 = d^2 \cdot n^2.$$

Die Primfaktorzerlegungen von m^2 und n^2 enthalten nur gerade Potenzen. In der Primfaktorzerlegung von d sind nach Definition von d nur einfache Potenzen enthalten, somit kann die Gleichung nicht erfüllt sein - Widerspruch. □

Im folgenden Abschnitt heißt ein quadratfreies $d \in \mathbb{Z}$ ***zulässig***, wenn $d \leq -1$ oder wenn $d \geq 2$.

Definition 66. Es sei definiert $\mathbb{Q}(\sqrt{d}) := \mathbb{Q} + \mathbb{Q}\sqrt{d} = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$.
Dann heißt der Körper $\mathbb{Q}(\sqrt{d})$ ***quadratischer Zahlkörper***, falls $d \in \mathbb{Z}$ zulässig ist.
$\mathbb{Q}(\sqrt{d})$ heißt für $d > 0$ ***reell-quadratisch*** und für $d < 0$ ***imaginär-quadratisch***.

Insbesondere gilt für $d < 0$, dass $\sqrt{d} = \mathrm{i}\sqrt{|d|}$ und jedes $\alpha \in \mathbb{Q}(\sqrt{d})$ hat die Darstellung $\alpha = a + \mathrm{i}b\sqrt{|d|}$ mit dem Realteil a und dem Imaginärteil $b\sqrt{|d|}$.

Bemerkung 67. Ein quadratischer Zahlkörper ist ein Erweiterungskörper von $\mathbb{Q}$ und ein Unterkörper von $\mathbb{C}$.

Beweis. [4, S. 229][9, S. 97]
Zu zeigen ist die Aussage: $\mathbb{Q}(\sqrt{d})$ ist ein Körper. Der Rest der Bemerkung folgt sofort.
Seien $(a + b\sqrt{d}), (r + s\sqrt{d})$ beliebige Elemente von $\mathbb{Q}(\sqrt{d})$ mit $(a, b), (r, s) \neq (0, 0)$.
Dann ist $\mathbb{Q}(\sqrt{d})$ abgeschlossen bezüglich der Multiplikation und Division, weil:

$$(a + b\sqrt{d})(r + s\sqrt{d}) = (ar + bsd) + (as + br)\sqrt{d} \qquad \in \mathbb{Q} + \mathbb{Q}\sqrt{d}$$

und:

$$\frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{(a+b\sqrt{d})(a-b\sqrt{d})} = \frac{a}{a^2-b^2d} - \frac{b}{a^2-b^2d}\sqrt{d} \qquad \in \mathbb{Q}+\mathbb{Q}\sqrt{d}$$

□

Für quadratische Zahlkörper und die darin enthaltenen Elemente der Form $\alpha = a+b\sqrt{d}$ existiert die ***Konjugationsabbildung***:

$$\begin{aligned}\sigma : \mathbb{Q}(\sqrt{d}) &\to \mathbb{Q}(\sqrt{d}),\\ a+b\sqrt{d} &\mapsto a-b\sqrt{d}\end{aligned}$$

Für das konjugierte Element zu α schreiben wir $\overline{\alpha}$, sodass $\overline{\alpha} = a - b\sqrt{d}$. In imaginärquadratischen Zahlkörpern, insbesondere den Gauß'schen Zahlen, wird das konjugierte Element auch als "komplexes konjugiertes Element" bezeichnet.

Bemerkung 68. Die Konjugationsabbildung ist ein Körperautomorphismus.

Beweis. Seien $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ mit $\alpha = a+b\sqrt{d}$ und $\beta = r+s\sqrt{d}$ und $a, b, r, s \neq 0$.

- $\sigma(0) = \sigma(0+0\sqrt{d}) = (0-0\sqrt{d}) = 0 \in \mathbb{Q}(\sqrt{d})$
- $\sigma(\alpha+\beta) = \sigma(a+b\sqrt{d}+r+s\sqrt{d}) = \sigma(a+r+(b+s)\sqrt{d}) = a+r-(b+s)\sqrt{d} = a-b\sqrt{d}+r-s\sqrt{d} = \sigma(\alpha)+\sigma(\beta)$
- $\sigma(\alpha\cdot\beta) = \sigma((a+b\sqrt{d})\cdot(r+s\sqrt{d})) = \sigma((ar+bsd)+(as+br)\sqrt{d}) = (ar+bsd)-(as+br)\sqrt{d} = (a-b\sqrt{d})\cdot(r-s\sqrt{d}) = \sigma(\alpha)\cdot\sigma(\beta)$

□

Definition 69. Sei $\mathbb{Q}(\sqrt{d})$ quadratischer Zahlkörper. Für $\alpha = a+b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ seien definiert:

Norm: $N(\alpha) := \alpha\cdot\overline{\alpha} = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2-db^2 \in \mathbb{Q}$

Spur: $S(\alpha) := \alpha+\overline{\alpha} = (a+b\sqrt{d})+(a-b\sqrt{d}) = 2a \in \mathbb{Q}$

Für Norm und Spur gelten insbesondere die folgenden Rechenregeln:

Proposition 70 (Rechenregeln für Norm und Spur)**.** *Für alle $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ gilt:*

(A1) $S(\alpha+\beta) = S(\alpha)+S(\beta)$

(A2) $N(\alpha\cdot\beta) = N(\alpha)\cdot N(\beta)$

(A3) $N(\alpha) = 0 \Leftrightarrow \alpha = 0$

Beweis. Sei $\alpha = a + b\sqrt{d}$ und $\beta = r + s\sqrt{d}$.

$$\begin{aligned}(A1) : S(\alpha+\beta) &= (\alpha+\beta) + \overline{(\alpha+\beta)} \\ &= (a + r + (b+s)\sqrt{d}) + (a + r - (b+s)\sqrt{d}) \\ &= 2(a+r) \\ &= 2a + 2r = S(\alpha) + S(\beta)\end{aligned}$$

$$\begin{aligned}(A2) : N(\alpha\cdot\beta) &= (\alpha\cdot\beta)\cdot\overline{(\alpha\cdot\beta)} \\ &= \Big((a+b\sqrt{d})\cdot(r+s\sqrt{d})\Big)\cdot\overline{\Big((a+b\sqrt{d})\cdot(r+s\sqrt{d})\Big)} \\ &= (ar+bsd+(as+br)\sqrt{d})\cdot(ar+bsd-(as+br)\sqrt{d}) \\ &= (ar+bsd)^2 - (as+br)^2 d \\ &= a^2r^2 + 2abrsd + b^2s^2d^2 - (a^2s^2d + 2abrsd + b^2r^2d) \\ &= a^2r^2 + b^2s^2d^2 - a^2s^2d - b^2r^2d \\ &= (a^2 - db^2)\cdot(r^2 - ds^2) = N(\alpha)\cdot N(\beta)\end{aligned}$$

(A3): " $\Leftarrow$": Aus $\alpha = 0$ folgt sofort $N(\alpha) = 0^2 - d\cdot 0^2 = 0$
" $\Rightarrow$": Fall 1: Sei $d \leq -1$, dann ist $N(\alpha) = a^2 + |d|b^2 \geq 0$, also muss aus $N(\alpha) = 0$ sofort $a = b = 0$ folgen.
Fall 2: Sei $d \geq 2$ und $N(\alpha) = a^2 - db^2 = 0$. Aus $b = 0$ folgt sofort $a = 0$, da $d = \frac{a^2}{b^2} \in \mathbb{Q}$ mit quadratfreiem d nicht möglich ist. [4, S. 229][14, S. 101] □

3.2 Ganzheitsringe in quadratischen Zahlkörpern

Bekanntlich ist die Menge der ganzen Zahlen $\mathbb{Z}$ eine Teilmenge der rationalen Zahlen $\mathbb{Q}$. Genauer gesagt ist $\mathbb{Z} \subset \mathbb{Q}$ ein Unterring des Körpers der rationalen Zahlen.
Sowohl $\mathbb{Z}$ als auch $\mathbb{Q}$ sind wiederum Teilmengen der komplexen Zahlen $\mathbb{C}$. Wir definieren den Unterring der komplexen Zahlen: $\mathbb{Z}[\sqrt{d}] := \mathbb{Z} + \mathbb{Z}\sqrt{d} = \{m + n\sqrt{d} : m, n \in \mathbb{Z}\} \subset \mathbb{Q} + \mathbb{Q}\sqrt{d} =: \mathbb{Q}(\sqrt{d})$[4]

Definition 71. Ein $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ heißt ***ganz***, wenn Norm und Spur ganzrational sind, also wenn $N(\alpha) \in \mathbb{Z} \wedge S(\alpha) \in \mathbb{Z}$.
Insbesondere kann nun definiert werden:
$\mathcal{O}_d := \{\alpha \in \mathbb{Q}(\sqrt{d}) : \alpha \text{ ganz }\}$
$\mathcal{O}_d$ heißt ***quadratischer Zahlring oder Ganzheitsring*** in $\mathbb{Q}(\sqrt{d})$.

Bemerkung 72. Im quadratischen Zahlring $\mathcal{O}_d$ kommen zu $\mathbb{Z}[\sqrt{d}]$ also noch genau die Elemente hinzu, die Nullstellen des Polynoms $f_\alpha := (X-\alpha)(X-\overline{\alpha}) = X^2 - (\alpha+\overline{\alpha})X + \alpha\overline{\alpha}$ sind, wobei α einer solchen Nullstelle entspricht und daher die Gleichung $x^2 - S(\alpha)x + N(\alpha) = x^2 - 2ax + a^2 - db^2 = 0$ erfüllt. Die Bedingung dabei ist, dass die Koeffizienten $S(\alpha)$ und $N(\alpha)$ in $\mathbb{Z}$ liegen müssen.

[4] Die übliche Notation für Zahlkörper erfolgt mit den runden Klammern ( ). Zahlringe werden mit eckigen Klammern [ ] notiert.

$\alpha \in \mathcal{O}_d$ heißt ganz in $\mathbb{Q}(\sqrt{d})$ und $\alpha \in \mathbb{Z}$ heißt ganzrational.

Ausgehend von den ganzen Zahlen kann für $\mathcal{O}_d$ nun festgestellt werden, wie die Ringe in Abhängigkeit von d aufgebaut sind:

Satz 73. *Für zulässige $d \in \mathbb{Z}$ gilt:*

a) $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$ *für* $d \equiv 2$ *oder* $d \equiv 3 \mod 4$
$\mathcal{O}_d = \{\frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z}, a - b \text{ gerade }\}$ *für* $d \equiv 1 \mod 4$

b) Für den Fall $d \equiv 1 \mod 4$ *ist* $\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}\rho$, *wobei* $\rho := \frac{1}{2}(1 + \sqrt{d})$.

c) $\mathcal{O}_d$ *ist ein Unterring von* $\mathbb{Q}(\sqrt{d})$. *Insbesondere ist* $\mathcal{O}_d$ *ein Integritätsbereich.*

d) $\mathcal{O}_d \cap \mathbb{Q} = \mathbb{Z}$

Beweis. Sei $\alpha = a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$.

a) Für jedes ganze $\alpha \in \mathcal{O}_d$ gilt, dass Norm und Spur ganzrational sind. Es ist also $S(\alpha) = 2a \in \mathbb{Z}$ und $N(\alpha) = a^2 - db^2 \in \mathbb{Z}$. Für ein $u := 2a \in \mathbb{Z}$ erhalten wir durch Einsetzen in die Norm

$$N(\alpha) = a^2 - db^2 = \frac{u^2 - 4db^2}{4} = \frac{u}{2}^2 - 4db^2.$$

Da $u \in \mathbb{Z}$ ist, muss auch $4db^2 = d(2b)^2$ ganz sein. In weiterer Folge muss dann auch $2b$ ganz sein, da das quadratfreie d den eventuellen Nenner von $(2b)^2$ nicht kürzen könnte. Wir können nun aus u und $v := 2b$ eine durch 4 teilbare ganze Zahl konstruieren mit der Form $u^2 - v^2 d$.

– Fall 1: $d \equiv 2$ oder $d \equiv 3 \mod 4$
Sei u ungerade, das heißt $u = 2k + 1$ für ein $k \in \mathbb{Z}$. Wir setzen für $d \equiv 2 \mod 4$, also $d = 4n + 2$ mit $n \in \mathbb{Z}$ ein und erhalten

$$u^2 - v^2 d = (2k+1)^2 - v^2(4n+2) = 4k^2 + 4k + 1 - v^2 \cdot 4n - 2v^2 = 4(k^2 + k - v^2) + 1 - 2v^2.$$

Dieser Term ist genau dann durch vier teilbar, wenn $4 \mid 1 - 2v^2$.
Wäre v gerade, so wäre $1 - 2v^2 \equiv 1 \mod 4$ und damit ein Widerspruch.
Wäre v ungerade, so wäre $1 - 2v^2 \equiv 3 \mod 4$ und erneut ein Widerspruch zur Teilbarkeitsvoraussetzung.
Für $d \equiv 3 \mod 4$ wird analog berechnet und eine Bedingung für v gesucht, sodass $4 \mid 1 - 3v^2$. Mit v ungerade ergibt sich die Kongruenz $1 - 3v^2 \equiv 2 \mod 4$, mit v gerade ergibt sich die Kongruenz $1 - 3v^2 \equiv 1 \mod 4$, also in beiden Fällen ein Widerspruch zur Teilbarkeitsvoraussetzung $4 \mid 1 - 3v^2$.

Seien u und v gerade. Dann ist $u^2 - v^2 d \equiv 0 \mod 4$ für $d \equiv 2$ oder $3 \mod 4$ und damit die Voraussetzung erfüllt und $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$.

– Fall 2: $d \equiv 1 \mod 4$
Seien u und v gerade. Dann folgt wegen $u = 2a$ und $v = 2b$ sofort $a, b \in \mathbb{Z}$. Sei u ungerade und wie vorausgesetzt $d = 4n+1$ für ein $n \in \mathbb{Z}$. Dann ergeben sich durch analoge Rechnung wie in Fall 1 die Kongruenzen $1 - v^2 \equiv 1 \mod 4$, wenn v gerade, und $1 - v^2 \equiv 0 \mod 4$, wenn v ungerade.
Insgesamt ergibt sich in diesem Fall also $u - v$ ist gerade und daher haben alle $\alpha \in \mathcal{O}_d$ die Form

$$\frac{a}{2} + \frac{b}{2}\sqrt{d}$$

mit $a, b \in \mathbb{Z}$ und $a - b$ gerade.

b) folgt sofort aus a) durch:

$$\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{d} = \frac{a-b}{2} + b \cdot \frac{1+\sqrt{d}}{2} = r + s \cdot \rho \quad \text{mit } r, s \in \mathbb{Z} \text{ und } \rho = \frac{1}{2}(1+\sqrt{d}).$$

c) $\mathcal{O}_d$ ist genau dann ein Integritätsbereich $\subset \mathbb{Q}(\sqrt{d})$, wenn aus $\alpha, \beta \in \mathcal{O}_d$ folgt, dass auch $\alpha - \beta$ und $\alpha \cdot \beta$ in $\mathcal{O}_d$ liegen.
Aus a) folgt sofort die Abgeschlossenheit der Addition. Für die Multiplikation ergibt sich die Abgeschlossenheit im Fall $d \equiv 2$ oder $d \equiv 3 \mod 4$ auch sofort aus a). Im Fall $d \equiv 1 \mod 4$ muss wegen b) nur $\rho^2 \in \mathcal{O}_d$ liegen:

$$\begin{aligned}
\rho^2 &= \left(\frac{1}{2}(1+\sqrt{d})\right)^2 \\
&= \frac{1}{4}(1 + 2\sqrt{d} + d) \\
&= \frac{1}{4} + \frac{1}{2}\sqrt{d} + \frac{1}{4}d \\
&= \frac{1}{2}\left(\frac{1}{2} + \frac{1}{2}d + \sqrt{d}\right) \\
&= \frac{1}{2}\left(\frac{d+1}{2} + \sqrt{d}\right) \\
&= \frac{1}{2}\left(\frac{4n+1+1}{2} + \sqrt{d}\right) \quad \in \mathcal{O}_d \quad \text{mit } n \in \mathbb{Z}
\end{aligned}$$

d) Für $d \equiv 2$ oder $d \equiv 3 \mod 4$ ist

$$\alpha = a + b\sqrt{d} \in \mathbb{Q} \Leftrightarrow b = 0 \Leftrightarrow \alpha = a \in \mathbb{Z}$$

Für $d \equiv 1 \mod 4$ ist

$$\alpha = \frac{a + b\sqrt{d}}{2} \in \mathbb{Q} \Leftrightarrow b = 0 \Leftrightarrow \alpha = \frac{a}{2} \in \mathbb{Z}, \text{ da } 2 \mid a \text{ wegen } a - b \text{ gerade.}$$

[3, S. 71f] [4, S. 231f] [9, S. 97f] [14, S. 100] □

3.2.1 Einheiten in quadratischen Zahlringen

Um im weiteren Verlauf dieser Arbeit die Teilbarkeit von Ganzheitsringen untersuchen zu können, müssen an dieser Stelle einige Begriffe, die aus allgemeinen Integritätsbereichen bzw. euklidischen Ringen bereits bekannt sind (siehe Kapitel 2.2.2 und Kapitel 2.3) hier im Speziellen analysiert werden. Ein erster Schritt ist dabei die Untersuchung von Einheiten in quadratischen Zahlringen.
Die Menge der Einheiten in $\mathbb{Q}(\sqrt{d})$ ist gegeben durch
$\mathcal{O}_d^* := \{\alpha \in \mathcal{O}_d : \text{Es gibt ein } \beta \in \mathcal{O}_d, \text{ dass die Gleichung } \alpha \cdot \beta = 1 \text{ erfüllt.}\}$

Bemerkung 74. $\mathcal{O}_d^*$ ist eine kommutative Gruppe bezüglich der Multiplikation und es gilt für jedes $\alpha \in \mathcal{O}_d^* \Leftrightarrow N(\alpha) \in \mathbb{Z}^* = \pm 1$.

Beweis. Jede Einheitengruppe ist eine kommutative Gruppe nach Bemerkung 23. Der Beweis des zweiten Teils der Aussage folgt aus den Rechenregeln für Norm und Spur in Satz 70.

"$\Rightarrow$" Seien $\alpha, \beta \in \mathcal{O}_d^*$ und $\alpha\beta = 1$. Daraus folgt $N(\alpha\beta) = 1 = N(\alpha)N(\beta)$, also muss $N(\alpha) = \pm 1$ gelten.

"$\Leftarrow$" Aus $N(\alpha) = \pm 1$ folgt $\alpha\overline{\alpha} = \pm 1$, also gilt für $\beta = \pm\overline{\alpha}$ sofort $\alpha\beta = 1$ und damit $\alpha \in \mathcal{O}_d^*$. [4, S. 233][9, S. 98]

□

Für die Bestimmung der Einheiten, also der Bestimmung der Elemente in $\mathcal{O}_d^*$ müssen demnach alle $\alpha = a + b\sqrt{d} \in \mathcal{O}_d$ gefunden werden, für die $N(\alpha) = \pm 1$ gilt. Wie wir bereits wissen, ist die Norm definiert als $N(\alpha) := \alpha\overline{\alpha} = a^2 - db^2$. Es müssen also alle Lösungen zu den sogenannten ***Pellschen Gleichungen*** gefunden werden:

$$a^2 - db^2 = \pm 1 \tag{2}$$

Wir untersuchen die Lösung dieser Gleichungen für den für uns relevanten Fall $d < 0$ und wollen zeigen

Proposition 75. *Die Einheitengruppen der Ganzheitsringe $\mathcal{O}_d^*$ sind für imaginär-quadratische Ringe gegeben durch*

$$\mathcal{O}_d^* = \begin{cases} \{\pm 1\} & \text{für } d = -2 \text{ oder } d \leq -5 \\ \{\pm 1, \pm \mathrm{i}\} & \text{für } d = -1 \\ \{\pm 1, \pm\frac{1+\sqrt{-3}}{2}, \pm\frac{1-\sqrt{-3}}{2}\} & \text{für } d = -3 \end{cases}$$

Beweis. Aus $d < 0$ folgt, dass wir die Gleichung (2) wie folgt schreiben können:

$$a^2 + |d|b^2 = \pm 1$$

Die Lösung dieser Gleichung kann nur positiv sein, daher schreiben wir noch einfacher:

$$a^2 + |d|b^2 = 1 \tag{3}$$

Sei $d \equiv 2$ oder $d \equiv 3 \mod 4$. Dann gilt nach Satz 73 $\mathcal{O}_d = \mathbb{Z}(\sqrt{d})$ und alle Elemente des Ganzheitsrings haben die Form $\alpha = a + b\sqrt{d}$ mit $a, b \in \mathbb{Z}$.
Für $d = -1$ sind die einzigen Lösungen von (3) gegeben durch: $a = \pm 1, b = 0$ und $a = 0, b = \pm 1$. Damit ist gezeigt, dass für $d = -1$ die Einheitengruppe genau die vierten Einheitswurzeln enthält, also

$$\mathcal{O}_{-1}^* = \{1, -1, \mathrm{i}, -\mathrm{i}\}.$$

Für $d = -2$ und alle weiteren $d < 0$ mit $d \equiv 2, 3 \mod 4$ ist ebenfalls sofort klar, dass nur die Lösungen $a = \pm 1, b = 0$ zu (3) infrage kommen.
Sei $d \equiv 1 \mod 4$. Dann gilt nach Satz 73 $\mathcal{O}_d = \{\frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z}, a - b \text{ gerade }\}$. Es gilt aber in jedem Fall $2a, 2b \in \mathbb{Z}$ und genau dies können wir mit $u = 2a, v = 2b$ substituieren. Damit folgt für $d = -3$ aus (3) die Gleichung

$$u^2 + 3v^2 = 4.$$

Nach kurzer Rechnung erhalten wir die Lösungen $u = \pm 2, v = 0$ und $u = \pm 1, v = \pm 1$, wodurch nach Rücksubstitution die sechsten Einheitswurzeln als Einheiten des Ganzheitsringes angegeben werden können, also

$$\mathcal{O}_{-3}^* = \{1, -1, \frac{1+\sqrt{-3}}{2}, -\frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, -\frac{1-\sqrt{-3}}{2}\}.$$

In allen anderen Fällen ist $|d| > 4$ für $d \equiv 1 \mod 4$. Damit kann die Gleichung (3) nur noch die Lösungen $a = \pm 1, b = 0$ haben und die Einheiten jedes Ganzheitsrings mit $d \leq 5$ sind $\{1, -1\}$ [4, S. 233f][9, S. 99]. □

Aus geometrischer Sicht liegen die Einheiten der Ganzheitsringe mit $d < 0$ in der Ebene genau auf dem Kreis (der Ellipse) mit Radius 1. Dort gilt $N(\alpha) = 1$.
Die Lösungen der Pellschen Gleichungen (2) für reell-quadratische Ganzheitsringe mit $d > 0$ sind wesentlich umfangreicher und schwieriger zu berechnen. Die zu lösenden Gleichungen können etwas genauer beschrieben werden durch:

$$a^2 - db^2 = \pm\mu, \quad a, b \in \mathbb{Z} \tag{4}$$

$$\text{mit } \mu = 1 \text{ für } d \equiv 2 \text{ oder } d \equiv 3 \mod 4$$
$$\text{und } \mu = 4 \text{ für } d \equiv 1 \mod 4$$

Eine umfangreichere Herleitung der Lösungen dieser Gleichung kann aus [9, S.101f] [17, S.116f] entnommen werden.

3.3 Imaginär-quadratische, euklidische Ganzheitsringe

3.3.1 Bestimmung der imaginär-quadratischen, euklidischen Ganzheitsringe

Um die Arithmetik in imaginär-quadratischen Ganzheitsringen vollständig untersuchen zu können, müssen wir uns mit der Frage beschäftigen: Welche Ganzheitsringe sind

euklidisch? Aus Abschnitt 2.3 wissen wir, dass sich daraus für diese Ringe einige Aussagen über Primelemente ableiten und ein euklidischer Algorithmus definieren lassen.
Dafür wird der zusammengesetzte Begriff ***normeuklidisch*** eingeführt:

Bemerkung 76. Normeuklidische Ganzheitsringe sind euklidische Ringe nach Definition 50 mit der Abbildung $\delta : R \to \mathbb{N}$, wobei ebendiese Abbildung jedenfalls mithilfe der in Abschnitt 3.1 definierten Norm $N(\alpha) = a^2 - db^2$ für $\alpha \in R$ gebildet wird.

In imaginär-quadratischen Zahlkörpern gilt für die Ganzheitsringe $\mathcal{O}_d$:

Satz 77. *Sei $d < 0$. Der Ganzheitsring $\mathcal{O}_d \in \mathbb{Q}(\sqrt{d})$ ist normeuklidisch genau dann, wenn*

$$d = -1, -2, -3, -7, -11.$$

Beweis. Zur Erinnerung: Wir suchen nach Definition 50 eine Abbildung $\delta : \mathcal{O}_d \to \mathbb{N}$, sodass gilt:

(i) $\delta(0) = 0$

(ii) $\delta(xy) \geq \delta(x)$ für $0 \neq x, y \in \mathcal{O}_d$

(iii) Für $\alpha, \beta \in \mathcal{O}_d$ mit $\beta \neq 0$ gibt es $q, r \in \mathcal{O}_d$, sodass $\alpha = q\beta + r$ und $\delta(r) < \delta(\beta)$.

Das Bild der Normabbildung $N(\alpha)$ liegt für ganze $\alpha \in \mathcal{O}_d$ in $\mathbb{Z}$. Mithilfe der bekannten (euklidischen) Betragsabbildung aus $\mathbb{Z}$ wird die normeuklidische Abbildung in $\mathcal{O}_d$ gebildet:

$$\delta = |N(\alpha)| : \mathcal{O}_d \to \mathbb{N}$$
$$a + b\sqrt{d} \Rightarrow |a^2 - db^2|$$

Aus der Definition der Norm und der Zusammensetzung von $\mathcal{O}_d$ für $d < 0$ folgen (i) und (ii) sofort. Es muss also nur noch (iii) gezeigt werden:
Seien $\alpha, \beta \in \mathcal{O}_d$ mit $\beta \neq 0$. Angenommen die Aussage stimmt für $d < 0$. Dann gibt es $q, r \in \mathcal{O}_d$ für die gilt:

$$r = \alpha - q\beta \quad \text{und weiter}$$
$$|N\Big(\frac{r}{\beta}\Big)| = |N\Big(\frac{\alpha}{\beta} - q\Big)| < 1$$

Aus geometrischer Sicht existiert also zu dem Quotienten $\frac{\alpha}{\beta}$ ein $q \in \mathcal{O}_d$, das einen Abstand kleiner als 1 hat, also innerhalb eines Kreises (einer Ellipse) mit Radius 1 liegt. Dabei muss der Aufbau des Gitters von $\mathcal{O}_d$ in Abhängigkeit von d unterschieden werden. Mithilfe dessen können wir nun alle $d < 0$ suchen, die euklidisch sind. Dafür betrachten wir den Quotienten $\frac{\alpha}{\beta}$ als Punkt in $\mathbb{Q}(\sqrt{d})$, also $\frac{\alpha}{\beta} = x + y\sqrt{d}$ mit $x, y \in \mathbb{Q}$.

Fall 1: $d \equiv 2, 3 \mod 4$

Im ersten Fall sind alle Elemente bekannterweise aufgebaut als $\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Daher ist der maximale Abstand von x bzw. y zum nächstgelegenen Gitterpunkt

in Richtung beider Achsen $\frac{1}{2}$ (siehe Abbildung 1).

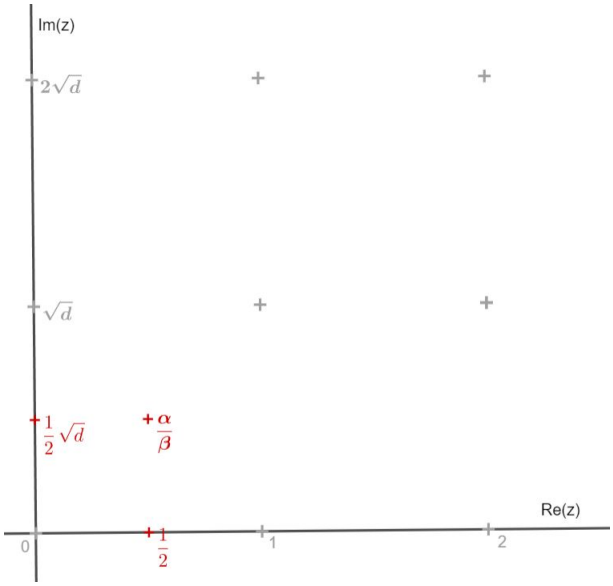


Abbildung 1: rechteckiger Gitteraufbau von $\mathcal{O}_d$ für $d \equiv 2, 3 \mod 4$ mit maximalem Abstand von $\frac{\alpha}{\beta}$ zum nächstgelegenen Gitterpunkt

Wir wählen also diese Punkte $u, v \in \mathbb{Z}$, sodass $q = u + v\sqrt{d}$ und sich mit $\frac{\alpha}{\beta} = x + y\sqrt{d}$ für $x, y \in \mathbb{Q}$ ebendies ergibt:

$$0 \leq |x - u| \leq \frac{1}{2} \quad \text{und}$$
$$0 \leq |y - v| \leq \frac{1}{2}.$$

Nun können wir $\delta(r) = |N(r)|$ bestimmen:

$$\begin{aligned}
|N(r)| &= |N((\frac{\alpha}{\beta} - q)\beta)| \\
&= |N(\frac{\alpha}{\beta} - q) \cdot N(\beta)| \\
&= |N((x-u) + (y-v)\sqrt{d})| \cdot |N(\beta)| \\
&= |((x-u)^2 - d(y-v)^2)| \cdot |N(\beta)| \\
&\leq |\frac{1}{4} - d\frac{1}{4}| \cdot |N(\beta)| \\
&= \frac{1}{4} \cdot |1 - d| \cdot |N(\beta)|
\end{aligned}$$

Im letzten Schritt setzen wir wie gewünscht

$$\frac{1}{4} \cdot |1 - d| < 1.$$

Diese Ungleichung kann aus den gegebenen Voraussetzungen nur für $d = -1, -2$ erfüllt werden und es gilt $|N(r)| < |N(\beta)|$.

Fall 2: $d \equiv 1 \mod 4$

Wir arbeiten nach demselben Vorgehen wie im ersten Fall. Hier ist $\mathcal{O}_d = \frac{1}{2}(\mathbb{Z} + \mathbb{Z}\sqrt{d})$. In diesem Fall sind die Elemente nicht auf einem rechteckigen Gitter angeordnet, sondern es entstehen Parallelogramme. Der maximale Abstand von x und y zu den nächstgelegenen Gitterpunkten ergibt sich aus dem Höhensatz (siehe Abbildung 2).

Lemma 78 (Höhensatz)**.** *Gegeben sei ein rechtwinkliges Dreieck mit der Hypothenuse c und der daraufliegenden Höhe h. Dann teilt die Höhe die Hypothenuse in die Strecken p und q und es gilt $h^2 = pq$.*

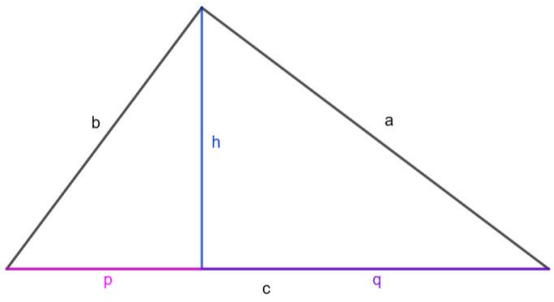


Abbildung 2: Höhensatz im rechtwinkligen Dreieck

$\frac{\alpha}{\beta}$ hat den größtmöglichen Abstand zu den drei umliegenden Gitterpunkten in Abbildung 3 und liegt daher auf dem Höhenschnittpunkt der drei Dreiecksseiten. Die maximale Entfernung des Quotienten zum nächstgelegenen Gitterpunkt entlang der imaginären Achse entspricht $p + q$ und wird wie folgt berechnet:

$$\begin{aligned}
q &= \frac{1}{4}\sqrt{d} && \text{weil } q \text{ die Höhe des gleichschenkligen Dreiecks halbiert} \\
h^2 = p \cdot q &= (\frac{1}{4})^2 && \text{wegen des Höhensatzes} \\
p &= (\frac{1}{4})^2 \cdot \frac{1}{\frac{1}{4}\sqrt{d}} = \frac{1}{4\sqrt{d}} \\
p + q &= \frac{1}{4\sqrt{d}} + \frac{1}{4}\sqrt{d} = \frac{1}{4}(\sqrt{d} + \frac{1}{\sqrt{d}})
\end{aligned}$$

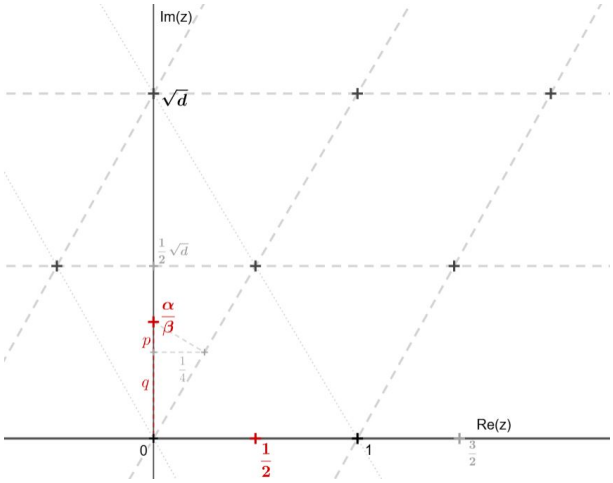


Abbildung 3: parallelogrammartiger Gitteraufbau von $\mathcal{O}_d$ für $d \equiv 1 \mod 4$ mit maximalem Abstand von $\frac{\alpha}{\beta}$ zum nächstgelegenen Gitterpunkt

Wir wählen erneut $u, v \in \mathbb{Z}$, wobei nun $q = u + v \cdot \frac{1+\sqrt{d}}{2}$, und folgendes erfüllt ist:

$$0 \leq |x - \frac{v}{2} - u| \leq \frac{1}{2} \quad \text{und}$$
$$0 \leq |y - \frac{v}{2}| \leq \frac{1}{4}.$$

Wir bestimmen erneut $|N(r)|$:

$$\begin{aligned} |N(r)| &= |N((x - \frac{v}{2} - u) - (y - \frac{v}{2})\sqrt{d})| \cdot |N(\beta)| \\ &= |((x - \frac{v}{2} - u)^2 - d(y - \frac{v}{2})^2)| \cdot |N(\beta)| \\ &\leq |\frac{1}{4} - d\frac{1}{16}| \cdot |N(\beta)| \\ &= \frac{1}{16} \cdot |4 - d| \cdot |N(\beta)| \end{aligned}$$

Die daraus resultierende Ungleichung

$$\frac{1}{16} \cdot |4 - d| < 1$$

wird nur für $d > -12$ erfüllt.

Insgesamt erhalten wir alle Werte für $d < 0$, für die der Ganzheitsring $\mathcal{O}_d$ euklidisch ist, nämlich:

$$d = \{-1, -2, -3, -7, -11\}.$$

[4, S. 236f] [6, 4.1f] [9, S. 103f] [14, S. 101f] □

Die Bestimmung der euklidischen Ganzheitsringe für $d > 0$ ist wesentlich schwieriger und bedarf einiger weiterer geometrischer Zusammenhänge. Wir halten fest

Satz 79. *Sei $d > 0$. Der Ganzheitsring $\mathcal{O}_d \in \mathbb{Q}(\sqrt{d})$ ist normeuklidisch für*

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Beweis. In Satz 77 haben wir den Beweis für $d = 2, 3, 5, 13$ bereits geführt und können diesen direkt übernehmen. Beweise für weitere Werte von d findet man beispielsweise bei Forster [6, S. 4.3f] oder Bundschuh [3, S. 74f]. □

In Abschnitt 2.4 wurden die Besonderheiten von euklidischen Ringen bereits zusammengefasst. So existiert in euklidischen Ganzheitsringen nicht nur eine Division mit Rest, wie wir gerade gezeigt haben, sondern auch ein euklidischer Algorithmus. Besonders interessant sind in euklidischen Ganzheitsringen die Untersuchung der primen Elemente und der Teilbarkeit.

3.3.2 Teilbarkeit in imaginär-quadratischen, euklidischen Ganzheitsringen

Wir wissen bereits, dass in allen Hauptidealringen, also auch in allen euklidischen Ringen gilt: Jedes irreduzible Element ist ein Primelement. ⇔ Jedes prime Element ist irreduzibel.
Es gilt also äquivalent zu Definition 25:

Definition 80. Ein Element q eines euklidischen Ganzheitsrings $\mathcal{O}_d$ heißt ***prim***, wenn gilt:

- q ist keine Einheit ($q \notin \mathcal{O}_d^*$).
- Aus $c \cdot z = q$ mit $c, z \in \mathcal{O}_d$ folgt $c \in \mathcal{O}_d^*$ oder $z \in \mathcal{O}_d^*$.

In Abschnitt 2.3 haben wir die folgenden Aussagen bereits allgemein bewiesen. Der Vollständigkeit halber werden sie hier in Bezug auf Ganzheitsringe wiederholt:

Satz 81 (Primfaktorzerlegung euklidischer Ganzheitsringe)**.** *Sei $\mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper und sein Ganzheitsring $\mathcal{O}_d$ euklidisch. Dann gilt für jedes Element $z \in \mathcal{O}_d$, dass sich z als Produkt von primen Elementen $q_i \in \mathcal{O}_d$, $i \in \{1, ...k\}$ des Ganzheitsrings darstellen lässt, sodass*

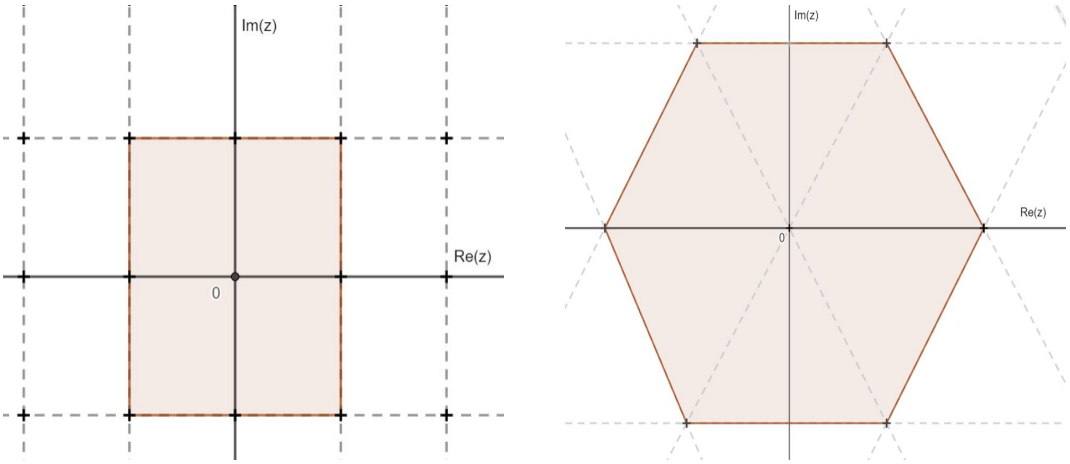
$$z = q_1 \cdot q_2 \cdots q_k,\ k \in \mathbb{N}.$$

Diese Darstellung heißt Primfaktorzerlegung von z. Die Primfaktorzerlegung jedes Elements ist bis auf die Anordnung der Primfaktoren und die Multiplikation mit Einheiten eindeutig.

Proposition 82. *Sei $\mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper und sein Ganzheitsring $\mathcal{O}_d$ euklidisch. Sei q ein primes Element und e eine Einheit dieses Ganzheitsrings. Dann gilt:*

- *eq liegt in $\mathcal{O}_d$ und ist prim.*
- *Das zu q konjugierte Element $\overline{q}$ liegt in $\mathcal{O}_d$ und ist prim.*

Die Einheitengruppen von imaginär-quadratischen Ganzheitsringen enthalten nach Proposition 75 zwei, vier oder sechs Elemente. Daher kommen die Primelemente von euklidischen Ganzheitsringen mit $d < 0$ immer in Gruppen zu je zwei, vier oder sechs Elementen vor. Solche Gruppen werden als ***Primagon*** bezeichnet. Aus geometrischer Sicht entspricht die Anordnung eines Primagons einer Strecke, einem Rechteck oder einem Sechseck mit Mittelpunkt im Koordinatenursprung (siehe Abbildung 4).



(a) Primagon aus vier Elementen für $d = -1$ (b) Primagon aus sechs Elementen für $d = -3$

Abbildung 4: Geometrie eines Primagons in Abhängigkeit des Aufbaus von $\mathcal{O}_d$

Bemerkung 83. Alle Elemente desselben Primagons sind zueinander assoziiert und haben daher denselben Normbetrag.

Beweis. Das Behauptete folgt direkt aus der Herleitung der Einheiten in Proposition 75: Für $q \in \mathcal{O}_d, q \notin \mathcal{O}_d^*, e \in \mathcal{O}_d^*$ ist $q = qe$ und daher $N(q) = N(eq) = N(e) \cdot N(q) = \pm 1 \cdot N(q)$. Aus geometrischer Sicht ist die Behauptung direkt anhand der Symmetrie um den Koordinatenursprung ersichtlich, da alle Elemente auf demselben Kreis (Ellipse) liegen (siehe Abbildung 4). □

Behauptung 84. *Das Primagon eines primen Elements q des imaginär-quadratischen Ganzheitsrings $\mathcal{O}_d$ stimmt nicht immer mit dem Primagon seines konjugierten Elements $\overline{q}$ überein.*

Beweis. Um die Behauptung zu beweisen müssen wir lediglich ein Gegenbeispiel für alle imaginär-quadratischen Ganzheitsringe finden, also für alle Werte $d = -1, -2, -3, -7, -11$.

- Im Fall $d = -1$ wählen wir das Element $q = 2 + \sqrt{-1}$. Das Primagon des Elements q enthält die Elemente

$$\{(2 + \sqrt{-1}), (-2 - \sqrt{-1}), (-1 + 2\sqrt{-1}), (1 - 2\sqrt{-1})\},$$

aber nicht sein konjugiertes Element $\overline{q} = 2 - \sqrt{-1}$.

- Im Fall $d = -2$ wählen wir das Element $q = 1 - \sqrt{-2}$. Das Primagon des Elements q enthält die Elemente
$$\{(1 - \sqrt{-2}), (-1 + \sqrt{-2})\},$$
aber nicht sein konjugiertes Element $\overline{q} = 1 + \sqrt{-2}$.

- Im Fall $d = -3$ wählen wir das Element $q = 2 + \sqrt{-3} = \frac{4+2\sqrt{-3}}{2}$. Das Primagon des Elements q enthält die Elemente
$$\{(2 + \sqrt{-3}), (-2 - \sqrt{-3}), (\frac{-1 + 3\sqrt{-3}}{2}), (\frac{1 - 3\sqrt{-3}}{2}), (\frac{5 - \sqrt{-3}}{2}), (\frac{-5 + \sqrt{-3}}{2})\},$$
aber nicht sein konjugiertes Element $\overline{q} = 2 - \sqrt{-3}$.

- Im Fall $d = -7$ wählen wir das Element $q = 2 + \sqrt{-7} = \frac{4+2\sqrt{-7}}{2}$. Das Primagon des Elements q enthält die Elemente
$$\{(2 + \sqrt{-7}), (-2 - \sqrt{-7})\},$$
aber nicht sein konjugiertes Element $\overline{q} = 2 - \sqrt{-3}$.

- Im Fall $d = -11$ wählen wir das Element $q = \frac{1+\sqrt{-11}}{2}$. Das Primagon des Elements q enthält die Elemente
$$\{(\frac{1 + \sqrt{-11}}{2}), (\frac{-1 - \sqrt{-11}}{2})\},$$
aber nicht sein konjugiertes Element $\overline{q} = \frac{1-\sqrt{-11}}{2}$.

□

3.3.3 Zerlegungsverhalten von Primelementen $p \in \mathbb{Z}$ im Ganzheitsring $\mathcal{O}_d$

Aus vielerlei Hinsicht ist es interessant die Primzahlen $p \in \mathbb{P}$ auf ihre Zerlegbarkeit in den euklidsichen Ganzeitsringen $\mathcal{O}_d$ zu untersuchen. Dass nicht jede Primzahl in einem euklidischen Ganzheitsring ein primes Element bleibt, zeigt sich sofort an

Beispiel 85. Die Primzahl $p = 2$ ist im Ganzheitsring $\mathcal{O}_{-1}$, den Gauß'schen Zahlen, zusammengesetzt, nämlich durch: $2 = (1 + \mathrm{i})(1 - \mathrm{i})$.
Die Teiler $(1 + \mathrm{i})$ und $(1 - \mathrm{i})$ sind echt, da sie keine Einheiten aus $\mathcal{O}_{-1}^* = \{\pm 1, \pm \mathrm{i}\}$ sind.

Eine Primzahl $p \in \mathbb{N}$ wird nach ihrem Verhalten im Ganzheitsring $\mathcal{O}_d$ eingeteilt.

Definition 86. Sei $p \in \mathbb{N}$ prim.
p hat **Typ (I)** $\Leftrightarrow$ p bleibt im Ganzheitsring $\mathcal{O}_d$ prim und heißt **"träge"** bzw. **"inert"**.
p hat **Typ (R)** $\Leftrightarrow$ $p = q^2$ für $q \in \mathcal{O}_d$ und heißt **"verzweigt"** bzw. **"ramified"**.
p hat **Typ (S)** $\Leftrightarrow$ $p = q_1 q_2$ für $q_1, q_2 \in \mathcal{O}_d$ und heißt **"zerfallend"** bzw. **"split"**.

Satz 87 (Charakterisierung der Primelemente in $\mathcal{O}_d$ über die Norm)**.** *Sei $p \in \mathbb{N}$ prim. Dann gilt genau eine der drei folgenden Aussagen:*

(i) p hat Typ (I) und $|N(q)| = p^2$ für ein primes Element $q \in \mathcal{O}_d$.

(ii) p hat Typ (R) und es gilt $p = q^2$ für ein primes Element $q \in \mathcal{O}_d$.

(iii) p hat Typ (S) und $p = q_1 q_2$ für die primen Elemente $q_1, q_2 \in \mathcal{O}_d$.

Beweis. Sei $p \in \mathbb{N}$ prim mit Primfaktorzerlegung $p = q_1 q_2 \cdots q_k$, $k \in \mathbb{N}$, $q_i \in \mathcal{O}_d$. Dann ist $p^2 = N(p) = N(q_1) \cdot N(q_2) \cdots N(q_k)$ mit $N(q_i) \in \mathbb{Z}$. Die Quadratzahl p^2 hat höchstens zwei Primteiler in $\mathbb{Z}$, daher enthält auch die Primfaktorzerlegung von $p^2 = N(q_1) \cdot N(q_2) \cdots N(q_k)$ höchstens zwei Primteiler und es gilt $k \leq 2$, da $N(q_i)$ keine Einheit sein kann, denn $q_i \mid N(q_i)$.
Daraus resultieren die möglichen Ergebnisse, nämlich folgt (i), wenn $k = 1$ ist, das heißt $p = q_1$ ist prim und daher träge.
Gilt $k = 2$ und es gibt zwei nicht assoziierte Primteiler $q_1 \not\sim q_2$, dann ist $p = q_1 q_2$ zerfallend und Aussage (iii) ist gezeigt. Sind $q_1 \sim q_2$ assoziiert, dann ist $N(q_1) \sim N(q_2) \Rightarrow q_1^2 = p$ und es folgt Aussage (ii) und p ist verzweigt. □

Bemerkung 88. Satz 87 gilt allgemein in faktoriellen Ganzheitsringen, da im Beweis weder die Definition 50 des euklidischen Rings noch die Definition 66 der (imaginär-) quadratischen Zahlkörper benötigt wurden.

Satz 89 (Charakterisierung der Primelemente über Primagons)**.** *Sei $p \in \mathbb{N}$ eine Primzahl und q ein primes Element des Ganzheitsrings $\mathcal{O}_d$. Dann gilt genau eine der drei folgenden Aussagen:*

(i) p hat Typ (I) und das Primagon, in dem p liegt enthält ganze Zahlen.

(ii) p hat Typ (R) und das Primagon, in dem das aus p gebildete prime Element q liegt, stimmt mit dem Primagon seines konjugierten Elements $\overline{q}$ überein, das heißt $q \sim \overline{q}$.

(iii) p hat Typ (S) und das Primagon, in dem das aus p gebildete prime Element q liegt, stimmt nicht mit dem Primagon seines konjugierten Elements $\overline{q}$ überein, das heißt $q \not\sim \overline{q}$.

Beweis.

(i) Die Primzahl $p \in \mathbb{N} \subset \mathbb{Z}$ liegt selbst in dem Primagon und da $-1 \in \mathcal{O}_d^*$ für alle imaginär-quadratischen, euklidischen Ganzheitsringe liegt auch $-p \in \mathbb{Z}$ in demselben Primagon.

(ii) Sei $p = q^2$. Dann ist $p = \overline{p} = \overline{q}^2$ und es folgt sofort $q \sim \overline{q}$. Damit ist das Behauptete gezeigt, da alle zueinander assoziierten Elemente auf demselben Primagon liegen.

(iii) Sei $p = q_1 q_2$ und $q_1 \not\sim q_2$, sonst wäre p verzweigt. Dann ist $p = \overline{p} = \overline{q_1 q_2} = \overline{q_1}\,\overline{q_2}$ und daher $q_1 q_2 = \overline{q_1}\,\overline{q_2}$, also ist $q_1 = \overline{q_2}$ oder $q_2 = \overline{q_1}$. Für p gilt daher $p = q_1\overline{q_1}$. Wegen der Voraussetzung gilt $q_1 \not\sim \overline{q_1}$ und damit ist die Behauptung gezeigt.

□

Lemma 90. *In jedem imaginiär-quadratischen, euklidischen Ganzheitsring $\mathcal{O}_d$ gibt es nur eine Primzahl $p \in \mathbb{N}$ vom Typ (R).*

Beweis. Sei v die kleinste aller Primzahlen vom Typ (R). Um über einer Primzahl vom Typ (R) zu liegen, muss das Primagon des aus p gebildeten primen Elements $q_v \in \mathcal{O}_d$ jeweils das zu sich selbst konjugierte Element enthalten. Daher haben die Elemente dieses Primagons nach 83 die Norm $v = N(q_v)$ und liegen auf einem Kreis mit Radius v.
Sei w eine weitere Primzahl vom Typ (R) und $w > v$. Dann gibt es ebenfalls einen Kreis mit Radius w für das aus w gebildete prime Element $q_w \in \mathcal{O}_d$ und sein konjugiertes Element. Dann ist aber q_w entweder ein Vielfaches von q_v und damit nicht prim oder $q_w = q_v$. □

Die vorangegangenen Ergebnisse werden nun zu einem ersten Zerlegungsgesetz zusammengefasst:

Zerlegungsgesetz (für Primzahlen im Ganzheitsring $\mathcal{O}_d$ mithilfe der Norm). Eine Primzahl $p \in \mathbb{P}$ ist im imaginär-quadratischen, euklidischen Ganzheitsring $\mathcal{O}_d$

- **prim**, d.h. $p = q$ mit Primelement $q \in \mathbb{Z}$, genau dann, wenn $|N(q)| = |N(p)| = p^2$.
- **verzweigt**, d.h. $p = q^2$ mit Primelement $q \in \mathbb{Z}$, genau für ein $p \in \mathbb{P}$ und $p = q^2 = q \cdot \overline{q} = N(q)$.
- **zerfallend**, d.h. $p = q_1 q_2$ mit den Primelementen $q_1, q_2 \in \mathbb{Z}$ und $q_1 \not\sim q_2$, in allen anderen Fällen und $p = q_1 q_2 = q_1\overline{q_1} = N(q_1)$.

Bemerkung 91 (Folgerung aus dem Zerlegungsgesetz)**.** Wird die einzige verzweigte Primzahl in $\mathbb{Z}$ ausgeschlossen, dann muss nur entschieden werden, ob $p \in \mathbb{Z}$ träge oder zerfallend ist. Hier gilt:
$p \in \mathbb{Z}$ ist zerfallend. $\Leftrightarrow$ p ist die Norm eines Elements aus $\mathcal{O}_d$, also $p = N(q)$ für ein $q \in \mathcal{O}_d$.

Im Verlauf dieser Arbeit wird dieses Zerlegungsgesetz mithilfe weiterer algebraischer Instrumente konkretisiert und insbesondere für den Fall $d = -3$, den imaginär-quadratischen, euklidischen Ring der Eisensteinzahlen, explizit ausgearbeitet, bewiesen und angewendet.

3.3.4 Teilbarkeit in euklidischen Ganzheitsringen

Die Untersuchung der Zerlegung von Primelementen in euklidischen Ganzheitsringen kann auch mithilfe von quadratischen Resten erfolgen. Dazu definieren wir

Definition 92. Sei $p \in \mathbb{P}$ und $p \neq 2$. Die Zahl $a \in \mathbb{Z}$ mit $p \nmid a$ heißt ***quadratischer Rest*** modulo p, wenn die Kongruenz

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

lösbar ist für ein $x \in \mathbb{Z}$. Ist die Kongruenz nicht lösbar, heißt a "quadratischer Nichtrest".

Daraus lässt sich das sogenannte Legendre-Symbol definieren:

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{falls } a \text{ quadratischer Rest modulo } p \\ -1, & \text{falls } a \text{ quadratischer Nichtrest modulo } p \end{cases}$$

Für das Rechnen mit dem Legendre-Symbol existieren einige Kriterien, deren Beweise hier nicht angeführt werden, aber beispielsweise bei Scheid und Frommer [14, S.239f] nachzulesen sind:

Proposition 93. *Seien p, q ungerade Primzahlen, $a, b \in \mathbb{Z}$, $p \nmid a$ und $p \nmid b$. Dann gilt:*

Euler'sches Kriterium:

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

Produktregel:

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

Folgerungen aus der Quadratischen Reziprozität:

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

Satz 94. *Sei $\mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper mit zulässigem d und sein Ganzheitsring $\mathcal{O}_d$ euklidisch. Sei p eine Primzahl. Dann gelten nach Forster und Frey folgende Aussagen:*

(i) Ist d ein quadratischer Nichtrest modulo $p > 2$, also $\left(\frac{d}{p}\right) = -1$, so gilt für alle $\alpha \in \mathcal{O}_d$: aus $p \mid N(\alpha)$ folgt $p \mid \alpha$.

(ii) Es ist 2 prim in $\mathcal{O}_d$ genau dann, wenn $d \equiv 5 \mod 8$.

(iii) Gilt $p \mid d$, so ist p kein Primelement in $\mathcal{O}_d$.

(iv) Sei $p > 2$ und $p \nmid d$. Es ist $\left(\frac{d}{p}\right) = -1$ genau dann, wenn p ein Primelement in $\mathcal{O}_d$ ist.

Beweis.

(i) Sei $\alpha \in \mathcal{O}_d$ mit $\alpha = a + b\sqrt{d}$ für $d \equiv 2, 3 \mod 4$ bzw. $\alpha = \frac{a+b\sqrt{d}}{d}$ für $d \equiv 1 \mod 4$ mit $a, b \in \mathbb{Z}$. Aus der Berechnung der Norm $N(\alpha)$ erhalten wir für beide Fälle die Kongruenz

$$a^2 \equiv db^2 \mod p.$$

Wäre $b \not\equiv 0 \mod p$, so wäre $\left(\frac{d}{p}\right) = 1$. Es muss daher $b \equiv 0 \mod p$, also auch $a \equiv 0 \mod p$ gelten. Daraus folgt $p \mid a$ und $p \mid b$ und daher $p \mid \alpha$.

(ii) Sei d gerade. Dann ist $2 \mid d = \sqrt{d} \cdot \sqrt{d}$, aber $2 \nmid \sqrt{d}$ und daher ist 2 nicht prim in $\mathcal{O}_d$.
Sei $d \equiv 3 \mod 4$, also $d \equiv 3, 7 \mod 8$. Dann haben die Elemente in $\mathcal{O}_d$ die Form $x + y\sqrt{d}$ mit $x, y \in \mathbb{Z}$ und es gilt $2 \mid 1 - d = (1 - \sqrt{d})(1 + \sqrt{d})$, aber $2 \nmid 1 \pm \sqrt{d}$ und daher ist 2 nicht prim in $\mathcal{O}_d$.
Sei $d \equiv 1 \mod 4$, also $d \equiv 1, 5 \mod 8$. Dann haben die Elemente in $\mathcal{O}_d$ die Form $z = \frac{x+y\sqrt{d}}{2}$ mit $x, y \in \mathbb{Z}$ mit der Norm

$$N(z) = \left(\frac{x}{2}\right)^2 - d\left(\frac{y}{2}\right)^2 = \frac{x^2}{4} - d\frac{y^2}{4} = \frac{1}{4}(x^2 - dy^2) \in \mathbb{Z} \tag{5}$$

Für $d \equiv 1 \mod 8$, also $8 \mid 1 - d$ gilt sicher $2 \mid \frac{1-d}{4} = (\frac{1-\sqrt{d}}{2})(\frac{1+\sqrt{d}}{2})$, aber $2 \nmid \frac{1\pm\sqrt{d}}{2}$ und daher ist 2 nicht prim in $\mathcal{O}_d$.
Im Fall $d \equiv 5 \mod 8$ muss zuvor die Norm $N(z)$ untersucht werden. Sind x, y beide ungerade, dann wäre $x^2 - dy^2$ wegen (5) teilbar durch 8, also $x^2 \equiv dy^2 \mod 8$. Das ist aber wegen $\left(\frac{d}{8}\right) = \left(\frac{5}{8}\right) = -1$ nicht möglich, daher sind x, y beide gerade. Daraus folgt $2 \mid x^2 - dy^2$ und es gilt $2 \mid z$.
Seien nun $\alpha, \beta \in \mathcal{O}_d$ und $2 \mid \alpha\beta$, das heißt $2 \mid N(\alpha)N(\beta)$. Aus dem gerade gezeigten Zusammenhang ergibt sich daher sofort $2 \mid \alpha$ oder $2 \mid \beta$ und daher ist 2 prim im Ganzheitsring $\mathcal{O}_d$.

(iii) Aus $p \mid d$ folgt $p \mid \sqrt{d} \cdot \sqrt{d}$. Es gilt nach Definition $p \nmid \sqrt{d}$ und daher ist p kein Primelement in $\mathcal{O}_d$.

(iv) Sei $\left(\frac{d}{p}\right) = 1$, also $x^2 \equiv d \mod p$ für ein $x \in \mathbb{Z}$. Dann folgt aus $p \mid x^2 - d = (x + \sqrt{d})(x - \sqrt{d})$ aber wegen $p \nmid x \pm \sqrt{d}$ sofort, dass p kein Primelement in $\mathcal{O}_d$ ist.
Sei $\left(\frac{d}{p}\right) = -1$ und seien $\alpha, \beta \in \mathcal{O}_d$, sodass $p \mid \alpha\beta$ mit $\alpha = a + b\sqrt{d}$ und $\beta = r + s\sqrt{d}$, wobei $a, b, r, s \in \mathbb{Z}$.
Aus $p \mid \alpha\beta$ folgt $p \mid N(\alpha)N(\beta)$. Weil die Primfaktorzerlegung in $\mathbb{Z}$ eindeutig ist, folgt daraus $p \mid N(\alpha)$ oder $p \mid N(\beta)$. Gelte $p \mid N(\alpha)$, sodass $p \mid a^2 - db^2$. Wäre $b \not\equiv 0 \mod p$, dann müsste d ein Quadrat mod p sein, was wegen $\left(\frac{d}{p}\right) = -1$ zu einem Widerspruch führt. Es gilt daher $b \equiv 0 \mod p$ und daher $p \mid a$ und daher ist p ein primes Element in $\mathcal{O}_d$.

[5, S. 3.7] [7, S. 225] [9, S. 105] □

Es können also mithilfe des Legendre - Symbols nach (i) diejenigen Primzahlen $p \in \mathbb{Z}$ bestimmt werden, die nach Lemma 4.2.1 prim in $\mathcal{O}_d$ bleiben, also den Typ (I) haben. Weiters können wir aus *(ii)* sofort ablesen, ob die Primzahl 2 im euklidischen Ganzheitsring ein Primelement bleibt.
Forster [5], [7] hat das Legendre - Symbol in Zusammenhang mit der Idealtheorie und der Diskriminante des Ganzheitsrings $\mathcal{O}_d$ gesetzt und kommt zu einem noch detaillierteren Ergebnis. In dieser Arbeit werden diese nur angeführt. Die umfangreichen Beweise zu den Aussagen können in den Originalwerken nachgelesen werden.

3.3.5 Teilbarkeit in allgemeinen quadratischen Zahlkörpern mit nicht notwendig faktoriellem Ganzheitsring $\mathcal{O}_d$

Sei für die folgenden Ausführungen $\mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper mit nicht notwendig faktoriellem Ganzheitsring $\mathcal{O}_d$ und zulässigem d.
Wir erinnern uns an die Idealtheorie aus Kapitel 2.2.3 und halten fest

Proposition 95. *Sei $I \subset \mathcal{O}_d$ ein Ideal, aber kein Hauptideal. Dann lässt sich jedes solche Ideal I durch zwei Elemente $\alpha, \beta \in \mathcal{O}_d$ erzeugen.*

Weiters kann der quadratische Zahlkörper $\mathbb{Q}(\sqrt{d})$ als zweidimensionaler Vektorraum über $\mathbb{Q}$ betrachtet werden mit der bekannten Darstellung aus 73:

$$\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}\rho \quad \text{mit } \rho := \begin{cases} \sqrt{d}, & \text{falls } d \equiv 2,3 \mod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{falls } d \equiv 1 \mod 4 \end{cases}$$

Seien weiter definiert

Definition 96. Zwei linear unabhängige Elemente $\rho_1, \rho_2 \in \mathbb{Q}(\sqrt{d})$ heißen ***Basis*** von $\mathbb{Q}(\sqrt{d})$ über $\mathbb{Q}$, wenn jedes Element von $\mathbb{Q}(\sqrt{d})$ in der Form $a_1\rho_1 + a_2\rho_2$ mit $a_1, a_2 \in \mathbb{Q}$ darstellbar ist.

Definition 97. Die ***Diskriminante*** D einer Basis $\rho_1, \rho_2 \in \mathbb{Q}(\sqrt{d})$ mit den dazu konjugierten Elementen $\overline{\rho_1}, \overline{\rho_2}$ sei definiert durch

$$D(\rho_1, \rho_2) := det \begin{pmatrix} \rho_1 & \overline{\rho_1} \\ \rho_2 & \overline{\rho_2} \end{pmatrix}^2 .$$

Die Diskriminante hängt nicht von der Wahl der Basis ab, das heißt für jede weitere Basis $\rho_1', \rho_2' \in \mathbb{Q}(\sqrt{d})$ gilt $D(\rho_1, \rho_2) = D(\rho_1', \rho_2')$. Die Diskriminante ist in Abhängigkeit von d folgendermaßen aufgebaut:

Satz 98. *Sei wie angegeben $\mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper mit Ganzheitsring $\mathcal{O}_d$. Dann ist*

$$D(\mathbb{Q}(\sqrt{d})) = D(\mathcal{O}_d) = \begin{cases} 4d, & \textit{für } d \equiv 2,3 \mod 4 \\ d, & \textit{für } d \equiv 1 \mod 4 \end{cases}$$

Mithilfe dieser Ausführungen kann nun das Zerlegungsverhalten einer Primzahl $p \in \mathbb{P}$ im Ganzheitsring $\mathcal{O}_d$ untersucht werden durch den folgenden

Satz 99 (Zerlegungsgesetz in allgemeinen quadratischen Zahlkörpern)**.** *Sei $p \in \mathbb{P}, p > 2$ und $(p) = p\mathcal{O}_d$ das von p erzeugte Hauptideal in $\mathcal{O}_d$. Dann gilt eine der drei Aussagen:*

(i) $p \mid D \Rightarrow$ *Es gibt genau ein p enthaltendes Primideal $P \subset \mathcal{O}_d$, nämlich $P = (p, \sqrt{d})$. Für das von p erzeugte Hauptideal gilt $(p) = P^2$.*

(ii) $\left(\frac{D}{p}\right) = 1 \Leftrightarrow$ *Es existiert ein x mit $x^2 \equiv d \mod p$. $\Rightarrow$ Es gibt genau zwei p enthaltende Primideale $P_1, P_2 \subset \mathcal{O}_d$, nämlich $P_{1,2} = (p, x \pm \sqrt{d})$. Für das von p erzeugte Hauptideal gilt $(p) = P_1 P_2$.*

(iii) $\left(\frac{D}{p}\right) = -1 \Rightarrow$ *(p) ist ein Primideal und p ein Primelement in $\mathcal{O}_d$.*

Für allgemeine Ganzheitsringe betreffend die Primzahl 2 halten wir fest

Satz 100. *Sei $p = 2$ und (2) das erzeugte Hauptideal in $\mathcal{O}_d$. Dann gilt:*

- $2 \mid D$ *genau dann, wenn $D = 4d$, also $d \equiv 2, 3 \mod 4$ und analog dem allgemeinen Fall (i) in Satz 99 gilt $(2) = P^2$.*
- $(2) = P_1 P_2$ *genau dann, wenn $d \equiv 1 \mod 8$.*
- (2) *ist ein Primideal genau dann, wenn $d \equiv 5 \mod 8$.*

Zusammengefasst ergibt sich wenig überraschend dasselbe Zerlegungsverhalten für eine Primzahl p im Ganzheitsring $\mathcal{O}_d$, das wir bereits ohne den Zusammenhang mit quadratischen Resten auf Seite 43 festgehalten haben. In diesem Fall können aber alle Ganzheitsringe eingeschlossen werden und das Zerlegungsgesetz muss nicht auf imaginär-quadratische, euklidische Ganzheitsringe eingeschränkt werden:

Zerlegungsgesetz (**für Primzahlen im Ganzheitsring $\mathcal{O}_d$ mithilfe von quadratischen Resten**)**.** Die Primzahl $p \in \mathbb{P}$ ist im Ganzheitsring $\mathcal{O}_d$ mit Diskriminante D

- **prim** und hat **Typ (I)** genau dann, wenn $\left(\frac{D}{p}\right) = -1$ für $p > 2$ und genau dann, wenn $D \equiv 5 \mod 8$ für $p = 2$.
- **verzweigt** und hat **Typ (R)** genau dann, wenn $p \mid D$.
- **zerfallend** und hat **Typ (S)** genau dann, wenn $\left(\frac{D}{p}\right) = 1$ für $p > 2$ und genau dann, wenn $D \equiv 1 \mod 8$ für $p = 2$.

Forster [5] geht noch einen Schritt weiter und berechnet im Ganzheitsring $\mathcal{O}_{-5}$ die trägen und zerfallenden Primzahlen konkret mithilfe einer Umformung und Restklassen.

Bemerkung 101. Satz 99 führt das Zerlegungsgesetz und die Bestimmung der trägen, verzweigten und zerfallenden Primzahlen auf die Berechnung des Legendre-Symbols $\left(\frac{D}{p}\right)$ zurück. In Kapitel 5 wird das Legendre-Symbol im Zusammenhang mit der Reduktionstheorie zu binären quadratischen Formen ebenfalls verwendet um das Zerlegungsgesetz im Ring der Eisensteinzahlen $\mathbb{Z}[\omega]$ aufzustellen und vollständig zu beweisen, jedoch ohne die Verwendung von Satz 99.

3.4 Zusammenfassung

Die Ganzheitsringe $\mathcal{O}_d$ sind in Abhängigkeit von d folgendermaßen aufgebaut (siehe 73):
$\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$ für $d \equiv 2$ oder $d \equiv 3 \mod 4$
$\mathcal{O}_d = \{\frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z}$,a - b gerade$\}$ für $d \equiv 1 \mod 4$.

In imaginär-quadratischen Zahlkörpern haben die euklidischen Ganzheitsringe $\mathcal{O}_d$ die Einheitengruppen (75):

$$\mathcal{O}_d^* = \begin{Bmatrix} \{\pm 1\} & \text{für } d = -2 \text{ oder } d \leq -5 \\ \{\pm 1, \pm \mathrm{i}\} & \text{für } d = -1 \\ \{\pm 1, \pm\frac{1+\sqrt{-3}}{2}, \pm\frac{1-\sqrt{-3}}{2}\} & \text{für } d = -3 \end{Bmatrix}$$

In imaginär-quadratischen Zahlkörpern sind die Ganzheitsringe $\mathcal{O}_d$ genau dann euklidisch, wenn $d = -1, -2, -3, -7, -11$ und haben die euklidische Normabbildung $\delta = |N(\alpha)|$ (77).

In imaginär-quadratischen Zahlkörpern mit euklidischem Ganzheitsring $\mathcal{O}_d$ ist die Primzahl $p \in \mathbb{P}$

- **prim** und hat **Typ (I)** genau dann, wenn $|N(p)| = |N(q)| = p^2$. Insbesondere ist p keine Norm eines Elements in $\mathcal{O}_d$.
- **verzweigt** und hat **Typ (R)** genau für ein $p \in \mathbb{P}$ mit $p = q^2$ für ein primes $q \in \mathcal{O}_d$.
- **zerfallend** und hat **Typ (S)** in allen anderen Fällen und es gilt $p = q_1 q_2$ für die Primelemente $q_1, q_2 \in \mathcal{O}_d$ und $q_1 \not\sim q_2$. Insbesondere ist p die Norm eines Elements in $\mathcal{O}_d$.

In quadratischen Zahlkörpern mit Ganzheitsring $\mathcal{O}_d$ ist die Primzahl $p \in \mathbb{P}$

- **prim** und hat **Typ (I)** genau dann, wenn $\left(\frac{D}{p}\right) = -1$ für $p > 2$ und genau dann, wenn $D \equiv 5 \mod 8$ für $p = 2$.
- **verzweigt** und hat **Typ (R)** genau dann, wenn $p \mid D$.
- **zerfallend** und hat **Typ (S)** genau dann, wenn $\left(\frac{D}{p}\right) = 1$ für $p > 2$ und genau dann, wenn $D \equiv 1 \mod 8$ für $p = 2$.

in Abhängigkeit ihrer Diskriminante $D(\mathcal{O}_d) = \begin{cases} 4d, & \text{für } d \equiv 2, 3 \mod 4 \\ d, & \text{für } d \equiv 1 \mod 4. \end{cases}$

4 Arithmetik im Ring der Eisensteinzahlen $\mathbb{Z}[\omega]$

In diesem Kapitel soll die Arithmetik des Rings der Eisensteinzahlen genau analysiert werden. Dabei werden zuerst die bereits kennengelernten Begriffe Teilbarkeit und Primelement in Bezug auf den euklidischen Ring analysiert und anhand von Beispielen dargestellt.
Als Eisensteinzahlen werden jene Elemente betrachtet, die zu dem Ganzheitsring $\mathcal{O}_{-3}$ des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-3})$ gehören. Bereits in Satz 73 wurde gezeigt, dass für alle $d \equiv 1 \mod 4$, also insbesondere auch für $d = -3$ gilt:

$$\mathcal{O}_{-3} = \{\frac{a + b\sqrt{-3}}{2} : a, b \in \mathbb{Z}, a - b \text{ gerade}\}$$

Anstelle der komplexen Formulierungen, die immer den Term $\sqrt{-3} = \mathrm{i}\sqrt{3}$ enthalten, vereinfachen wir die Schreibweise mithilfe der primitiven, dritten Einheitswurzel $\omega^3 = 1$ mit den Eigenschaften:

- $\omega \neq 1$ und $\omega^2 \neq 1$
- $\omega^2 + \omega + 1 = 0$
- $\omega = e^{\frac{2\pi \mathrm{i}}{3}} = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$

Der Ganzheitsring $\mathcal{O}_{-3}$ ist nach Satz 73 ein Integritätsbereich und aufgebaut durch

$$\mathcal{O}_{-3} = \mathbb{Z} + \mathbb{Z}\omega := \mathbb{Z}[\omega]$$

und alle Elemente $z \in \mathbb{Z}[\omega]$ haben nach 73b) die Form $z = x + y\omega$ mit $x, y \in \mathbb{Z}$ und $\omega = -\rho = -\frac{1+\sqrt{d}}{2}$.

4.1 $\mathbb{Z}[\omega]$ ist euklidisch

Es wurde bereits in Abschnitt 3.3 bewiesen, dass der Ganzheitsring $\mathcal{O}_d$ für $d = -3$ euklidisch ist. Nach Satz 55 und Korollar 56 gilt ebenso, dass $\mathbb{Z}[\omega]$ Hauptidealring und faktorieller Ring ist.
Im euklidischen Ring $\mathbb{Z}[\omega]$ gibt es wie im allgemeinen quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ die Konjugationsabbildung σ für ein Element $z = x + y\omega$. Sie ergibt sich aus dem Zusammenhang $\omega^2 + \omega + 1 = 0$ und lautet:

$$\begin{aligned} \sigma : \mathbb{Z}[\omega] &\to \mathbb{Z}[\omega], \\ x + y\omega &\mapsto x + y\omega^2 \end{aligned}$$

Das konjugierte Element wird auch als $\overline{z}$ bezeichnet. Für die Normabbildung gilt:

Behauptung 102. *Sei $\mathbb{Z}[\omega] \ni z = x + y\omega$ und $N(z) = z \cdot \overline{z}$. Dann heißt $N(z)$ die Norm von z in $\mathbb{Z}[\omega]$. Offensichtlich ist $N(z) \geq 0$ für alle $z \in \mathbb{Z}[\omega]$. Weiter gilt: $N(z) = x^2 - xy + y^2 \in \mathbb{N}$.*

Beweis.

$$\begin{aligned} N(z) = z \cdot \overline{z} = (x + y\omega)(x + y\omega^2) = \\ = x^2 + xy\omega + xy\omega^2 + y^2\omega^3 = \\ = x^2 + xy\omega + xy(-1 - \omega) + y^2 = \\ = x^2 + xy\omega - xy - xy\omega + y^2 = \\ = x^2 - xy + y^2 \end{aligned}$$

Dieser Term ist für alle $x, y \in \mathbb{Z}$ sicher ≥ 0. □

Bemerkung 103. Der Absolutbetrag einer Eisensteinzahl $|z|$ wird auch als die Länge von z bezeichnet und ist $|z| = \sqrt{N(z)}$.

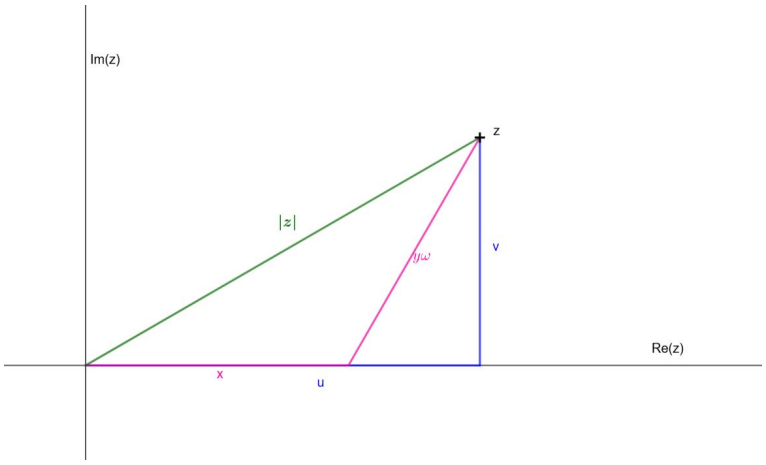


Abbildung 5: Herleitung der Länge $|z|$

Beweis. Sei $z = x + y\omega$ eine Eisensteinzahl mit $x, y \in \mathbb{Z}$. Dann ist nach Abbildung 5 der Absolutbetrag durch Anwendung des Satz von Pythagoras $|z| = \sqrt{u^2 + v^2}$ für $u, v \in \mathbb{R}$. Aus $x + y\omega = x + y(-\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}) = x - \frac{y}{2} + \frac{y \cdot \sqrt{3}}{2}\mathrm{i}$ werden $u = x - \frac{y}{2}$ und $v = \frac{y \cdot \sqrt{3}}{2}$ erhalten. Durch Einsetzen in den obigen Term folgt

$$\begin{aligned} |z| &= \sqrt{(x - \frac{y}{2})^2 + \left(\frac{y \cdot \sqrt{3}}{2}\right)^2} \\ &= \sqrt{x^2 - xy + \frac{y^2}{4} + \frac{3y^2}{4}} \\ &= \sqrt{x^2 - xy + y^2} \\ &= \sqrt{N(z)} \end{aligned}$$

□

Die Teilbarkeit in $\mathbb{Z}[\omega]$ ist analog zu allgemeinen Integritätsbereichen (siehe Definition 22) definiert als:

Definition 104. Seien $z, c \in \mathbb{Z}[\omega]$. Die Eisensteinzahl z heißt Teiler von c, falls es ein $m \in \mathbb{Z}[\omega]$ gibt, sodass $z \cdot m = c$. Man schreibt $z \mid c$. c heißt Vielfaches von z.

Bemerkung 105. Seien $z, c \in \mathbb{Z}[\omega], c \neq 0$ und $z \mid c$, dann gilt $N(z) \mid N(c)$.

Beweis. Aus $z \mid c$ folgt nach Definition, dass es ein $m \in \mathbb{Z}[\omega]$ gibt, sodass $c = z \cdot m$. Da $c \neq 0$ muss auch $m \neq 0$ gelten, also gilt sicher $1 \leq N(m)$. Und daraus folgt sofort

$$N(z) = N(z) \cdot 1 \leq N(z) \cdot N(m) = N(c).$$

□

Ebenso analog zu allgemeinen Integritätsbereichen (siehe Definition 28) definieren wir im Ring $\mathbb{Z}[\omega]$:

Definition 106. Ein Element $d \in \mathbb{Z}[\omega]$ heißt größter gemeinsamer Teiler (ggT) einer Teilmenge $M \subset \mathbb{Z}[\omega], M \neq \emptyset$ oder der Elemente von M, wenn gilt:

- $d \mid a$ für jedes $a \in M$
- $d' \mid a$ für jedes $a \in M \Rightarrow d' \mid d$

Aus Proposition 75 kennen wir bereits die Einheiten des Rings der Eisensteinzahlen, nämlich

$$\begin{aligned}\mathbb{Z}[\omega]^* = \mathcal{O}_{-3}^* &= \{1, -1, \frac{1+\sqrt{-3}}{2}, -\frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, -\frac{1-\sqrt{-3}}{2}\} \\ &= \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}\end{aligned}$$

Wir werden uns noch kurz mit den Grundrechnungsarten im Ring der Eisensteinzahlen beschäftigen. Aufgrund der Eigenschaften jedes Integritätsbereichs liegen die Ergebnisse von Addition, Subtraktion und Multiplikation wieder in $\mathbb{Z}[\omega]$. Dies wird gezeigt anhand:

Beispiel 107. Seien $z = x + y\omega$ und $t = u + v\omega$ mit $x, y, u, v \in \mathbb{Z} \setminus 0$.

Addition:

$$z + t = x + y\omega + u + v\omega = (x + u) + (y + v)\omega$$

Subtraktion:

$$z - t = x + y\omega - (u + v\omega) = (x - u) + (y - v)\omega$$

Multiplikation:

$$\begin{aligned}z \cdot t &= (x + y\omega)(u + v\omega) = \\ &= xu + xv\omega + uy\omega + yv\omega^2 = \\ &= xu + (xv + uy)\omega + yv(-1 - \omega) = \\ &= (xu - yv) + (xv + uy - yv)\omega\end{aligned}$$

Für das Durchführen einer Division wird ein kleiner Trick verwendet, der bereits im Beweis zu Bemerkung 67 verwendet wurde. Es wird mit dem konjugierten Element des Nenners erweitert, um die nach Behauptung 102 sicher ganzzahlige Norm des Nenners zu erhalten. Die Division ist nur im quadratischen Zahlkörper $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ über $\mathbb{Z}[\omega]$ möglich.

Beispiel 108. Seien $z = x + y\omega$ und $t = u + v\omega$ mit $x, y, u, v \in \mathbb{Z} \setminus \{0\}$.

Division:

$$\frac{z}{t} = \frac{x + y\omega}{u + v\omega} = \frac{x + y\omega}{u + v\omega} \cdot \frac{u + v\omega^2}{u + v\omega^2} =$$

$$= \frac{xu + xv\omega^2 - uy\omega + vy\omega^3}{u^2 - uv + v^2}$$

$$= \frac{(xu - xv + vy) - (uy + xv)\omega}{N(t)}$$

Beispiel 109. Zur Veranschaulichung lösen wir dazu eine einfache Aufgabe mit den Zahlen $7 + 9\omega$ und $4 - 3\omega$.

Addition:

$$7 + 9\omega + 4 - 3\omega = 11 + 6\omega$$

Subtraktion:

$$7 + 9\omega - (4 - 3\omega) = 3 + 12\omega$$

Multiplikation:

$$\begin{aligned}
&(7 + 9\omega)(4 - 3\omega) = \\
&= 28 - 21\omega + 36\omega - 27\omega^2 = \\
&= 28 + 15\omega - 27(-1 - \omega) = \\
&= 55 + 42\omega
\end{aligned}$$

Division:

$$\frac{7 + 9\omega}{4 - 3\omega} = \frac{7 + 9\omega}{4 - 3\omega} \cdot \frac{4 - 3\omega^2}{4 - 3\omega^2} =$$

$$= \frac{28 - 21\omega^2 + 36\omega - 27\omega^3}{16 + 12 + 9}$$

$$= \frac{12 + 57\omega}{37}$$

$$= \frac{12}{37} + \frac{57}{37}\omega$$

Offensichtlich liegt das Ergebnis dieser Division wie zuvor behauptet nicht mehr in $\mathbb{Z}[\omega]$, sondern in seinem quadratischen Zahlkörper $\mathbb{Q}(\sqrt{-3})$.
In Analogie zu den ganzen Zahlen kann aber auch in $\mathbb{Z}[\omega]$ eine Division mit Rest durchgeführt werden.

Satz 110 (Division mit Rest)**.** *Seien $a, b \in \mathbb{Z}[\omega]$ und $b \neq 0$.*
Dann gibt es $q \in \mathbb{Z}[\omega]$ und $r \in \mathbb{Z}[\omega]$, sodass $a = q \cdot b + r$ und $N(r) \leq \frac{N(b)}{3}$ gilt.

Beweis. Wir haben bereits in Satz 77 in Kapitel 3.3 gezeigt, dass $\mathbb{Z}[\omega]$ euklidisch ist, sowie den Großteil der Behauptung allgemein für alle imaginär-quadratischen, euklidischen Ganzheitsringe bewiesen. Zu zeigen bleibt die Aussage $N(r) \leq \frac{1}{3} \cdot N(b)$, was mithilfe der Geometrie des aus den Eisensteinzahlen aufgebauten ebenen Gitters geschieht.
a ist ein Punkt in der Ebene der Eisensteinzahlen, deren Gitter, wie in Satz 77 gezeigt, aus Parallelogrammen aufgebaut ist. Sei nun $q \cdot b$ der Gitterpunkt jenes Vielfachen von b, das den kleinsten Abstand zu a hat (siehe Abbildung 6[5]). Alle weiteren Vielfachen von b bilden zu diesem Gitterpunkt gleichschenklige Dreiecke mit der Länge $|b| = \sqrt{N(b)}$. Die maximale Entfernung zwischen den beiden Punkten a und $q \cdot b$ ergibt sich aus der Elementargeometrie, nämlich als genau $\frac{2}{3} \cdot h = \frac{2}{3} \cdot \frac{\sqrt{3}}{2} \cdot \sqrt{N(b)} = \frac{\sqrt{3}}{3} \cdot \sqrt{N(b)}$.
Daher ist $|r| = \sqrt{N(r)} \leq \sqrt{N(b)} \cdot \frac{\sqrt{3}}{3}$ und da $N(r), N(b) \geq 0$ gilt sogar $N(r) \leq N(b) \cdot \frac{1}{3}$. [16, S. 108]

□

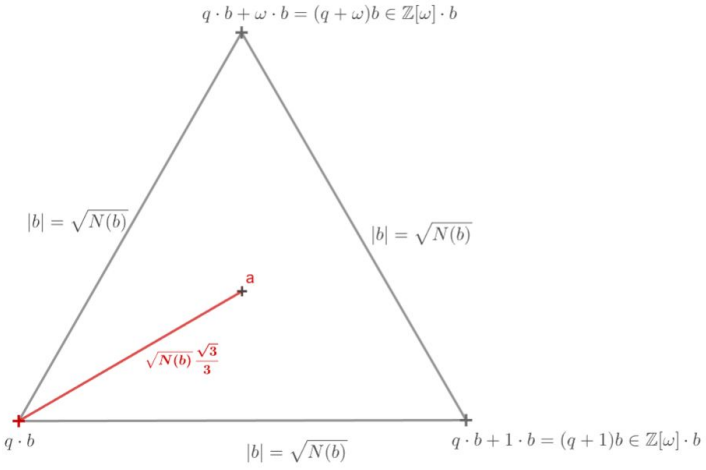


Abbildung 6: maximale Entfernung von z zum Gitterpunkt $q \cdot b$

Anwendungen der Division mit Rest, insbesondere in Bezug auf das Finden eines ggT mithilfe eines euklidischen Algorithmus werden in Abschnitt 4.3 gezeigt.
An dieser Stelle wird ein interessanter Zusammenhang zwischen dem Ring $\mathbb{Z}[\omega]$ und

[5] nach dem Vorbild von Abbildung 4.13 aus Weissman

$\mathbb{Z}[\sqrt{-3}]$ festgehalten. Dieser Zusammenhang ist für diese Arbeit von zentraler Bedeutung und wird, angelehnt an Forster [6, 4.8], gegeben im folgenden

Satz 111. *Zu jedem Element $z \in \mathbb{Z}[\omega]$ gibt es ein assoziiertes Element in $\mathbb{Z}[\sqrt{-3}]$.*

Beweis. Ein Element des Ganzheitsrings $z \in \mathcal{O}_{-3}$ hat die Form $\frac{1}{2}(x+y\sqrt{-3})$ mit $x, y \in \mathbb{Z}$ und $x - y$ gerade.
Dann gilt entweder $x \equiv y \mod 4$ oder $x \equiv -y \mod 4$. Wir betrachten die Fälle einzeln:

Fall 1: $x \equiv y \mod 4$: Wir multiplizieren z mit der Einheit ω:

$$\begin{aligned} z \cdot \omega &= \frac{1}{2}(x + y\sqrt{-3}) \cdot \frac{1}{2}(-1 + \sqrt{-3}) \\ &= \frac{1}{4}(-x - y\sqrt{-3} + x\sqrt{-3} - 3y) \\ &= \frac{1}{4}(-(x + 3y) + (x - y)\sqrt{-3}) \end{aligned}$$

Nach der Voraussetzung folgt daher für x, y:

$$x - y \equiv 0 \mod 4 \quad \text{und} \quad x + 3y \equiv 0 \mod 4 \Rightarrow z \cdot \omega \in \mathbb{Z}[\sqrt{-3}]$$

Fall 2: $x \equiv -y \mod 4$: In diesem Fall multiplizieren wir mit $\overline{\omega} = \omega^2$:

$$\begin{aligned} z \cdot \omega^2 &= \frac{1}{2}(x + y\sqrt{-3} \cdot \frac{1}{2}(-1 - \sqrt{-3} = \\ &= \frac{1}{4}(-x - y\sqrt{-3} - x\sqrt{-3} + 3y) \\ &= \frac{1}{4}(-x + 3y - (x + y)\sqrt{-3}) \end{aligned}$$

Nach der Voraussetzung folgt in diesem Fall für x, y:

$$x + y \equiv 0 \mod 4 \quad \text{und} \quad -x + 3y \equiv 0 \mod 4 \Rightarrow z \cdot \omega \in \mathbb{Z}[\sqrt{-3}]$$

□

4.2 Primelemente in $\mathbb{Z}[\omega]$

Da der Ring $\mathbb{Z}[\omega]$ euklidisch ist, können wir die Begriffe irreduzibel und prim als äquivalent bezeichnen und definieren:

Definition 112. Sei $q \in \mathbb{Z}[\omega] \setminus \mathbb{Z}[\omega]^*$. q heißt prim, wenn gilt: $q = z \cdot t \Rightarrow z \in \mathbb{Z}[\omega]^*$ oder $t \in \mathbb{Z}[\omega]^*$.

Für prime Eisensteinzahlen gelten einige wichtige Zusammenhänge, die direkt aus Abschnitt 3.3 abgeleiten werden können. Insbesondere der Übertrag der Primfaktorzerlegung in euklidischen Ganzheitsringen, siehe Satz 81 und Proposition 82, werden in diesem Abschnitt eine große Rolle spielen.

Die Einheitengruppe des Rings $\mathcal{O}_{-3}$ enthält nach Proposition 75 sechs Elemente und bildet in Multiplikation mit einem Primelement $q \in \mathcal{O}_{-3}$ eine Menge mit sechs Elementen, die nach Abschnitt 3.3.2 als Primagon bezeichnet werden.

4.2.1 Zusammenhang der Arithmetik von $\mathbb{Z}$ und $\mathbb{Z}[\omega]$: Zerlegungsgesetz

Besonders interessant bei der Untersuchung des Rings der Eisensteinzahlen ist die Arithmetik von Primzahlen. Ausgehend vom Ring der ganzen Zahlen sollen einige Eigenschaften von Primelementen in $\mathbb{Z}[\omega]$, sowie die Zerlegung aller Elemente aus $\mathbb{Z}[\omega]$ in ihre Primfaktoren analysiert werden. Wir untersuchen also den Spezialfall $d = -3$ für die bereits in Abschnitt 3.3.2 hergeleiteten Zerlegungsgesetze. Der folgende Abschnitt orientiert sich stark an Kapitel 4 aus "An illustrated theory of numbers" von Martin H. Weissman [16, S. 99f].

Seien für die folgenden Überlegungen $p \in \mathbb{N}$ eine Primzahl und $q \in \mathbb{Z}[\omega]$ eine prime Eisensteinzahl. Im Folgenden wird untersucht, wie sich eine Primzahl aus $\mathbb{N}$ (bzw. der Primelemente aus $\mathbb{Z}$) in $\mathbb{Z}[\omega]$ verhält und umgekehrt. Dieses Verfahren wird als ***Lifting und Lowering von Primelementen*** bezeichnet, mitdessen Hilfe ein konkretes Zerlegungsgesetz für die Primelemente in jedem euklidischen Ring gefunden werden kann. Dafür stellen wir uns die Zahlenmengen als "Ebenen" vor, wobei die Ebene der Eisensteinzahlen höher als jene der ganzen Zahlen liegt. Wie auch im allgemeinen quadratischen Zahlkörper mit Ganzheitsring $\mathcal{O}_d$ werden die primen Elemente in die Typen (I), (R), oder (S) nach Definition 86 eingeteilt.

a. Lifting von Primelementen aus $\mathbb{Z}$

Sei $p \in \mathbb{Z}$ und $q \in \mathbb{Z}[\omega]$. Wir sagen p ***liegt unter*** q, wenn $q \mid p$. Da $p = \overline{p}$ folgt diese Teilbarkeit nur genau dann, wenn auch $\overline{q} \mid p$ gilt. Die Primzahl p liegt also nicht nur unter q, sondern unter den beiden Primagonen von q und $\overline{q}$, also unter sechs oder sogar zwölf primen Elementen aus $\mathbb{Z}[\omega]$ (vgl. Kap 3.3.3)

Satz 113. *Seien $p \in \mathbb{P}$ und $q \in \mathbb{Z}[\omega]$ und prim. Dann gilt genau eine der Aussagen:*

(i) p ist eine prime Eisensteinzahl und hat Typ (I).

(ii) p ist reduzibel in $\mathbb{Z}[\omega]$ und hat Typ (R). Es ist $p = q\overline{q}$, wobei $q \sim \overline{q}$, sodass gilt $q = \overline{q} \cdot e, e \in \mathbb{Z}[\omega]^*$. p liegt unter sechs primen Eisensteinzahlen.

(iii) p ist reduzibel in $\mathbb{Z}[\omega]$ und hat Typ (S). Es ist $p = q\overline{q}$, wobei $q \nsim \overline{q}$. p liegt unter zwölf primen Eisensteinzahlen.

Beweis.
Seien $p \in \mathbb{N}$ und $q \in \mathbb{Z}[\omega]$ prim und gelte $q \mid p$. Dann gibt es eine Zahl $m \in \mathbb{Z}[\omega]$, sodass $p = qm$ und daher auch $p = \overline{qm}$.
Für p^2 folgt daher $p^2 = q\overline{q}m\overline{m}$.
Aus $1 \neq q\overline{q} \in \mathbb{N}$ und $q\overline{q} \mid p^2$, folgt sofort $q\overline{q} = p$ oder $q\overline{q} = p^2$.

Sei $q\overline{q} = p^2$. Dann gilt $m\overline{m} = 1$, also ist m eine Einheit und daher muss p selbst eine prime Eisensteinzahl vom Typ (I) sein und liegt auf seinem Primagon, das auch $\overline{q}$ enthält.

Sei $q\overline{q} = p$. Dann kann p nicht Typ (I) haben, es muss also Typ (R) oder Typ (S) vorliegen. Damit ist $q\overline{q} = p$ bereits die Zerlegung von p in Primfaktoren in $\mathbb{Z}[\omega]$ und p liegt unter den Primagonen von q und $\overline{q}$.
Sei nun $q \sim \overline{q}$, sodass $q = \overline{q} \cdot e$. Dann liegen q und $\overline{q}$ auf demselben Primagon und p hat Typ (R). Andernfalls hat p Typ (S). □

Korollar 114. *Wenn p unter q liegt, dann ist p ein Faktor von $q\overline{q}$.*

b. Lowering von Primelementen aus $\mathbb{Z}[\omega]$

Wir sagen q ***liegt über*** p, wenn $p \mid q\overline{q}$. Da $q = \overline{\overline{q}}$ folgt aus $p \mid \overline{q}\overline{\overline{q}}$ auch, dass $\overline{q}$ über p liegt. Es liegen also die beiden Primagone von q und $\overline{q}$ über p.

Satz 115. *Seien $p \in \mathbb{P}$, $q \in \mathbb{Z}[\omega]$ prim und q liegt über der Primzahl p. Dann ist genau eine der beiden Aussagen erfüllt:*

(i) Das Primagon von q enthält die Primzahl p von Typ (I), sodass $q\overline{q} = p^2$.

(ii) q liegt über einer Primzahl von Typ (R) oder (S) und es gilt $q\overline{q} = p$.

Beweis.
Sei $p \in \mathbb{P}$ und gelte $p \mid q\overline{q}$. Aus Satz 113 folgt, dass p eine prime Eisensteinzahl vom Typ (I) ist oder dass $p = r\overline{r}$ für ein primes $r \in \mathbb{Z}[\omega]$ gilt.

Sei p prim in $\mathbb{Z}[\omega]$. Dann folgt aus der Eindeutigkeit der Primfaktorenzerlegung (Proposition 81), dass $p = q \cdot e$ oder $p = \overline{q} \cdot e$ gilt. Da $p = \overline{p}$ sind äquivalent $p \mid q$ und $p \mid \overline{q}$ und daher liegt p sicher auf dem Primagon von q und hat Typ (I). Daher gilt auch $q\overline{q} = p^2$ und q liegt über p und keiner weiteren Primzahl aus $\mathbb{Z}$.

Sei $p = r\overline{r}$ für ein primes $r \in \mathbb{Z}[\omega]$. Dann ist $q\overline{q}$ ein Vielfaches von $r\overline{r}$. Aus der Eindeutigkeit der Primfaktorenzerlegung folgt aber auch, dass $r = q \cdot e$ oder $r = \overline{q} \cdot e$ gilt. Damit gilt $p = r\overline{r} = q\overline{q}$ und p ist der einzige Primfaktor von $q\overline{q}$. p hat Typ (R) oder Typ (S). □

Korollar 116. *Wenn p ein Faktor von $q\overline{q}$ ist, dann ist q ein Primfaktor von p.*

Aus der Zusammenfassung der beiden Korollare folgen weiter

Korollar 117. *Wenn p unter q liegt, dann ist q ein Primfaktor von p.*

Korollar 118. *q liegt über p genau dann, wenn p unter q liegt.*

c. Das Zerlegungsgesetz für die Elemente aus $\mathbb{Z}[\omega]$

Durch das vorgestellte Verfahren des Lifting und Lowering von Primelementen wird auch hier eine Unterscheidung in die Typen (I), (R) und (S) möglich und kann für den Ring der Eisensteinzahlen abgeleitet werden aus dem allgemeinen Fall in Abschnitt 3.3.2 und konkretisiert werden durch

Zerlegungsverhalten (für Primzahlen im Ring der Eisensteinzahlen $\mathbb{Z}[\omega]$ mithilfe der Norm). Eine Primzahl $p \in \mathbb{N}$ ist im Ring der Eisensteinzahlen $\mathbb{Z}[\omega]$ mit Primelement $q \in \mathbb{Z}[\omega]$

- **prim** und hat **Typ (I)** genau dann, wenn gilt $N(q) = p^2$. Das Primagon indem q liegt enthält die ganze Zahl p sowie das zu q konjugierte Element $\overline{q}$ und besteht aus sechs primen Elementen aus $\mathbb{Z}[\omega]$.
- **verzweigt** und hat **Typ (R)** genau dann, wenn gilt $N(q) = p$ und $q \sim \overline{q}$. Das Primagon indem q liegt stimmt mit dem Primagon seines konjugierten Elements $\overline{q}$ überein und enthält sechs Elemente aus $\mathbb{Z}[\omega]$.
- **zerfallend** und hat **Typ (S)** genau dann, wenn gilt $N(q) = p$ und $q \nsim \overline{q}$. Das Primagon indem q liegt stimmt nicht mit dem Primagon seines konjugierten Elements $\overline{q}$ überein und p enthält zwölf prime Eisensteinzahlen.

Dieses Gesetz gibt uns schon eine Auskunft über die Typen, aber erlaubt uns noch keine konkrete Darstellung des Primelements q. Daher erarbeiten wir ein noch genaueres Zerlegungsgesetz und starten mit

Proposition 119. 3 *ist die einzige Primzahl vom Typ (R).*

Beweis. Da wir bereits in Behauptung 90 gezeigt haben, dass es in jedem imaginärquadratischen Ganzheitsring nur eine Primzahl vom Typ (R) gibt, müssen wir nur noch zeigen, dass es ein primes Element $q \in \mathbb{Z}[\omega]$ gibt, sodass $N(q) = p$ und $q \sim \overline{q}$. Wir wählen $q = 1 - \omega$. Das konjugierte Element ist $\overline{q} = 1 - \omega^2 = 2 + \omega$ und $N(1 - \omega) = 3$. Das Primagon von q über der Primzahl 3 enthält die primen Elemente $\{1 - \omega, -1 + \omega, 1 + 2\omega, -1 - 2\omega, -2 - \omega, 2 + \omega\}$, also auch sein konjugiertes Element $\overline{q}$. □

Die Primzahlen vom Typ (S) sind besonders interessant, da dabei weitere Primelemente in $\mathbb{Z}[\omega]$ gefunden werden können. Daher untersuchen wir

Proposition 120. *Sei p eine Primzahl und $p \neq 3$. Dann gibt es $x, y \in \mathbb{Z}$, sodass $p = x^2 - xy + y^2$ genau dann, wenn p eine Primzahl vom Typ (S) ist.*

Beweis. Typ (R) ist wegen $p \neq 3$ bereits ausgeschlossen.

- $\Leftarrow$ Liegt Typ (S) vor, so gibt es ein über p liegendes primes Element $q = x + y\omega$ und aus $p = q\overline{q}$ folgt $p = x^2 - xy + y^2$.
- $\Rightarrow$ Wenn p die Gestalt $p = x^2 - xy + y^2$ für $x, y \in \mathbb{Z}$ hat, dann kann p dargestellt werden durch $p = (x + y\omega)(\overline{x + y\omega}) = (x + y\omega)(x + y\omega^2)$. Sei $q = (x + y\omega)$, dann gilt $p = q\overline{q}$ und p hat Typ (S).

□

Da jedes Element des Rings $\mathbb{Z}[\omega]$ assoziiert zu einem Element in $\mathbb{Z}[\sqrt{-3}]$ ist, kann bezüglich der Norm für Primzahlen mit Typ (S) außerdem festgehalten werden:

Korollar 121. *Eine Primzahl p vom Typ (S) hat genau dann die Form $x^2 - xy + y^2$ mit $x, y \in \mathbb{Z}$, wenn es $u, v \in \mathbb{Z}$ gibt, sodass die Gleichung $u^2 + 3v^2 = p$ ebenso erfüllt wird.*

Beweis. Die Eisensteinzahl $z = x + y\omega$ hat die Norm $N(z) = x^2 - xy + y^2 = p$ nach Behauptung 102. Für den Ring $\mathbb{Z}[\omega]$ gilt: $\mathbb{Z}[\omega] = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] = \mathcal{O}_{-3} \subseteq \mathbb{Q}(\sqrt{-3})$ und daher kann auch mithilfe der Normdarstellung in allen quadratischen Zahlkörpern nach Definition 69 gearbeitet werden und die Norm geschrieben werden als $N(\alpha) = a^2 - db^2$, also $p = u^2 + 3v^2$. □

Satz 122 (Satz über quadratische Formen)**.** *Eine Primzahl $p \in \mathbb{Z}$ kann genau dann als $x^2 - xy + y^2$ mit $x, y \in \mathbb{Z}$ dargestellt werden, wenn $p = 3$ oder $p \equiv 1 \mod 3$.*

Der Beweis dieses Satzes erfordert einen eigenen Abschnitt 5 zum Thema quadratische Formen und wird daher auf Seite 74 nachgereicht.
Bei zerfallenden Primzahlen ist es interessant die Gestalt von q und $\overline{q}$ direkt angeben zu können. Direkt aus Korollar 121 und Satz 122 folgt

Korollar 123. *Sei $p \equiv 1 \mod 3$ eine Primzahl und $p = q\overline{q}$ mit $q \in \mathbb{Z}[\omega]$. Dann folgt aus $p = u^2 + 3v^2$ mit $u, v \in \mathbb{Z}$ die explizite Gestalt von q mit*

$$q = 2v + (v - u)\omega.$$

Beweis. Sei $q = 2v + (v - u)\omega$. Dann ist
$q \cdot \overline{q} = N(q) = 4v^2 - 2v^2 + 2vu + v^2 - 2vu + u^2 = u^2 + 3v^2 = p.$ □

Die hier genannte Darstellung liefert nur jeweils ein Element jedes Primagons, das über p liegt. Durch Multiplikation mit den Einheiten lassen sich die anderen Elemente schnell berechnen. Dies wird in Abschnitt 4.3 zur Anwendung kommen.

Aus den gewonnenen Erkenntnissen kann nun endgültig ein detailliertes explizites Zerlegungsgesetz für die primen Elemente in $\mathbb{Z}[\omega]$ aufgestellt werden:

Zerlegungsgesetz (für Primzahlen im Ring der Eisensteinzahlen). Eine Primzahl $p \in \mathbb{P}$ ist im Ring der Eisensteinzahlen $\mathbb{Z}[\omega]$

- **prim** und hat **Typ (I)** genau dann, wenn $p \equiv 2 \mod 3$.
- **verzweigt** und hat **Typ (R)** genau dann, wenn $p = 3$.
- **zerfallend** und hat **Typ (S)** genau dann, wenn $p \equiv 1 \mod 3$; das prime Element über $p = u^2 + 3v^2$ hat die Form $q = 2v + (v - u)\omega$.



Abbildung 7: Darstellung der Primzahlen der Typen (I), (R) und (S) am Zahlenstrahl

Die Darstellung dieses Zerlegungsgesetztes erfolgt mithilfe eines Zahlenstrahls (siehe Abbildung 7).
Ebenso in Analogie zu Kapitel 3.3.4 kann das Verhalten der Primzahlen im Ring $\mathbb{Z}[\omega]$ auch mithilfe von quadratischen Resten untersucht werden. Eine erste einfache Anwendung sei gegeben in

Korollar 124. *Die Primzahl $p = 2$ bleibt prim im Ring der Eisensteinzahlen und hat daher Typ (I).*

Beweis. folgt direkt aus Satz 94, da $-3 \equiv 5 \mod 8$. □

Etwas detaillierter können wir das Zerlegungsgesetz von Seite 47 in Abhängigkeit der quadratischen Reste direkt auf den Ring der Eisensteinzahlen übertragen, wobei wir zuerst die Diskriminante nach Satz 98 berechnen:

$$D = -3 \quad \text{für } d \equiv 1 \mod 4.$$

Damit können wir bereits alle Elemente vom Typ (R) angeben, nämlich jene $p \in \mathbb{P}$, für die gilt $p \mid D = -3$, also $p = 3$.

Damit sind wir bereits fertig. Wünschenswert wäre es aber noch, die Primzahlen vom Typ (I) und Typ (S) konkret angeben zu können. Daher zeigen wir wie angekündigt die Methode von Forster [5] anhand unseres Beispiels. Dazu sei zuerst festgehalten, dass Forster das Legendre-Symbol $\left(\frac{D}{p}\right)$ mithilfe der quadratischen Reziprozität und einiger weiterer Zusammenhänge betreffend der Diskriminante zu einer Darstellung in Abhängigkeit von den Restklassen $a \mod D$ umformt, nämlich

$$\chi_D(a) := \prod_{j=1}^{m} \left(\frac{a}{q_j}\right).$$

q_j sind dabei die Primfaktoren von $|D|$. Es gilt $p > 2$ hat Typ (I), falls $\chi_D(a) = -1$ und Typ (S), falls $\chi_D(a) = 1$. In unserem Fall ergibt sich die Primfaktorzerlegung $|D| = 3$. Die möglichen (teilerfremden) Restklassen sind 1 und 2 und daher ergibt sich aus

$$\left(\frac{1}{3}\right) = 1 \qquad \left(\frac{2}{3}\right) = -1$$

das bereits gezeigte Zerlegungsgesetz von Seite 58.

4.2.2 Primzahltest in $\mathbb{Z}[\omega]$

Satz 125 (Kleiner Satz von Fermat)**.** *Für jede Primzahl p und jede dazu teilerfremde ganze Zahl a gilt:*

$$a^{p-1} \equiv 1 \quad mod\ p$$

Euler lieferte für diesen Satz einen kurzen Beweis durch vollständige Induktion. Dabei werden der binomische Lehrsatz und die Eigenschaften des Binomialkoeffizienten verwendet.

Beweis.

- $a = 1$: $a^p \equiv a \mod p$
- $a > 1$: Gilt $a^p \equiv a \mod p$, dann gilt auch $(a+1)^p \equiv a^p + 1 \equiv a + 1 \mod p$.

□

Durch Umkehrung dieser Bedingung kann für jede Zahl $n \in \mathbb{Z}$ getestet werden, ob sie zusammengesetzt ist. Dabei orientieren sich die folgenden Ausführungen an Bundschuh [3, S. 99f] und Forster [7, S. 73f].
Zuerst sei festgehalten, dass die Umkehrung des kleinen Satzes von Fermat leider nur eine notwendige, aber keine hinreichende Bedingung bei der Untersuchung ist. Wir veranschaulichen diese Aussage mithilfe von einem kurzen

Beispiel 126. Sei die zu untersuchende Zahl $n = 645$.
Offensichtlich ist die Zahl n keine Primzahl, weil sie sicher durch 3 und 5 teilbar ist.
Wir berechnen nun für zu n teilerfremde Zahlen $a \in \mathbb{Z}$:

$$a^{n-1} = a^{644} \mod 645$$

Dabei liefern $a = 2 \Rightarrow 2^{644} \equiv 1 \mod 645$ und $a = 11 \Rightarrow 11^{644} \equiv 1 \mod 645$ ein nicht aussagekräftiges Ergebnis, ob n eine Primzahl ist.
Für $a = 7 \Rightarrow 7^{644} \equiv 436 \mod 645$ ergibt sich ein anderes Ergebnis.

Das Beispiel verdeutlicht die Notwendigkeit der Bedingung $a^{n-1} \equiv 1 \mod n$. Um nun Primzahlen mit einer bestimmten Sicherheit bestimmen zu können muss die Äquivalenz also für unterschiedliche, teilerfremde $a \in \mathbb{Z}$ wiederholt werden. Das führt uns direkt zu

Algorithmus 127 (Fermat'scher Primzahltest)**.** Wähle eine ganze Zahl n.
Wähle eine zu n teilerfremde Basis a mit $1 < a < n$. Es gilt:
Wenn $a^{n-1} \not\equiv 1 \mod n$, dann ist n zusammengesetzt. Ansonsten erhält man keine Aussage.
Der Test wird für verschiedene Basen a wiederholt. Erhält man immer das Ergebnis "keine Aussage", kann auf das Ergebnis "vermutlich Primzahl" geschlossen werden.

Alle bekannten Primzahltests für die natürlichen Zahlen haben eine kleine Unsicherheit oder sind in der Praxis nicht durchführbar. In diesem Fall liegt die Unsicherheit des Tests in den sogenannten "Fermatschen Pseudoprimzahlen". Damit sind genau jene natürlichen Zahlen gemeint, die im Fermat'schen Primzahltest fälschlicherweise zu bestimmten Basen das Ergebnis "vermutlich Primzahl" liefern. Es gibt nur sehr wenige Zahlen, die zu allen teilerfremden Basen a ein falsches Ergebnis liefern, die sogenannten Carmichael-Zahlen: $561, 1105, 1729, 2465, 2821, \ldots$.
Es gibt durchaus Primzahltests, die eine weitaus geringere Unsicherheit haben, einige davon sind in den angegebenen Quellen [3][7] nachzulesen.
In dieser Arbeit wird kein Primzahltest verwendet werden, der eine 100-prozentige Sicherheit bietet. Mit derselben Unsicherheit wie in den ganzen Zahlen kann aber für jedes Element $z \in \mathbb{Z}[\omega]$ überprüft werden, ob vermutlich eine Primzahl vorliegt. Dazu müssen wir den Fermat'schen Primzahltest für die Norm $N(z)$ durchführen, da nach Abschnitt 4.2.1 jede prime Eisensteinzahl über einer Primzahl p liegen muss. Ein sicherer Test, der auf den Ring der Eisensteinzahlen aus $\mathbb{Z}$ übertragen werden könnte, ist der sogenannte "A-K-S Test"[6]. Darauf wird in dieser Arbeit aufgrund des Umfangs nicht weiter eingegangen.

Algorithmus 128 (Fermat'scher Primzahltest in $\mathbb{Z}[\omega]$)**.** Wähle eine Zahl $z = x + y\omega$ aus dem Ring der Eisensteinzahlen $\mathbb{Z}[\omega]$. Berechne die Norm $N(z) = x^2 - xy + y^2$. Wähle eine zu $N(z)$ teilerfremde Basis $a \in \mathbb{N}$ mit $1 < a < N(z)$. Es gilt:
Wenn $a^{N(z)-1} \not\equiv 1 \bmod N(z)$, dann ist $N(z)$ zusammengesetzt und z nicht prim in $\mathbb{Z}[\omega]$.
Ansonsten erhält man keine Aussage.
Der Test wird für verschiedene Basen a wiederholt. Erhält man immer das Ergebnis "keine Aussage", kann für $N(z)$ auf das Ergebnis "vermutlich Primzahl" und damit für $z \in \mathbb{Z}[\omega]$ auf "vermutlich prim" geschlossen werden.

Eine konkrete Anwendung des Primzahltests wird im anschließenden Abschnitt durchgeführt.
Der Fermat'sche Primzahltest ist auch direkt in $\mathbb{Z}[\omega]$ ohne die Rückführung auf die Norm möglich. Aufgrund des deutlich größeren Umfangs in der praktischen Durchführung wird auf diese Methode in dieser Arbeit verzichtet.

4.3 Beispiele und Anwendung

4.3.1 Anwendungen der Division mit Rest

In Satz 110 wurde die Division mit Rest im Ring der Eisensteinzahlen bereits formal gezeigt und bewiesen. Dabei sollen der Faktor $q \in \mathbb{Z}[\omega]$ und der Summand $r \in \mathbb{Z}[\omega]$ zu bekannten $a, b \in \mathbb{Z}[\omega]$ gefunden werden, sodass $a = q \cdot b + r$ gilt. Die praktische Durchführung läuft analog zu dem Mechanismus in $\mathbb{Z}$ ab:

[6] AGRAWAL, M., KAYAL, N., SAXENA, N.: PRIMES is in P. Departement of Computer Science & Engineering, Indian Institute of Technology, Kanpur. 2003
abrufbar unter: `https://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf`

1. Führe die exakte Division $a : b$ durch.
2. Wähle den im Gitter der Eisensteinzahlen $\mathbb{Z}[\omega]$ nächstgelegenen Gitterpunkt q zu $a : b$.
3. Führe die Division mit Rest durch, um r zu finden.

Beispiel 129.
Führe eine Division mit Rest der beiden Eisensteinzahlen $a = 7 + 9\omega$ und $b = 4 - 3\omega$ durch.

1. Die exakte Division liefert nach Beispiel 109 das Ergebnis $\frac{12}{37} + \frac{57}{37}\omega$.
2. Wir wählen für den Realteil und den Imaginärteil die beiden nächstliegenden ganzen Zahlen für q. In diesem Fall liefert das $q = 1 + 2\omega$.
3. Die Division mit Rest läuft nun analog zu $\mathbb{Z}$ ab:

$$\begin{aligned}(7 + 9\omega) : (4 - 3\omega) &= 1....\\ (3 + 12\omega)&\end{aligned}$$

$$\begin{aligned}(7 + 9\omega) : (4 - 3\omega) &= 1 + 2\omega\\ 3 + 12\omega&\\ -3 - 2\omega &= r\end{aligned}$$

Das Ergebnis lautet $(7 + 9\omega) = (1 + 2\omega) \cdot (4 - 3\omega) + (-3 - 2\omega)$.
Zur vollständigen Veranschaulichung zeigen wir, dass auch $N(r) \leq N(b)\frac{\sqrt{3}}{3}$ erfüllt ist:

$$N(r) = 9 - 6 + 4 = 7 \leq 21,36.. = \frac{37\sqrt{3}}{3} = N(b)\frac{\sqrt{3}}{3}$$

Letztlich wird noch die Probe durchgeführt

$$\begin{aligned}(1 + 2\omega) \cdot (4 - 3\omega) + (-3 - 2\omega) =&\\ (10 + 11\omega) + (-3 - 2\omega) =&\\ (7 + 9\omega) = a&\end{aligned}$$

Die bekannteste Anwendung der Division mit Rest in $\mathbb{Z}$ ist der euklidische Algorithmus (siehe Algorithmus 62 und Behauptung 63. Ebenso können wir im Ring der Eisensteinzahlen einen euklidischen Algorithmus definieren:

Algorithmus 130. Seien $a, b \in \mathbb{Z}[\omega]$. Wir führen wiederholt eine Division mit Rest durch, sodass wir eine Folge von Zahlen $\mathbb{Z}[\omega] \ni g_i, 1 \leq i \leq m+1$ mit $i, m \in \mathbb{N}$ erhalten. Die rekursive Darstellung der Folge lautet

$$\begin{aligned} g_0 &= a \\ g_1 &= b \\ g_{n-1} &= q_n \cdot g_n + g_{n+1} \end{aligned}$$

Der Algorithmus bricht nach endlich vielen Schritten ab mit $g_{m+1} = 0$.

Beweis. Der Beweis wird äquivalent zu jenem in den ganzen Zahlen geführt:
Für alle g_i gilt, dass $N(g_{n+1}) \leq N(g_n) \cdot \frac{\sqrt{3}}{3}$ und $\frac{\sqrt{3}}{3} < 1$. Daraus folgt $N(g_{n+1}) < N(g_n)$ und da für die Norm nur positive Werte möglich sind, gibt es auch nur endlich viele mögliche Schritte bis wir bei $g_{m+1} = 0$ ankommen. □

Behauptung 131. *Der letzte Wert $\neq 0$ im Euklidischen Algorithmus g_m ist der größte gemeinsame Teiler der beiden Eisensteinzahlen a und b.*

Beweis. Der Beweis der Behauptung kann direkt aus der äquivalenten Behauptung 63 in $\mathbb{Z}$ übernommen werden. □

Im Ring der Eisensteinzahlen können wir die Schreibweise des Algorithmus noch um Einheiten erweitern zu:

$$g_{n-1} = q_n \cdot g_n \cdot e_n + g_{n+1}.$$

Beispiel 132. Finde mithilfe des euklidischen Algorithmus den größten gemeinsamen Teiler der beiden Eisensteinzahlen $a = -49 - 7\omega = g_0$ und $b = 28 + 22\omega = g_1$.

erste Division

Exakte Division: $(-49 - 7\omega) : (28 + 22\omega) = \frac{-224}{326} + \frac{441}{326}\omega$
Bestimmen des Gitterpunkts: $q_1 = -1 + \omega$
Division mit Rest:

$$\begin{aligned} (-49 - 7\omega) : (28 + 22\omega) &= -1 + \omega \\ -21 + 15\omega & \\ 1 + 9\omega = g_2 & \end{aligned}$$

zweite Division

Exakte Division: $(28 + 22\omega) : (1 + 9\omega) = \frac{-26}{73} + \frac{-230}{73}\omega$
Bestimmen des Gitterpunkts: $q_2 = 0 - 3\omega$
Division mit Rest:

$$\begin{aligned} (28 + 22\omega) : (1 + 9\omega) &= -3\omega \\ 1 - 2\omega = g_3 & \end{aligned}$$

dritte Division

Exakte Division: $(1+9\omega) : (1-2\omega) = \frac{-15}{7} + \frac{11}{7}\omega$
Bestimmen des Gitterpunkts: $q_3 = -2+2\omega$
Division mit Rest:

$$\begin{aligned}(1+9\omega) &: (1-2\omega) = -2+2\omega \\ 3&+5\omega \\ -1&-\omega = \omega^2 = g_4\end{aligned}$$

vierte Division

Exakte Division: $(1-2\omega) : (-1-\omega) = 2+3\omega$
Bestimmen des Gitterpunkts: $q_4 = 2+3\omega$
Letzter Wert im Euklidischen Algorithmus: $g_5 = 0$

Damit ist der euklidische Algorithmus abgeschlossen und mit $g_4 = -1-\omega = \omega^2$ ist der größte gemeinsame Teiler von $a = -49-7\omega$ und $b = 28+22\omega$ gefunden. Damit sind a und b sogar teilerfremd.

4.3.2 Anwendungen zur Primzerlegung

Das Zerlegungsgesetz und die Gestalt von $q\overline{q}$ aus Abschnitt 4.2.1 erlaubt uns eine Darstellung der Primzahlen bis 100 in Eisensteinzahlen. Im ersten, einfachen Schritt wird der Typ jeder Primzahl bestimmt.

$2 \equiv 2 \mod 3$	Typ (I)		$43 \equiv 1 \mod 3$	Typ (S)
$3 \equiv 0 \mod 3$	Typ (R)		$47 \equiv 2 \mod 3$	Typ (I)
$5 \equiv 2 \mod 3$	Typ (I)		$53 \equiv 2 \mod 3$	Typ (I)
$7 \equiv 1 \mod 3$	Typ (S)		$59 \equiv 2 \mod 3$	Typ (I)
$11 \equiv 2 \mod 3$	Typ (I)		$61 \equiv 1 \mod 3$	Typ (S)
$13 \equiv 1 \mod 3$	Typ (S)		$67 \equiv 1 \mod 3$	Typ (S)
$17 \equiv 2 \mod 3$	Typ (I)		$71 \equiv 2 \mod 3$	Typ (I)
$19 \equiv 1 \mod 3$	Typ (S)		$73 \equiv 1 \mod 3$	Typ (S)
$23 \equiv 2 \mod 3$	Typ (I)		$79 \equiv 1 \mod 3$	Typ (S)
$29 \equiv 2 \mod 3$	Typ (I)		$83 \equiv 2 \mod 3$	Typ (I)
$31 \equiv 1 \mod 3$	Typ (S)		$89 \equiv 2 \mod 3$	Typ (I)
$37 \equiv 1 \mod 3$	Typ (S)		$97 \equiv 1 \mod 3$	Typ (S)
$41 \equiv 2 \mod 3$	Typ (I)			

Nun wenden wir den zweiten Schritt des Zerlegungsgesetzes an. Wir bestimmen die explizite Gestalt von $q\overline{q}$ der verzweigten Primzahlen mit Typ (S). Wir sehen uns das Verfahren anhand der Primzahl 37 im Detail an:

Beispiel 133.

1. Finde ganzzahlige Lösungen der Gleichung $37 = u^2 + 3 \cdot v^2$.

$$37 = 5^2 + 3 \cdot 2^2$$
$$37 = (5 + 2\sqrt{-3})(5 - 2\sqrt{-3})$$

2. Wandle die Darstellung in ein Element aus $\mathbb{Z}[\omega]$ der Form $z = x + y\omega$ um.

$$x = 2v \qquad \text{und } y = v - u$$
$$x = 2 \cdot 2 = 4 \text{ und } y = 2 - 5 = -3$$

Damit haben wir die primen Elemente $q = 4 - 3\omega$ und $\overline{q} = 4 - 3\omega^2 = 7 + 3\omega$ gefunden.

Das Verfahren liefert jedoch nur zwei der zwölf primen Eisensteinzahlen die über der Primzahl 37 liegen. Um die anderen zehn primen Elemente zu erhalten müssen q und $\overline{q}$ jeweils mit den Einheiten multipliziert werden, sodass wir in diesem Fall folgende zwölf Elemente erhalten:

$$(4 - 3\omega), (-4 + 3\omega), (3 + 7\omega), (-3 - 7\omega), (-7 - 4\omega), (7 + 4\omega),$$
$$(7 + 3\omega), (-7 - 3\omega), (-3 + 4\omega), (3 - 4\omega), (-4 - 7\omega), (4 + 7\omega)$$

Das Verfahren läuft für alle anderen Primzahlen von Typ(S) äquivalent ab und liefert eine vollständige Tabelle. Auf die Multiplikation mit den Einheiten und die Angabe aller Primelemente über den Primzahlen sowie auf die erneute Angabe der Primzahlen vom Typ (I) wird aus Platzgründen verzichtet.

$3 \equiv 0 \mod 3$	Typ (R)	$(1 - \omega), (2 + \omega)$
$7 \equiv 1 \mod 3$	Typ (S)	$(2 - \omega), (3 + \omega)$
$13 \equiv 1 \mod 3$	Typ (S)	$(4 + \omega), (3 - \omega)$
$19 \equiv 1 \mod 3$	Typ (S)	$(2 - 3\omega), (5 + \omega)$
$31 \equiv 1 \mod 3$	Typ (S)	$(6 + \omega), (5 - \omega)$
$37 \equiv 1 \mod 3$	Typ (S)	$(4 - 3\omega), (7 + 3\omega)$
$43 \equiv 1 \mod 3$	Typ (S)	$(6 - \omega), (7 + \omega)$
$61 \equiv 1 \mod 3$	Typ (S)	$(4 - 5\omega), (9 + 5\omega)$
$67 \equiv 1 \mod 3$	Typ (S)	$(2 - 7\omega), (9 + 7\omega)$
$73 \equiv 1 \mod 3$	Typ (S)	$(8 - \omega), (9 + \omega)$
$79 \equiv 1 \mod 3$	Typ (S)	$(10 + 3\omega), (7 - 3\omega)$
$97 \equiv 1 \mod 3$	Typ (S)	$(8 - 3\omega), (11 + 3\omega)$

Oliver Knill lehrt an der Harvard University am Department of Mathematics und hat die primen Eisensteinzahlen auf besonders eindrucksvolle Weise dargestellt (siehe Abbildung 8)[7].

Die Liste lässt sich unendlich erweitern. Gerade deshalb ist es auch in den Eisensteinzahlen von besonderer Bedeutung, dass wir einen Primzahltest durchführen können. Dieser gestaltet sich, wie bereits in Korollar 128 gezeigt, äußerst einfach.

[7] abrufbar unter: `https://people.math.harvard.edu/~knill/primes/eisenstein.html`

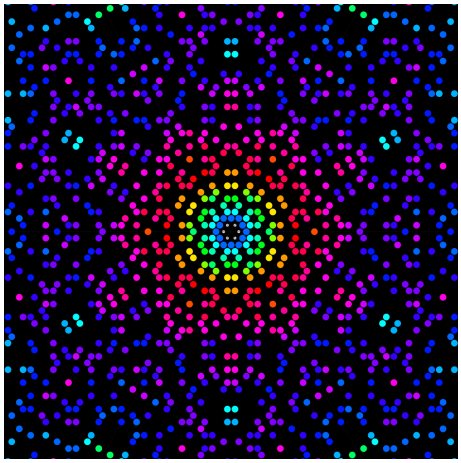


Abbildung 8: Abbildung der primen Eisensteinzahlen von Oliver Knill

Beispiel 134.

- Führe den Fermat'schen Primzahltest in $\mathbb{Z}[\omega]$ für das Element $z = 5 - 2\omega$ durch.
  $N(z) = 5^2 + 5 \cdot 2 + 2^2 = 39$
  Wähle teilerfremdes $a \in \mathbb{N}, a < N(z)$: a = 2.
  $2^{38} = 274877906944 \equiv 4 \mod 39 \not\equiv 1 \mod 39$
  Daraus folgt bereits, dass 39 eine zusammengesetzte Zahl ist und z kein primes Element der Eisensteinzahlen ist.

- Führe den Fermat'schen Primzahltest in $\mathbb{Z}[\omega]$ für das Element $z = 11 - 9\omega$ durch.
  $N(z) = 11^2 + 11 \cdot 9 + 9^2 = 247$
  Wähle teilerfremdes $a \in \mathbb{N}, a < N(z)$: a = 2.
  $2^{246} = 1,13 \cdot 10^{74} \equiv^{(*)} 220 \mod 247 \not\equiv 1 \mod 247$ $^{(*)}$Berechnung mit Technologieeinsatz
  Daraus folgt, dass 247 eine zusammengesetzte Zahl ist und z kein primes Element der Eisensteinzahlen ist.

- Führe den Fermat'schen Primzahltest in $\mathbb{Z}[\omega]$ für das Element $z = 7 - 6\omega$ durch.
  $N(z) = 7^2 + 7 \cdot 6 + 6^2 = 127$
  Wähle teilerfremdes $a \in \mathbb{N}, a < N(z)$: a = 2.
  $2^{126} = 8,06 \cdot 10^{37} \equiv 1 \mod 127$
  $3^{126} = 1,31 \cdot 10^{60} \equiv 1 \mod 127$
  $5^{126} = 1,18 \cdot 10^{88} \equiv 1 \mod 127$
  ...
  Daraus folgt, dass 127 vermutlich eine Primzahl ist und das Element $z = 7 - 6\omega \in \mathbb{Z}[\omega]$ vermutlich prim ist.

Bei kleinen Werten für $N(z)$ lässt sich der Primzahltest sehr schnell durchführen und das Ergebnis als "sicher prim" angenommen werden, da die Carmichael-Zahlen bis 100.000

bekannt und überschaubar sind. Bei sehr großen $N(z)$ kann die Sicherheit des Ergebnisses mithilfe weiterer Primzahltests erhöht werden.

Abschließend wird nun die Faktorisierung in Primfaktoren im Ring $\mathbb{Z}[\omega]$ durchgeführt. Dazu definieren wir:

Algorithmus 135. Sei $m \in \mathbb{Z}[\omega]$.

1. (nur für sehr große m notwendig) Führe den Primzahltest für m durch. Erhält man als Ergebnis "keine Primzahl", können die weiteren Schritte durchgeführt werden.
2. Berechne die Primfaktorzerlegung für $N(m) \in \mathbb{Z}$, sodass
$$N(m) = p_1^{s_1} \cdot p_2^{s_2} \cdots p_n^{s_n}, \quad \text{mit} \quad p_i \in \mathbb{P},\ 1 \leq i \leq n \quad \text{und } i, n, s \in \mathbb{N}.$$
3. Führe die Primfaktoren auf prime Eisensteinzahlen zurück. Dabei gilt:
   a) Ist p^s in der Primfaktorzerlegung von $N(m)$ enthalten und p eine Primzahl vom Typ (I). Dann enthält die Primfaktorzerlegung von m in $\mathbb{Z}[\omega]$ den Primfaktor p genau $\frac{s}{2}$-Mal, also den Faktor $p^{\frac{s}{2}}$.
   b) Ist p eine Primzahl vom Typ (S) oder (R). Dann ist in der Faktorisierung von $m \in \mathbb{Z}[\omega]$ eines der über p liegenden primen Elemente q oder $\overline{q}$ enthalten.

Beweis. Die Bedingungen 3.a) und 3.b) müssen noch bewiesen werden. Sei dazu wie angegeben $m \in \mathbb{Z}[\omega]$ und nicht prim. Sei weiter mit $N(m) = p_1 \cdot p_2 \cdots p_n$ eine Primfaktorenzerlegung für die Norm in den ganzen Zahlen gefunden. Die Bedingungen folgen direkt aus der Definition der Norm und dem Zerlegungsgesetz für Eisensteinzahlen. Sei $m = q_1 \cdot q_2 \cdots q_n\ n \in \mathbb{N}$ die Primfaktorzerlegung von m. Dann ist

$$\begin{aligned} N(m) =& m \cdot \overline{m} = \\ & q_1 \cdot q_2 \cdots q_n \cdot \overline{q_1 \cdot q_2 \cdots q_n} = \\ & q_1 \cdot q_2 \cdots q_n \cdot \overline{q_1} \cdot \overline{q_2} \cdots \overline{q_n} = \\ & q_1\overline{q_1} \cdot q_2\overline{q_2} \cdots q_n\overline{q_n} = \\ & p_1 \cdot p_2 \cdots p_n \end{aligned}$$

Damit ist b) bereits gezeigt. Für a), also Primzahlen vom Typ (I) gilt, dass $N(p) = p^2$. Also gilt für $N(p^{\frac{s}{2}}) = p^{\frac{s}{2}^2} = p^{\frac{2s}{2}} = p^s$.

□

Ebenso wie in allen anderen euklidischen Ringen gilt auch hier, dass die Darstellung einer Eisensteinzahlen in Primfaktoren bis auf die Reihenfolge und Multiplikation mit Einheiten eindeutig ist.

Beispiel 136.

- Gib die Primfaktorenzerlegung der Zahl $m = 12 - 27\omega$ an.

1. $N(m) = 1197$ und $2^{1196} \equiv 256 \not\equiv 1 \mod 1197$
2. $N(m) = 1197 = 3^2 \cdot 7 \cdot 19$
3. $m = (1-\omega)^2 \cdot (2-\omega) \cdot (2-3\omega)$

- Gib die Primfaktorenzerlegung der Zahl $m = -124 + 94\omega$ an.

1. $N(m) = 35868$ und $2^{35867} \equiv 30944 \not\equiv 1 \mod 35868$
2. $N(m) = 35868 = 2^2 \cdot 3 \cdot 7^2 \cdot 61$
3. $m = 2 \cdot (1-\omega) \cdot (2-\omega)^2 \cdot (4-5\omega)$

Alle gezeigten Anwendungen sind sowohl direkt im Ring der Eisensteinzahlen als auch über die Normabbildung möglich.

5 Binäre quadratische Formen

5.1 Grundlagen

Für den Beweis von Satz 122 wird einiges an Vorwissen über binäre quadratische Formen benötigt, das nicht vorausgesetzt werden kann und daher in Anlehnung an Kapitel 3 aus "Advanced Number Theory with Applications" von Richard A. Mollin [12, S. 97f] hier gegeben wird. Dabei wird das Hauptaugenmerk auf positiv definiten Formen liegen, sowie auf dem für den Beweis relevanten Fall $f(x, y) = x^2 - xy + y^2$.

Definition 137. Es sei definiert $f(x, y) = ax^2 + bxy + cy^2$ mit $a, b, c \in \mathbb{Z}$. Dann heißt $f(x, y)$ eine ***ganzzahlige binäre quadratische Form***. Weiter heißt eine binäre quadratische Form ***primitiv***, wenn $ggT(a, b, c) = 1$.

Zur einfacheren Notation wird anstelle der vollständigen quadratischen Form auf die Variablen verzichtet und f als Tripel (a, b, c) notiert.

Definition 138. Je zwei quadratische Formen $f(x, y)$ und $g(x, y)$ heißen ***äquivalent*** ($f \sim g$), wenn es $p, q, r, s \in \mathbb{Z}$ mit $ps - qr = 1$ gibt, sodass

$$f(x, y) = g(px + qy, rx + sy).$$

Kann eine ganze Zahl n mithilfe der quadratischen Form $f(x, y)$ ausgedrückt werden, also $n = f(x, y)$, und ist $ggT(x, y) = 1$, so heißt n eine durch $f(x, y)$ repräsentierte Zahl.

Bemerkung 139. Die oben definierten äquivalenten Formen werden im Allgemeinen als "eigentlich äquivalent" bezeichnet. Gibt es für die Formen f und g eine Transformation mit $ps - qr = -1$ heißen sie "uneigentlich äquivalent". Dieser Fall wird in der vorliegenden Arbeit nicht benötigt und aufgrund der besseren Lesbarkeit wird daher auf die Unterscheidung gänzlich verzichtet.
Selbige Unterscheidung gibt es bei (eigentlich) repräsentierten Zahlen, die im nachfolgenden Lemma 140 besprochen werden. Auch hier wird aus Gründen der Einfachheit auf den "uneigentlichen" Fall verzichtet.

Lemma 140. *Äquivalente Formen repräsentieren dieselben ganzen Zahlen.*

Beweis. Seien $f(x, y)$ und $g(X, Y)$ äquivalente Formen nach Defintion 138, also $X = px + qy$ und $Y = rx + sy$. Dann lässt sich aus der Bedingung $ps - qr = 1$ durch einfache Umformungen der Zusammenhang $x = sX - qY$ und $y = -rX + pY$ herleiten, nämlich:

$$\begin{aligned} sX - qY &= s(px + qy) - q(rx + sy) \\ &= spx + sqy - qrx - qsy \\ &= x(sp - qr) = s \cdot 1 = x \\ -rX + pY &= -r(px + qy) + p(rx + sy) \\ &= -rpx - rqy + prx + psy \\ &= y(-rq + ps) = y \cdot 1 = y \end{aligned}$$

Aufgrund dieses Zusammenhangs gilt $ggT(x, y) = 1$ genau dann, wenn auch $ggT(X, Y) = 1$ gilt und damit ist die Behauptung gezeigt. □

Damit kann eine erste wichtige Beziehung zwischen repräsentierten Zahlen und äquivalenten Formen festgehalten werden.

Proposition 141. *Sei $n \in \mathbb{Z}$ und $f(x,y)$ eine ganzzahlige, binäre quadratische Form. Es gilt $n = f(x,y)$ genau dann, wenn es eine zu $f(x,y)$ äquivalente quadratische Form der Gestalt $nX^2 + Bxy + Cy^2$ mit $B, C \in \mathbb{Z}$ gibt.*

Beweis.

"$\Leftarrow$" Sei $h = nX^2 + Bxy + Cy^2$ eine zu $f(x,y)$ äquivalente Form. Für $x = 1$ und $y = 0$ wird n durch die quadratische Form h repräsentiert und nach Lemma 140 muss jede äquivalente Form ebenfalls n repräsentieren, also $n = f(x,y)$.

"$\Rightarrow$" Schreibe $f(x,y) = ax^2+bxy+cy^2$. Sei nun $f(p,q) = n$ mit $p, q \in \mathbb{Z}$ und $ggT(p,q) = 1$. Dann existieren die ganzen Zahlen r, s mit $ps - qr = 1$. Wir definieren die zu f äquivalente Form $g := f(px+ry, qx+sy)$ und schreiben $g(x,y) = Ax^2+Bxy+Cy^2$. Für die Koeffizienten A, B und C gilt dann:

$$\begin{aligned} g(x,y) &= a(px+ry)^2 + b(px+ry)(qx+sy) + c(qx+sy)^2 \\ &= a(p^2x^2 + 2prxy + r^2y^2) + b(pqx^2 + psxy + qrxy + rsy^2) + c(q^2x^2 + 2qsxy + s^2y^2) \\ &= x^2 \cdot (ap^2 + bpq + cq^2) + xy \cdot (2apr + bps + bqr + 2cqs) + y^2 \cdot (ar^2 + brs + cs^2) \end{aligned}$$

also

$$A = ap^2 + bpq + cq^2$$
$$B = 2apr + bps + bqr + 2cqs$$
$$C = ar^2 + brs + cs^2$$

Da $n = f(p,q) = ap^2 + bpq + cq^2$ folgt $n = A$, das heißt g ist die gesuchte quadratische Form.

□

Definition 142. Es sei definiert $D := b^2 - 4ac$ für $f(x,y) = ax^2+bxy+cy^2$. Dann heißt D die ***Diskriminante*** der quadratischen Form f.
Weiter heißt f indefinit, falls $D > 0$, negativ definit für $D < 0, a < 0$ und positiv definit für $D < 0, a > 0$.

In allem Weiteren werden wir uns auf positiv definite Formen beschränken. An dieser Stelle sei auch die bereits bekannte Definition einer Diskriminante einer Basis eines quadratischen Zahlkörpers 97 aus dem Kapitel über quadratische Reste erwähnt, die als äquivalent zu betrachten ist.

Bemerkung 143. Äquivalente Formen haben dieselbe Diskriminante.

Beweis. Im Beweis zu Proposition 141 wurden bereits die Koeffizienten A, B, C berechnet. Aus einer weiteren einfachen Rechnung erhalten wir die Gleichheit der beiden Diskriminanten $B^2 - 4AC = (b^2 - 4ac)(ps - qr)^2 = (b^2 - 4ac)$. □

Definition 144. Sei $D \equiv 0 \mod 4$ bzw. $D \equiv 1 \mod 4$. Dann heißen $(1, 0, -\frac{D}{4})$ bzw. $(1, 1, -\frac{D-1}{4})$ ***Stammformen*** der Diskriminante D.

5.2 Reduktionstheorie positiv definiter, quadratischer Formen

Definition 145. Die positiv definite, quadratische Form $f(x,y) = ax^2 + bxy + cy^2$ heißt ***reduziert*** genau dann, wenn gilt:

(i) $|b| \leq a \leq c$

(ii) $|b| = a$ oder $a = c \Rightarrow\ b \geq 0$

Die Anzahl h_D der Klassen von primitiven, positiv definiten Formen mit Diskriminante D ist endlich und entspricht genau der Anzahl an redzuzierten Formen mit Diskriminante D.

Satz 146. *Jede positiv definite Form ist äquivalent zu genau einer reduzierten Form.*

Beweis. Sei $f(x,y) = ax^2 + bxy + cy^2$ eine binäre quadratische Form und positiv definit. Sei n die kleinste positive ganze Zahl, die durch f repräsentiert wird. Dann gibt es nach Proposition 141 eine quadratische Form $g(X,Y) = nX^2 + BXY + CY^2$ mit $B, C \in \mathbb{Z}$, die äquivalent zu f ist.
Für ein $z \in \mathbb{Z}$ ergibt die Transformation $X = x - zy, Y = y$ die quadratische Form

$$h(x,y) = nx^2 + (B - 2nz)xy + (nz^2 - Bz + C)y^2.$$

Sei z die nächstgelegene ganze Zahl zum Quotienten $\frac{B}{2n}$, also

$$\begin{aligned} -\frac{1}{2} < \frac{B}{2n} - z \leq \frac{1}{2} \\ \Rightarrow -n \leq B - 2nz \leq n \quad \text{und} \quad |B - 2nz| \leq n \end{aligned}$$

Wir setzen $b_1 = B - 2nz$ und $c_1 = nz^2 - Bz + C$ und erhalten $h(x,y) = nx^2 + b_1xy + c_1y^2$ mit $|b_1| \leq n$.
h ist äquivalent zu f und ist ebenfalls positiv definit (wegen $f \sim g$ und $n > 0$). Da c_1 mit $x = 0, y = 1$ von g repräsentiert wird ist $c_1 \geq n$. Damit ist gezeigt, dass f äquivalent zu einer reduzierten Form ist. Nun ist noch zu zeigen:

Lemma 147. *Je zwei äquivalente, reduzierte Formen sind ident.*

Beweis. Sei $f(x,y) \sim g(X,Y)$ mit $X = px + qy, Y = rx + sy$ und $ps - qr = 1$. Dann sind die Koeffizienten A, B, C nach Proposition 141 berechnet durch

$$\begin{aligned} A &= ap^2 + bpr + cr^2 \\ B &= 2apq + bps + bqr + 2crs \\ C &= aq^2 + bqs + cs^2 \end{aligned}$$

Sei o.B.d.A $a \geq A$ und wegen $D < 0, a > 0$ auch $|b| \leq a \leq c$. Für A gilt daher

$$\begin{aligned} A = ap^2 - bpr + cr^2 &\geq ap^2 - |bpr| + cr^2 \\ &\geq ap^2 - |bpr| + ar^2 = a(p^2 - r^2) - |bpr| \end{aligned} \tag{6}$$

Da weiter $p^2 + r^2 \geq 2|pr|$ folgt

$$a(p^2 + r^2 - |bpr| \geq 2a|pr| - |bpr| \geq a|pr| \quad \text{also} \quad A \geq a|pr|.$$

Aus der zuvor getroffenen Annahme $a \geq A$ folgt $|pr| \leq 1$.
Falls $|pr| = 0 : A = ap^2 + bpr + cr^2 \geq ap^2 + ar^2 = a(p^2 + r^2) \geq a \Rightarrow a = A$.
Falls $|pr| = 1 : A \geq a \Rightarrow A = a$.
Nun ist noch $b = B$ zu zeigen. Die Gleichheit $C = c$ folgt anschließend sofort aus der Gleichheit der Diskriminanten $D_f = D_g$.

Fall 1: Sei $c > C$. Dann ist $c > a$ weil $C \geq A = a$. Wäre $|pr| = 1$ so folgt aus Gleichung 6 sofort der Widerspruch $cr^2 > ar^2 \Rightarrow A > a$. Es muss daher $|pr| = 0$ gelten. Wäre $p = 0$ folgt aus Gleichung 6 sofort erneut der Widerspruch $A > a$, also muss $r = 0$ gelten. Aus $ps - qr = 1$ folgt $ps = 1$ und weil g reduziert ist wissen wir $|B| \leq A = a$ und erhalten $-a \leq |B| - |b| \leq a$. Wir setzen alle bekannten Komponenten ein und erhalten aus $B = 2apq + b$ die Folgerung $q = 0$ und $B = b$.

Fall 2: Sei $c < C$. Der Fall wird analog zum ersten Fall mit vertauschten Rollen für a, b, c bzw. A, B, C bewiesen.

□

Damit ist Satz 146 vollständig bewiesen. □

Beispiel 148. Eisensteinzahlen vom Typ (S) haben nach Kapitel 4.2.1 die Gestalt $p = x^2 - xy + y^2 = f(x, y)$, was einer primitiven, ganzzahligen binären quadratischen Form mit Koeffizienten $(1, -1, 1)$ entspricht.
Die Diskriminante ist $D = b^2 - 4ac = (-1)^2 - 4 \cdot 1 \cdot 1 = -3$ und die Form daher positiv definit.
Die Stammform zur Diskriminante $D = -3 \equiv 1 \mod 4$ ist gegeben durch $g = (1, 1, 1)$, was auch eine reduzierte Form der Diskriminante D ist. Genauer gesagt ist g die einzige reduzierte Form zu Diskriminante $D = -3$, da die Gleichung $-3 = b^2 - 4ac$ unter den Voraussetzungen von Definition 145 in $\mathbb{Z}$ keine weitere Lösung hat. Damit ist $h_{-3} = 1$. Insbesondere ist daher $f \sim g$.

Quadratische Formen stehen in engem Zusammenhang mit quadratischen Resten und können deshalb unter anderem mithilfe des Legendre-Symbols genauer strukturiert werden.

Proposition 149. *Sei $D \in \mathbb{Z}$ mit $D \equiv 0, 1 \mod 4$ und $n \in \mathbb{Z}$ ungerade und teilerfremd zu D. Es existiert eine quadratische Form f der Diskriminante D, die n repräsentiert genau dann, wenn $\left(\frac{D}{|n|}\right) = 1$.*

Beweis.

"⇒" Sei die quadratische Form $f(x, y)$ primitiv und $n \in \mathbb{Z}$ durch f repräsentiert, dann gilt nach Proposition 141 o. E. $f(x, y) = nx^2 + bxy + cy^2$ und daher $D = b^2 - 4nc$. Damit ist D ein quadratischer Rest *modulo* n.

"$\Leftarrow$" Sei $D \equiv b^2 \mod |n|$ und wie angegeben n ungerade. Dann können wir falls notwendig b durch $b+n$ ersetzen, wodurch D und b entweder beide gerade oder beide ungerade sind. Mit $D \equiv 0,1 \mod 4$ folgt daher, dass $D \equiv b^2 \mod 4|n|$. Dann gibt es ein $m \in \mathbb{Z}$, sodass $D = b^2 - 4mn$, also die Diskriminante einer Form $f(x,y) = nx^2 + bxy + my^2$ entspricht. f repräsentiert n durch $(1,0)$ und wegen der Teilerfremdheit von n und D gilt $ggT(n,b,m) = 1$ und f ist primitiv.

□

Damit wurden die wichtigsten Voraussetzungen allgemein gezeigt. Abschließend wird der konkrete Fall $D = -3 \equiv 1 \mod 4$ noch näher ausgeführt und die folgenden Zusammenhänge aus Forster [6, S. 4.7] und Mollin [12, S. 148f] verwendet.

Lemma 150. *Sei $a \in \mathbb{Z}$. Dann gilt für das Quadrat a^2 eine der beiden folgenden Bedingungen:*

- $a^2 \equiv 0 \mod 3$
- $a^2 \equiv 1 \mod 3$

Es folgt für $m \in \mathbb{Z}, 3 \nmid m$:

$$\left(\left(\frac{m}{3}\right) = 1 \Leftrightarrow m \equiv 1 \mod 3\right) \Rightarrow \left(\frac{m}{3}\right) \equiv m \mod 3.$$

Beweis. Sei $a \in \mathbb{Z}$ und $n \in \mathbb{N}$.
Wenn $|a| \equiv 0 \mod 3$, dann ist $|a|^2 = (3n)^2 = 9n^2 = 3(3n^2) \equiv 0 \mod 3$.
Wenn $|a| \equiv 1 \mod 3$, dann ist $|a|^2 = (3n+1)^2 = 9n^2 + 6n + 1 = 3(3n^2 + 2n) + 1 \equiv 1 \mod 3$.
Wenn $|a| \equiv 2 \mod 3$, dann ist $|a|^2 = (3n+2)^2 = 9n^2 + 12n + 4 = 3(3n^2 + 4n + 1) + 1 \equiv 1 \mod 3$. □

Lemma 151. *Sei p prim und ungerade. Dann gilt: $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot \left(\frac{-1}{p}\right)$*

Beweis. Der Beweis folgt sofort aus der Definition des Legendre-Symbols und der quadratischen Reziprozität, sowie aus Lemma 150:

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(3-1)(p-1)}{4}} = (-1)^{\frac{p-1}{2}} \qquad \text{(Quadratische Reziprozität)}$$

$$\left(\frac{p}{3}\right) = \begin{cases} +1, & \text{wenn } p \equiv 1 \mod 3 \\ -1, & \text{wenn } p \equiv 2 \mod 3 \end{cases} \qquad \text{(nach Lemma 150)}$$

$$\Rightarrow \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) \cdot \left(\frac{-1}{p}\right) \qquad \text{(1. Ergänzungssatz)}$$

□

Proposition 152. *Sei p prim und $p > 3$. Es gilt $\left(\frac{-3}{p}\right) = 1$ genau dann, wenn $p \equiv 1 \mod 3$.*

Beweis.

"⇒" Es gilt $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right) \cdot \left(\frac{-1}{p}\right) = 1$ genau dann, wenn beide Terme 1 oder beide -1.

Fall 1: $\left(\frac{3}{p}\right) = 1$ und $\left(\frac{-1}{p}\right) = 1$

$\left(\frac{3}{p}\right) \overset{151}{=} \left(\frac{p}{3}\right) \cdot \left(\frac{-1}{p}\right) = 1$ gilt ebenfalls genau dann, wenn beide Terme 1 oder beide -1. Aufgrund der Voraussetzung $\left(\frac{-1}{p}\right) = 1$ muss nur der positive Fall untersucht werden:
$\left(\frac{p}{3}\right) = 1 \overset{150}{\Leftrightarrow} p \equiv 1 \mod 3$ und $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \mod 4$, also $p \equiv 1 \mod 12$.

Fall 2: $\left(\frac{3}{p}\right) = -1$ und $\left(\frac{-1}{p}\right) = -1$

$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot \left(\frac{-1}{p}\right) = -1$ gilt wegen der Voraussetzung genau dann, wenn $\left(\frac{p}{3}\right) = 1$:
$\left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 1 \mod 3$ und $\left(\frac{-1}{p}\right) = -1 \Leftrightarrow p \equiv 3 \mod 4$, also $p \equiv -5 \mod 12$.

In Summe gilt also $p \equiv 1 \mod 12$ oder $p \equiv -5 \mod 12$ und daher in jedem Fall $p \equiv 1 \mod 3$.

"⇐" Folgt sofort aus Lemma 150 und Lemma 151.

□

Zuletzt wird der endgültige Beweis für das Zerlegungsverhalten der Primelemente in den Eisensteinzahlen fertiggestellt:

Beweis zum Satz über quadratische Formen 122.
Zu zeigen ist die Aussage: Die Primzahl $p \in \mathbb{Z}$ kann genau dann als $x^2 - xy + y^2$ mit $x, y \in \mathbb{Z}$ dargestellt werden, wenn $p = 3$ oder $p \equiv 1 \mod 3$.

Sei zunächst $p \neq 3, p \in \mathbb{P}$.
$p \equiv 1 \mod 3 \overset{152}{\Leftrightarrow} \left(\frac{-3}{p}\right) = 1 \overset{149}{\Leftrightarrow}$ Es existiert eine binäre quadratische Form f mit Diskriminante $D = -3$ und f repräsentiert p.
$\overset{148}{\Leftrightarrow} p$ wird wegen $h_{-3} = 1$ durch genau eine reduzierte quadratische Form, nämlich durch $g = x^2 + xy + y^2$, repräsentiert.
$\overset{148}{\Leftrightarrow} h$ repräsentiert p, da für $h = x^2 - xy + y^2$ gilt $h \sim g$ mit den Transformationskoeffizienten $p = s = 0, q = 1, r = -1$.
$\overset{102}{\Leftrightarrow}$ Es existiert $z = x + y\omega \in \mathbb{Z}[\omega]$ mit $x, y \in \mathbb{Z}$, sodass $N(z) = N(x + y\omega) = p$.

Schließlich wird $p = 3$ dargestellt als $3 = 1^2 + 1 \cdot 1 + 1^2$. □

6 Fazit

Das Ziel dieser Masterarbeit war es, den Ring der Eisensteinzahlen im Hinblick auf seine Arithmetik näher zu untersuchen und dabei besonders die Teilbarkeit und die Primelemente zu analysieren sowie eine Faktorisierung zu erarbeiten, die mit den bekannten Methoden in $\mathbb{Z}$ verglichen werden kann.
Zur Erreichung dieses Ziels wurden zuerst die Grundlagen aus Algebra und Zahlentheorie in Bezug auf die Struktur von Ringen erarbeitet. Demnach gibt es in allen euklidischen Ringen, das sind gemäß Definition Integritätsbereiche R mit einer Abbildung $\delta : R \to \mathbb{N}$, eine Division mit Rest und einen euklidischen Algorithmus, der den größten gemeinsamen Teiler zweier Elemente liefert. Zusätzlich dazu gibt es in all solchen Ringen R eine eindeutige Primfaktorzerlegung und jedes Primelement ist irreduzibel. Im Anschluss wurden jene imaginär-quadratischen Zahlkörper gesucht, die euklidisch sind und damit genau eine solche Darstellung von zusammengesetzten Elementen in irreduzible Primfaktoren liefern. Dabei wurde der Schwerpunkt auf die imaginär-quadratischen Zahlkörper gelegt, da die Eisensteinzahlen im Zahlkörper $\mathbb{Q}(\sqrt{-3})$ liegen. Als abschließende Resultate des dritten Kapitels wurden Zerlegungsgesetze mithilfe von Norm, quadratischen Resten und der Diskriminante geliefert, die Aufschluss darüber geben, ob eine Primzahl p im Ganzheitsring $\mathcal{O}_d$ ein primes Element bleibt oder zusammengesetzt ist. Im vierten Kapitel konnte dadurch zuerst gezeigt werden, dass der Ring der Eisensteinzahlen $\mathbb{Z}[\omega]$ mit der Normabbildung $\delta = N(z) = z \cdot \overline{z}, z \in \mathbb{Z}[\omega]$ euklidisch ist und daher eine Division mit Rest durchführbar ist. Ebenso wurde die Existenz des euklidischen Algorithmus in $\mathbb{Z}[\omega]$ gezeigt und anhand von Beispielen verdeutlicht. Für die Erarbeitung der Primelemente wurden die allgemeinen Zerlegungsgesetze in Abhängigkeit von $p \mod 3$ konkretisiert und eine exakte Zerlegung für zerfallende Primzahlen in $\mathbb{Z}[\omega]$ hergeleitet. Zusätzlich wurde für Eisensteinzahlen $z \in \mathbb{Z}[\omega]$ mit besonders großer Norm $N(z)$ der aus den ganzen Zahlen bekannte Fermat'sche Primzahltest auf den Ring der Eisensteinzahlen übertragen und angewendet. Anschließend konnte mithilfe aller vorherigen Ergebnisse eine Primfaktorenzerlegung in $\mathbb{Z}[\omega]$ hergeleitet und durchgeführt werden. Mithilfe der Analyse der binären quadratischen Form $f(x, y) = x^2 - xy + y^2$ und der im letzten Kapitel vorgestellten Reduktionstheorie wurde das Zerlegungsgesetz im Ring der Eisensteinzahlen abschließend vollständig bewiesen.
Eine faszinierende Anwendung der Arithmetik der Eisensteinzahlen, die in dieser Arbeit nicht thematisiert wurde, ist der Beweis des Reziprozitätsgesetzes für kubische Reste. Der erstmalige Beweis für das Gesetz wurde von Eisenstein selbst gegeben. Die bekannteste Anwendung dürfte der Beweis des Großen Satz von Fermat: $a^n + b^n \neq c^n$ für $n = 3$ sein. Potenzial zur Fortführung des Themas hat auch die ausgeweitete Untersuchung von weiteren binären quadratischen Formen, die im Ansatz bereits in Abschnitt 5 gezeigt wurden. Eine weitere Möglichkeit an diese Arbeit anzuknüpfen ist die Idee von Oliver Knill [8], der eines der bekanntesten ungelösten Probleme der Zahlentheorie, die Goldbachsche Vermutung, unter anderem auf prime Eisensteinzahlen anwendet.

[8] KNILL, O.: Goldbach for Gaussian, Hurwitz, Octavian and Eisenstein primes. Department of Mathematics, Harvard University, Cambridge, MA. 2016. abrufbar unter: `https://arxiv.org/pdf/1606.05958`

Abbildungsverzeichnis

1 rechteckiger Gitteraufbau von $\mathcal{O}_d$ für $d \equiv 2,3 \mod 4$ mit maximalem Abstand von $\frac{\alpha}{\beta}$ zum nächstgelegenen Gitterpunkt 36
2 Höhensatz im rechtwinkligen Dreieck 37
3 parallelogrammartiger Gitteraufbau von $\mathcal{O}_d$ für $d \equiv 1 \mod 4$ mit maximalem Abstand von $\frac{\alpha}{\beta}$ zum nächstgelegenen Gitterpunkt 38
4 Geometrie eines Primagons in Abhängigkeit des Aufbaus von $\mathcal{O}_d$ 40
5 Herleitung der Länge $|z|$ 50
6 maximale Entfernung von z zum Gitterpunkt $q \cdot b$ 53
7 Darstellung der Primzahlen der Typen (I), (R) und (S) am Zahlenstrahl . 59
8 Abbildung der primen Eisensteinzahlen von Oliver Knill 66
9 Abbildung der primen Eisensteinzahlen von Oliver Knill 76

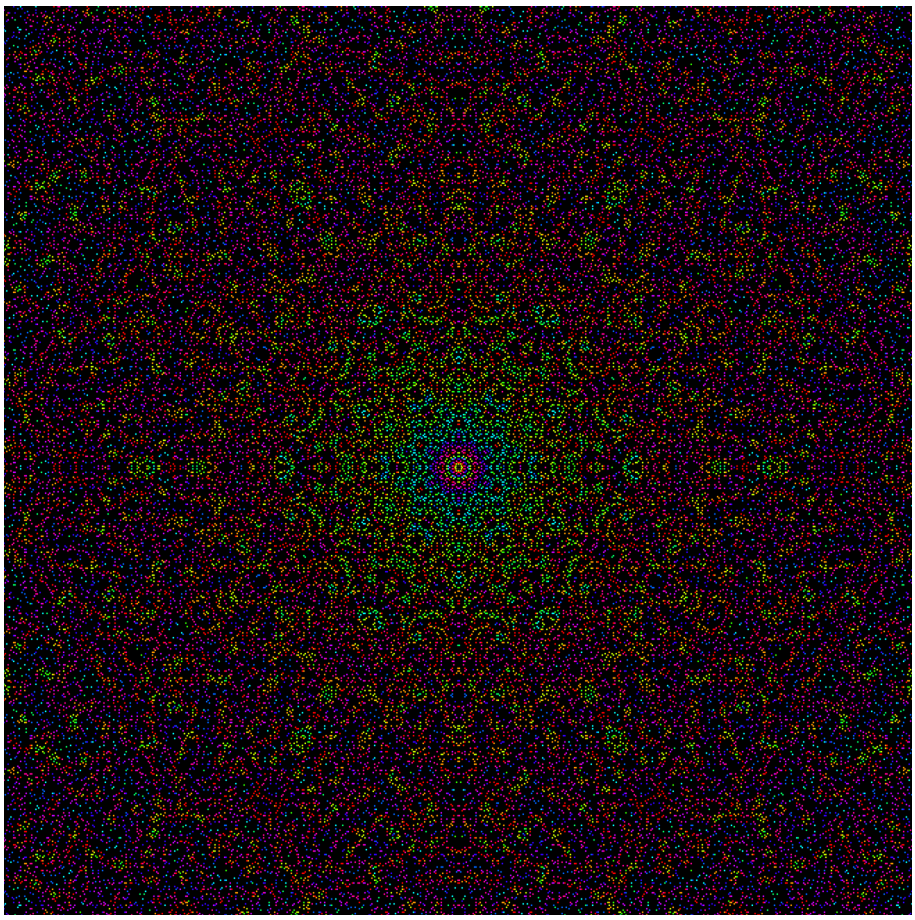


Abbildung 9: Abbildung der primen Eisensteinzahlen von Oliver Knill

Literatur

[1] BIERMANN, K.-R.: Gotthold Eisenstein: Die wichtigsten Daten seines Lebens und Wirkens. In Journal für die reine und angewandte Mathematik. Band 214/215, Berlin: Walter de Gruyter & Co., 1964
abrufbar unter: https://gdz.sub.uni-goettingen.de/id/PPN243919689_0214_0215

[2] BOSCH, S.: Algebra. 8. Auflage, Berlin: Springer Spektrum, 2013

[3] BUNDSCHUH, P.: Einführung in die Zahlentheorie. 6. Auflage, Berlin: Springer, 2008

[4] FISCHER, G.: Lehrbuch der Algebra: Mit lebendigen Beispielen, ausführlichen Erläuterungen und zahlreichen Bildern. 3. Auflage, Wiesbaden: Springer Spektrum, 2013

[5] FORSTER, O.: 3. Quadratische Zahlkörper. In Algebraische Zahlentheorie: Vorlesung von O. Forster im SS 2014 am Mathematischen Institut der LMU München. Homepage der LMU München: https://www.mathematik.uni-muenchen.de, 15.10.2017
abrufbar unter: https://www.mathematik.uni-muenchen.de/~forster/lehre/vorlB4s_ant.html

[6] FORSTER, O.: 4. Norm-euklidische quadratische Zahlkörper. In Algebraische Zahlentheorie: Vorlesung von O. Forster im SS 2014 am Mathematischen Institut der LMU München. Homepage der LMU München: https://www.mathematik.uni-muenchen.de, 15.10.2017
abrufbar unter: https://www.mathematik.uni-muenchen.de/~forster/lehre/vorlB4s_ant.html

[7] FORSTER, O.: Algorithmische Zahlentheorie. 2. Auflage, Wiesbaden: Springer Spektrum, 2015

[8] FORSTER, O.: 16. Das Quadratische Reziprozitätsgesetz. In Einführung in die Zahlentheorie: Vorlesung von O. Forster im SS 2004 am Mathematischen Institut der LMU München. Homepage der LMU München: https://www.mathematik.uni-muenchen.de, 10.07.2004
abrufbar unter: https://www.mathematik.uni-muenchen.de/~forster/v/zth/inzth_16.pdf

[9] FREY, G.: Elementare Zahlentheorie. Braunschweig: Vieweg, 1984

[10] JACOBSON, N.: Basic Algebra I, 2. Auflage, New York: W.H. Freeman and Company, 1985

[11] KARPFINGER, C., MEYBERG, K.: Algebra: Gruppen - Ringe - Körper. 3. Auflage, Berlin: Springer, 2013

[12] MOLLIN, R. A.: Advanced Number Theory with Applications. Boca Raton: CRC Press, 2010

[13] NEUE DEUTSCHE BIOGRAPHIE: herausgegeben von der historischen Kommission bei der Bayerischen Akademie der Wissenschaften. Dittel - Falck. 4. Band, Berlin: Duncker & Humblot, 1959

[14] SCHEID, H., FROMMER, A.: Zahlentheorie. 4. Auflage, Berlin: Springer Spektrum, 2013

[15] SCHICHL, H., STEINBAUER, R.: Einführung in das mathematische Arbeiten. 2. Auflage, Berlin: Springer Spektrum, 2012

[16] WEISSMAN, M. H.: An illustrated theory of numbers. Providence, Rhode Island: American Mathematical Society, 2017

[17] WÜSTHOLZ, G.: Algebra: Für Studierende der Mathematik, Physik, Informatik. 3. Auflage, Wiesbaden: Springer, 2020