GAUSS'SCHE ZAHLEN $\mathbb{Z}[i]$ UND $\mathbb{Z}[\sqrt{3}]$

JÖRAN SCHLÖMER

Auf den folgenden Seiten untersuchen wir die grundlegenden Eigenschaften der gauss'schen Zahlen $\mathbb{Z}[i]$, sowie des Ringes $\mathbb{Z}[\sqrt{3}]$. Insbesondere werden wir zeigen, dass beide Ringe euklidisch sind, ihre Einheiten bestimmen sowie in beiden Fällen die Primelemente bis auf Assoziiertheit bestimmen.

Definitionen

Wir beginnen mit den notwendigen Definitionen, die wir im weiteren Verlauf benötigen. Zuerst gilt es unsere beiden Ringe zu definieren.

Definition 1. *Wir bezeichnen mit $\mathbb{Z}[i]$ die Menge*

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

Für $(a + bi), (c + di) \in \mathbb{Z}[i]$ definieren wir die Operationen

$$(a + bi) + (c + di) = (a + c) + (c + d)i,$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Mit diesen Operationen ist $\mathbb{Z}[i]$ ein Ring, welchen wir Gauss'sche Zahlen nennen. Für ein Element $x = (a + bi)$ definieren wir das konjugierte Element $\bar{x} = (a - bi)$.

Analog dazu definieren wir auch den zweiten Ring, den wir untersuchen werden:

Definition 2. *Wir bezeichnen mit $\mathbb{Z}[\sqrt{3}]$ die Menge*

$$\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}.$$

Für $(a + b\sqrt{3}), (c + d\sqrt{3}) \in \mathbb{Z}[\sqrt{3}]$ definieren wir die Operationen

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (c + d)\sqrt{3},$$
$$(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}.$$

Mit diesen Operationen ist auch $\mathbb{Z}[\sqrt{3}]$ ein Ring. Für ein Element $x = (a + b\sqrt{3})$ definieren wir das konjugierte Element $\bar{x} = (a - b\sqrt{3})$.

Wir benötigen für unsere weiteren Untersuchungen einige Begrifflichkeiten aus der Teilbarkeitstheorie, welche wir nun kurz wiederholen. Dabei folgen wir den Definition in A. Schmidts Buch über algebraische Zahlentheorie [2]. Im Folgenden sind alle Ringe kommutativ mit 1-Element.

Definition 3. *In einem Ring R nennen wir zwei Elemente $a, b \in R$ assoziiert, wenn die beiden Elemente sich gegenseitig teilen, in Symbolen ausgedrückt $a \mid b$ und $b \mid a$. Für assoziierte Elemente schreiben wir $a \sim b$.*

Für uns von besonderem Interesse in Ringen sind irreduzible Elemente und Primelemente.

Definition 4. *In einem Ring R wird ein Element $\pi \in R$ irreduzibel genannt, wenn es von Null verschieden sowie keine Einheit ist und gilt*

$$\pi = ab \implies a \text{ oder } b \text{ ist eine Einheit.}$$

Ein Element $\pi \in R$ ist ein Primelement, wenn es von Null verschieden ist und keine Einheit ist, sowie gilt

$$\pi \mid ab \implies \pi \mid a \text{ oder } \pi \mid b.$$

Definition 5. *Ein Ring heisst Integritätsring, wenn*

$$ab = 0 \implies a = 0 \text{ oder } b = 0.$$

Lemma 6. *In einem Integritätsring R gilt $a \sim b$ genau dann wenn eine Einheit $u \in R$ existiert, so dass $a = bu$.*

Beweis. Wenn $a = bu$ für eine Einheit $u \in R$, dann gilt auch $b = au'$ für eine Einheit u'. Es folgt, dass $a \mid b$ und $b \mid a$. Für die Gegenrichtung gilt, wenn $a = 0$, so gilt auch $b = 0$. Wenn $a \neq 0$, so folgt nach Annahme, dass es $u, u' \in R$ gibt, so dass $a = bu$ und $b = au'$. Es folgt $a = auu'$, weshalb also $a(1 - uu') = 0$ folgt. In einem Integritätsring folgt dann aber wegen $a \neq 0$, dass $(1 - uu') = 0$, so dass u und u' Einheiten sind. Die Behauptung folgt. □

Darüber hinaus werden uns zwei Typen von Ringen besonders interessieren. Auf der einen Seite sind das die sogenannten faktoriellen Ringe.

Definition 7. *Ein Integritätsring R heißt faktoriell wenn jede von Null verschiedene Nicht-Einheit $a \in R$ eine bis auf Einheiten und Reihenfolge eindeutige Zerlegung als Produkt irreduzibeler Elemente hat.*

Darüber hinaus möchten wir zeigen, dass $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$ sogenannte euklidische Ringe sind.

Definition 8. *Ein Integritätsring R heißt euklidisch, wenn es eine Abbildung $N : R\backslash\{0\} \to \mathbb{N}$ gibt, so dass es für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren, die*

$$a = qb + r \text{ und } N(r) < N(b) \text{ oder } r = 0$$

erfüllen. Wir nennen eine solche Abbildung (euklidische) Normfunktion.

Euklidische Ringe sind von Bedeutung, da es in ihnen möglich ist eine verallgemeinerte Version der euklidischen Division zu definieren mit Hilfe derer beispielsweise die Bestimmung eines größten gemeinsamen Teilers für beliebige Element des Ringes möglich ist.

Bemerkung 9. Auf einem Ring kann es mehrere euklidische Normfunktionen geben.

Nachdem wir nun alle notwendigen Definitionen gegeben haben, zeigen wir zunächst einige Eigenschaften euklidischer Ringe, bevor wir uns den Ringen $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$ zuwenden.

Euklidische Ringe

In diesem Abschnitt beweisen wir einige Eigenschaften euklidischer Ringe, die im weiteren Verlauf nützlich sein werden. Wir orientieren uns weiterhin stark an [2].

Proposition 10. *Für einen euklidischen Ring R gibt es eine euklidische Normfunktion N mit*

$$N(a) \leqslant N(ab) \tag{1}$$

für alle von Null verschiedenen Elemente $a, b \in R$.

Beweis. Sei N' eine beliebige euklidische Normfunktion auf R. Wir definieren nun eine weitere Abbildung

$$N : R\backslash\{0\} \to N, a \mapsto \min_{a' \sim a'} N'(a').$$

Um zu sehen, dass es sich bei N um eine euklidische Normfunktion handelt, wählen wir $a, b \in R$ mit $b \neq 0$. Sei nun b' das zu b assozierte Element in R welches $N(b) = N'(b')$ erfüllt. Da R euklidisch ist können wir $q, r \in R$ wählen, so dass $a = qb' + r$ und $r = 0$ oder $N(r') < N(b')$ gilt. Wir können $b' = be$ für eine Einheit $e \in R$ schreiben und erhalten $a = qeb + r$ mit $r = 0$ oder $N(r) \leqslant N'(r) \leqslant N'(b') = N(b)$ wegen der Minimalität von b', weshalb N eine euklidische Normfunktion ist. Wir zeigen, per Widerspruch, dass die euklidische Normfunktion N die gewünschte Eigenschaft erfüllt. Sei $a \in R$ ein beliebiges von Null verschiedenes Element und sei $b \in R$ ein weiteres von Null verschiedenes Element, für welches $N(ab)$ minimal ist. Angenommen es wäre $N(a) > N(ab)$. Per Definition nimmt N auf assozierten Elementen den selben Wert an, weshalb b keine Einheit sein kann. Da R euklidisch ist existieren $q, r \in R$ so dass $a = q(ab) - r$ und entweder $r = 0$ oder $N(r) < N(ab)$. Da aber b keine Einheit ist folgt mit $a \neq 0$ aus $a(1 - qb) = r$, dass $r \neq 0$ gilt. Dann ist $N(r) = N(a(1 - qb)) < N(ab)$, was der Minimalität von b widerspricht. Also erfüllt N die gewünschte Eigenschaft. □

Bemerkung 11. Sei N eine euklidische Normfunktion wie in Prop 10. Dann folgt aus $a \mid b$, dass $N(a) \leqslant N(b)$.

Die im weiteren Verlauf wichtigste Eigenschaft zeigt das folgende Lemma:

Lemma 12. *Euklidische Ringe sind faktoriell.*

Beweis. Sei R ein euklidischer Ring mit Normfunktion N. Wir zeigen, dass R ein Hauptidealring ist. Sei I ein Ideal in R. Wenn $I = 0$, dann gilt $I = (0)$. Wenn $I \neq 0$, dann wähle ein von nullverschiedenes Element $a \in I$ so dass für alle $b \in I$ gilt $N(a) \leqslant N(b)$. Da R ein euklidischer Ring ist, existieren zu einem beliebigen $b \in I$ $q, r \in R$ so dass $a = qb + r$, wobei $N(r) < N(a)$ gilt. Da aber I ein Ideal ist, also $r = a - qb \in I$, und da a minimal gewählt wurde, folgt $r = 0$. Also gilt $a = bq$ und deshalb $I = (a)$. Die Behauptung folgt nun, da Hauptidealringe faktorielle Ringe sind. □

Ein grundlegender Fakt aus der Algebra ist das folgende Lemma, welches wir ohne Beweis angeben:

Lemma 13. *In einem faktoriellen Ring sind ist jedes irreduzibeles Element ein Primelement.*

Da wir die Einheiten der beiden Ringe $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$ bestimmen möchten, beweisen wir als letztes Lemma in diesem Abschnitt, den folgenden Fakt:

Proposition 14. *Sei R ein nicht-leerer euklidischer Ring. Für eine euklidische Normfunktion welche die Ungleichung (1) erfüllt ist ein Element $e \in R$ eine Einheit dann und nur dann, wenn $N(e) = N(1)$ gilt.*

Beweis. Sei $e \in R$ eine Einheit. Dann existiert ein $a \in R$ so dass $ea = 1$. Sei N eine Normfunktion wie in Proposition 10. Es gilt $e \mid 1$, woraus folgt, dass $N(e) \leqslant N(1)$. Gleichzeitig gilt aber offensichtlich $1 \mid a$ für jedes $a \in R$, weshalb $N(u) = N(1)$ folgt.
Sei nun $e \in R$ so dass $N(e) = N(1)$. Da unser Ring euklidisch ist existieren $q, r \in R$ mit $1 = qe + r$ wobei entweder $r = 0$ oder $N(r) < N(e)$. Angenommen $r \neq 0$, dann folgt mit $N(r) < N(u) = N(1)$ ein Widerspruch, da $N(1)$ wie oben beschrieben immer minimal ist. Also gilt $qe = 1$ und es folgt, dass e eine Einheit ist. □

Die Ringe $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$

In diesem Abschnitt befassen wir uns mit den Eigenschaften von $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$. Wir beginnen damit zu zeigen, dass es sich bei beiden Ringen tatsächlich um euklidische Ringe handelt. Zuerst befassen wir uns mit den Gauss'schen Zahlen.

Proposition 15. *Die Abbildung $N : \mathbb{Z}[i]\backslash\{0\} \to \mathbb{N}$ definiert durch*

$$(a + bi) \mapsto a^2 + b^2$$

ist eine euklidische Normfunktion für $\mathbb{Z}[i]$. Insbesondere macht N $\mathbb{Z}[i]$ zu einem euklidischer Ring.

Bemerkung 16. Die Normfunktion N ist die Restriktion des Quadrats des komplexen Absolutbetrags auf die Teilmenge $\mathbb{Z}[i] \subset \mathbb{C}$. Es gilt also $N(a) = a\bar{a}$.

Bevor wir Proposition 15 beweisen zeigen wir

Lemma 17. *Die Abbildung N aus Proposition 15 ist multiplikativ, das heisst für alle $a, b \in R$ gilt*

$$N(ab) = N(a)N(b).$$

Beweis. Seien $a = a_1 + a_2 i$ und $b = b_1 + b_2 i$ zwei Elemente in $\mathbb{Z}[i]$. Dann gilt

$$\begin{aligned} N(ab) &= (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_1)^2 \\ &= (a_1b_1)^2 - 2a_1b_1a_2b_2 + (a_2b_2)^2 + (a_1b_2)^2 + 2a_1b_1a_2b_2 + (a_2b_1)^2 \\ &= (a_1b_1)^2 + (a_1b_2)^2 + (a_2b_1)^2 + (a_2b_2)^2 \\ &= (a_1^2 + a_2^2)(b_1^2 + b_2^2) \\ &= N(a)N(b) \end{aligned}$$

□

Nun widmen wir uns dem Beweis von Proposition 15.

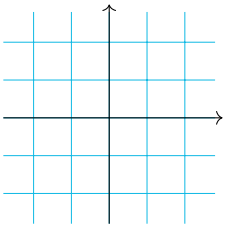

FIGURE 1. Visualisierung von $\mathbb{Z}[i]$ als Gitter in der komplexen Ebene. Die Elemente von $\mathbb{Z}[i]$ entsprechen den Knotenpunkten

Beweis. Es ist offensichtlich, dass die Abbildung N wohldefiniert ist. Seien nun $a, b \in \mathbb{Z}[i]$, wobei $b \neq 0$. Wir müssen nun die Existenz von zwei Gauss'schen Zahlen $q, r \in \mathbb{Z}[i]$ zeigen, die $a = qb + r$ sowie $r = 0$ oder $N(r) < N(b)$ erfüllen. Die Zahl $\frac{a}{b}$ ist eine komplexe Zahl. Geometrisch bilden die Gauss'schen Zahlen ein Gitter in der komplexen Ebene (siehe Fig. 1), dessen Kanten zwischen Knoten immer Länge 1 haben. Da $\frac{a}{b}$ innerhalb einer Masche dieses Gitters liegen muss, hat $\frac{a}{b}$ zum nächsten Gitterpunkt einen Abstand der kleiner gleich $\frac{\sqrt{2}}{2}$ ist. Deshalb existiert ein $q \in \mathbb{Z}[i]$, so dass $|a/b - q| < 1$. Wir setzen nun $r = a - bq \in \mathbb{Z}[i]$ und beobachten, dass

$$N(r) = N(a - bq) = |b(\frac{a}{b} - q)|^2 = |b|^2 |\frac{a}{b} - q|^2 < |b|^2 = N(b),$$

wie gewünscht. Die Behauptung folgt. □

Wir bestimmen nun als nächstes die Einheiten in $\mathbb{Z}[i]$.

Lemma 18. *Die Einheiten in $\mathbb{Z}[i]$ sind die Elemente $\{1, -1, i, -i\}$.*

Beweis. Durch Proposition 14 wissen wir, dass eine Einheit $e \in \mathbb{Z}[i]$ $N(e) = N(1)$ erfüllen muss. Da gilt $N(1) = 1^2 = 1$ folgt, dass die Einheiten genau jene Elemente sind die $N(e) = 1$ erfüllen. Schreiben wir $e = a + bi$ so folgt mit $N(a + bi) = a^2 + b^2$ die Behauptung. □

Bemerkung 19. Wir halten fest, dass eine Einheit in $\mathbb{Z}[i]$ unter N auf 1 abgebildet wird.

Bevor wir mit der Bestimmung der Primelemente beginnen, widmen wir uns zwischenzeitlich dem Ring $\mathbb{Z}[\sqrt{3}]$. Wie für $\mathbb{Z}[i]$ beginnen wir damit zu zeigen, dass es sich bei $\mathbb{Z}[\sqrt{3}]$ ebenfalls um einen euklidischen Ring handelt.

Proposition 20. *Die Abbildung $N_{\sqrt{3}} : \mathbb{Q}[\sqrt{3}]\backslash\{0\} \to \mathbb{Q}_{>0}$ definiert durch*

$$(a + b\sqrt{3}) \mapsto |a^2 - 3b^2|$$

eingeschränkt auf $\mathbb{Z}[\sqrt{3}]$ ist eine euklidische Normfunktion auf $\mathbb{Z}[\sqrt{3}]$.

Der Beweis ist analog zu dem Beweis von Proposition 15, wobei wir dem Beweis aus [2] folgen. Wieder zeigen wir zuerst

Lemma 21. *Die Abbildung $N_{\sqrt{3}}$ ist multiplikativ.*

Beweis. Seien $a = a_1 + a_2\sqrt{3}$ und $b = b_1 + b_2\sqrt{3}$ Elemente von $\mathbb{Q}[\sqrt{3}]$. Dann gilt:

$$\begin{aligned}
N_{\sqrt{3}}(ab) &= N_{\sqrt{3}}((a_1 + a_2\sqrt{3}])(b_1 + b_2\sqrt{3})) \\
&= N_{\sqrt{3}}((a_1b_1 + 3a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{3}) \\
&= |(a_1b_1 + 3a_2b_2)^2 - 3(a_1b_2 + a_2b_1)^2| \\
&= |(a_1b_1)^2 + (3a_2b_2)^2 - 3((a_1b_2)^2 - (a_2b_1)^2)| \\
&= |a_1^2 - 3a_2^2||b_1^2 - 3b_2^2| \\
&= N_{\sqrt{3}}((a_1 + a_2\sqrt{3}]))N_{\sqrt{3}}((b_1 + b_2\sqrt{3})) \\
&= N_{\sqrt{3}}(a)N_{\sqrt{3}}(b)
\end{aligned}$$

□

Nun beweisen wir Proposition 20

Beweis. Die Wohldefiniertheit der Abbildung ist klar. Wir bemerken, dass für rationale $p, q \in \mathbb{Q}$ mit $|p| \leqslant \frac{1}{2}$ und $|q| \leqslant \frac{1}{2}$ gilt

$$|p^2 - 3q^2| \leqslant \frac{3}{4} < 1.$$

Seien nun $x = u + v\sqrt{3}$ sowie $y = u' + v'\sqrt{3}$ für $u, v, u', v' \in \mathbb{Q}$, dann haben $x + y, xy$ und x/y die selbe Form. Seien nun $a, b \in \mathbb{Z}[\sqrt{3}]$ mit $b \neq 0$, dann ist $\frac{a}{b} = u + v\sqrt{3}$ für $u, v \in \mathbb{Q}$. Wir wählen nun ganze Zahlen $m, n \in \mathbb{Z}$ so dass $|u - m| \leqslant \frac{1}{2}$ und $|v - n| \leqslant \frac{1}{2}$. Mit $q = m + n\sqrt{3}$ gilt dann

$$N_{\sqrt{3}}(\frac{a}{b} - q) = |(u - m)^2 - 3(v - n)^2| < 1.$$

Deshalb ist für $r = a - bq \in \mathbb{Z}[\sqrt{3}]$

$$N_{\sqrt{3}}(r) = N_{\sqrt{3}}(a - bq) = N_{\sqrt{3}}(b)N_{\sqrt{3}}(\frac{a}{b} - q) < N_{\sqrt{3}}(b),$$

und die Behauptung folgt. □

Wir können nun auch die Einheiten in $\mathbb{Z}[\sqrt{3}]$ bestimmen.

Bemerkung 22. Es gilt $N_{\sqrt{3}}(1) = 1$. Desweiteren ist $N_{\sqrt{3}}(a) = |a\bar{a}|$.

Es gilt das

Lemma 23. *Die Einheiten in $\mathbb{Z}[\sqrt{3}]$ sind alle Zahlen $a + b\sqrt{3}$, welche $a^2 - 3b^2 = \pm 1$ erfüllen.*

Beweis. Sei $x = a + b\sqrt{3}$ mit $a^2 - 3b^2 = \pm 1$. Dann gilt offensichtlich $N_{\sqrt{3}}(x) = 1$, woraus mit Bemerkung 22 und Proposition 14 folgt, dass x eine Einheit ist. Sei umgekehrt $x = a + b\sqrt{3}$ eine Einheit, dann gilt wieder wegen Bemerkung 22 und Proposition 14 $N_{\sqrt{3}}(x) = 1$ weshalb $a + b\sqrt{3} = \pm 1$ sein muss. Die Behauptung folgt. □

Primelemente in $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$

In diesem Abschnitt bestimmen wir nun die Primelemente in $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$ bis auf Assoziiertheit.

Bemerkung 24. Wenn wir im folgenden von Primzahlen in $\mathbb{Z}$ sprechen, so meinen wir die Primelemente von $\mathbb{Z}$, weshalb auch Zahlen mit negativem Vorzeichen Primzahlen sind.

Um uns zu vergewissern, dass diese Klassifizierung nicht trivial ist, betrachten wir die folgenden zwei Beispiele

Beispiel 25. *In $\mathbb{Z}[i]$ können wir die Primzahl $2 \in \mathbb{Z}$ schreiben als $(1 - i)(1 + i)$. Deshalb ist 2 kein Primelement in $\mathbb{Z}[i]$.*

Ähnlich finden wir auch in $\mathbb{Z}[\sqrt{3}]$, dass nicht alle Primzahlen aus $\mathbb{Z}$ zu Primelementen in $\mathbb{Z}[\sqrt{3}]$ werden.

Beispiel 26. *Wir können die Primzahl 13 in $\mathbb{Z}[\sqrt{3}]$ als $(4 + \sqrt{3})(4 - \sqrt{3})$ zerlegen.*

Bevor wir uns der Klassifizierung der Primelemente widmen, beweisen wir zwei nützliche Hilfslemmas. Wir beginnen mit dem

Lemma 27. *Ist $\pi \in \mathbb{Z}[i]$ (resp. $\mathbb{Z}[\sqrt{3}]$) ein Element mit $N(\pi) = p$ (resp. $N_{\sqrt{3}}(\pi) = p$) für eine Primzahl $p \in \mathbb{Z}$, so ist π ein Primelement in $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[\sqrt{3}]$).*

Beweis. Der Beweis verwendet nur die Multiplikativität der jeweiligen euklidischen Norm, sowie Proposition 14 zusammen mit Bemerkung 19 bzw. Bemerkung 22. Deswegen können wir o.B.d.A. nur den Fall $\mathbb{Z}[i]$ betrachten. Sei π wie in der Annahme. Angenommen $\pi = ab$ für $a, b \in \mathbb{Z}[i]$, so folgt aus der Multiplikativität von N

$$p = N(\pi) = N(ab) = N(a)N(b),$$

weshalb mit p prim folgt, dass entweder $N(a) = 1$ oder $N(b) = 1$ gilt, so dass eines der Elemente eine Einheit sein muss. Es folgt, dass π ein irreduzibeles Element ist. Mit Lemma 13 folgt, dass π ein Primelement ist. □

Desweiteren gilt auch das folgende

Lemma 28. *Ist $\pi \in \mathbb{Z}[i]$ ein Primelement, so folgt $N(\pi) \in \{p, p^2\}$ für eine Primzahl $p \in \mathbb{N}$.*

Beweis. Sei $\pi \in \mathbb{Z}[i]$ ein Primelement. Dann folgt mit $N(\pi) = \pi\bar{\pi}$, dass $\pi \mid N(\pi) \in \mathbb{N}$ teilt. Wir können eine Primzerlegung für $N(\pi)$ finden und schreiben $N(\pi) = p_1 \dots p_n$ für Primzahlen $p_i \in \mathbb{N}$. Da π ein Primelement ist teilt π eine der Primzahlen, sagen wir p_k. Dann gilt $p_k = \pi b$ für ein $b \in \mathbb{Z}[i]$. Mit der Multiplikativität der Normfunktion folgt

$$p^2 = N(p_k) = N(\pi b) = N(\pi)N(b),$$

weshalb $N(\pi) = p$ oder $N(\pi) = p^2$ gelten muss. □

Gleichermassen gilt

Lemma 29. *Ist $\pi \in \mathbb{Z}[\sqrt{3}]$ ein Primelement, so folgt $N_{\sqrt{3}}(\pi) \in \{p, p^2\}$ für eine Primzahl $p \in \mathbb{N}$.*

Der Beweis ist sehr änhlich zu dem Beweis von Lemma 28.

Beweis. Sei $\pi \in \mathbb{Z}[\sqrt{3}]$ ein Primelement. Aus $N_{\sqrt{3}}(\pi) = |\pi\bar{\pi}|$ folgt mit $N_{\sqrt{3}}(\pi) = p_1 \dots p_n$ und dem Wissen, dass π ein Primelement ist, dass $\pi \mid p_k$ für ein p_k aus obigem Produkt. Mit $p_k = \pi b$ folgt mittels Multiplikativität

$$p^2 = N_{\sqrt{3}}(p_k) = N_{\sqrt{3}}(\pi b) = N_{\sqrt{3}}(\pi)N_{\sqrt{3}}(b),$$

weshalb $N_{\sqrt{3}}(\pi) = p$ oder $N_{\sqrt{3}}(a) = p^2$, wie gewünscht. □

Bemerkung 30. Ist π ein Primelement in $\mathbb{Z}[i]$ oder $\mathbb{Z}[\sqrt{3}]$, dann folgt aus den obigen Lemmas für den Fall, dass $N(\pi) = p^2$ bzw. $N_{\sqrt{3}}(\pi) = p^2$ mit Lemma 6, dass π assoziiert zu p ist. Ausserdem gilt, dass $\pi \mid p$.

Abschliessend bestimmen wir nun die Primelemente von $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$ bis auf Assoziiertheit. Wir beginnen mit $\mathbb{Z}[i]$ und beweisen hierfür noch ein weiteres Hilfslemma:

Wir reporduzieren dabei die Argumentation in Neukirchs *Algebraische Zahlentheorie* [1]:

Proposition 31. *Für Primzahlen $p \neq 2$ gilt*

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

Beweis. Angenommen p ist eine ungerade Primzahl der Form $p = a^2 + b^2$ $(a, b \in \mathbb{Z})$. Dann folgt $p \equiv 1 \bmod 4$, da für Quadratzahlen gilt, dass sie

$$a^2 \equiv 1 \bmod 4 \text{ oder } a^2 \equiv 0 \bmod 4$$

erfüllen und weil p ungerade ist. Für die andere Richtung genügt es zu zeigen, dass eine Primzahl mit $p \equiv 1 \bmod 4$ kein Primelement in $\mathbb{Z}[i]$ ist. In diesem Fall gibt es eine Zerlegung $p = ab$ in zwei Nicht-Einheiten $a, b \in \mathbb{Z}[i]$. Mit Lemma 17 können erhalten wir, dass

$$p^2 = N(p) = N(ab) = N(a)N(b)$$

gilt, woraus mit Bemerkung 19 $N(a) = N(b) = p$ folgt. Also gilt dann mit $a = a_1 + a_2 i$, dass $a_1^2 + a_2^2 = p$, wie gewünscht. Um zu sehen, dass eine Primzahl wie in der Annahmen kein Primelement in $\mathbb{Z}[i]$ bleibt verwenden wir, dass nach dem Satz von Wilson für Primzahlen p gilt

$$(p-1)! \equiv_p -1 \bmod p.$$

Sei nun $p = 4k + 1$, so gilt mit

$$\begin{aligned} -1 \equiv_p (p-1)! &= (1 \dots 2k)(p-1 \dots p-2k) \\ &\equiv_p (2k)!((-1)^{2k}2k)! \\ &= ((2k)!)^2, \end{aligned}$$

dass für $x = (2k)!$ gilt $p \mid x^2 + 1 = (x+i)(x-i)$. Es gilt aber offensichtlich $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$, so dass p keinen der Faktoren teilt und deshalb kein Primelement in $\mathbb{Z}[i]$ ist. □

Wir beweisen nun

Theorem 32. *Die Primzahlen in $\mathbb{Z}[i]$ bis auf Assoziiertheit sind:*

- $1 + i$
- $a + bi$ *wobei* $a^2 + b^2 = p \in \mathbb{Z}\backslash\{2\}$ *eine Primzahl* $\equiv 1 \bmod 4$ *ist*

- *p, wobei $p \equiv 3 \bmod 4$ eine Primzahl in $\mathbb{Z}$ ist.*

Auch in diesem Fall folgen wir der Argumentation in [1].

Beweis. Mit Hilfe von Lemma 27 ist es in den ersten zwei Fällen klar, dass es sich bei den Elemente um Primelemente handelt. Sei nun $p \in \mathbb{Z}[i]$ mit $p \equiv 3 \bmod 4$. Wenn p kein Primelement ist, dann ist es wegen Lemma 13 auch nicht irreduzibel und wir können $p = ab$ für Nicht-Einheiten $a, b \in \mathbb{Z}[i]$ schreiben. In diesem Fall folgt mit $p^2 = N(p) = N(a)N(b)$, dass $N(a) = p$ gilt, weshalb mit $a = a_1 + a_2 i$ der Widerspruch $p = a_1^2 + a_2^2 \iff p \cong 1 \bmod 4$ ensteht. Nun bleibt nur zu zeigen, dass alle Primelemente assoziiert zu einem dieser drei Elemente ist. Sei π ein beliebiges Primelement in $\mathbb{Z}[i]$. Wegen Lemma 28 gilt dann $N(\pi) \in \{p, p^2\}$, wobei $p \in \mathbb{N}$ eine Primzahl ist. Angenommen es gilt $N(\pi) = p$. Schreiben wir $\pi = a + bi$, so folgt $a^2 + b^2 = p$. Im Fall $p = 2$ müssen dann sowohl a als auch b Absolutbetrag 1 haben, weshalb nur vier Elemente in Frage kommen. Durch Betrachtung der Einheiten sehen wir sofort, dass alle diese vier Elemente zu $1 + i$ assoziiert sind. Für $p \neq 2$ folgt wegen Proposition 31 in diesem Fall $p \cong 1 \bmod 4$, so dass π einem Primelement aus unserer obigen Liste entspricht. Ist dagegen $N(\pi) = p^2$, so folgt mit Bemerkung 30, dass π assoziiert zu p ist. Desweiteren gilt $p \cong 3 \bmod 4$, da sonst entweder $p = 2$, woraus dann $2 = (1 + i)(1 - i)$ folgt, oder aber es ist $p \cong 1 \bmod 4$ womit dann nach Proposition 31 $a^2 + b^2 = p$ gelten muss und somit $p = (a + bi)(a - bi)$ wäre. In beiden Fällen teilt p kein Element auf der rechten Seite, woraus folgt, dass p kein Primelement ist. Da Assoziierte von Primelementen auch Primelemente sind, impliziert dies, dass auch π kein Primelement ist. Ein Widerspruch zur Annahme. Das Theorem folgt. □

Als letztes Theorem klassifizieren wir nun die Primelemente von $\mathbb{Z}[\sqrt{3}]$ bis auf Assoziiertheit.

Theorem 33. *Die Primzahlen in $\mathbb{Z}[\sqrt{3}]$ sind bis auf Assoziiertheit:*

- $-1 + \sqrt{3}$
- $\sqrt{3}$
- $a + b\sqrt{3}$ *wobei* $a^2 - 3b^2 = \pm p \in \mathbb{Z}\backslash\{2, 3\}$ *eine Primzahl ist sodass* 3 *ein Quadrat in* $\mathbb{Z}/p\mathbb{Z}$ *ist* ($\iff p \cong \pm 1 \bmod 12$)
- *p, wobei p eine Primzahl ist sodass* 3 *kein Quadrat in* $\mathbb{Z}/p\mathbb{Z}$ *ist* ($\iff p \cong \pm 5 \bmod 12$)

Im Beweis von Theorem 33 werden wir das folgende Lemma verwenden.

Lemma 34. *Für eine Primzahl $p \in Z$ gilt $\pm p = a^2 - 3b^2 \implies 3$ ist ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$.*

Beweis. Sei p prim mit $\pm p = a^2 - 3b^2$. Angenommen $b \equiv_p 0 \bmod p$, dann folgt auch $a \equiv_p 0 \bmod p$, was aber wegen $\pm p = a^2 - 3b^2$ nicht eintreten kann. Es ist also $b \not\equiv_p 0 \bmod p$. Dann gilt

$$\begin{aligned} & a^2 - 3b^2 && = \pm p \\ \iff & a^2 - 3b^2 && \equiv_p 0 \\ \iff & a^2 && \equiv_p 3b^2 \\ \iff & a^2(b^{-1})^2 && \equiv_p 3 \\ \iff & (ab^{-1})^2 && \equiv_p 3 \end{aligned}$$

und die Behauptung folgt. □

Bemerkung 35. Allgemein gilt für eine Primzahl p, wenn $a^2 - 3b^2 \equiv_p 0$, dass entweder $a \equiv_p b \equiv_p 0$ oder 3 ist ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$.

Der Beweis ist ähnlich zu dem Beweis von Theorem 32.

Beweis. Mit Hilfe von Lemma 27 ist es auch hier klar, dass es sich bei den ersten drei Elementen der Liste jeweils um Primzahlen handelt. Sei nun $p \in \mathbb{Z}$ ein Primelement, sodass 3 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist. Angenommen p ist kein Primelement in $\mathbb{Z}[\sqrt{(3)}]$, dann können wir für zwei Nicht-Einheiten $a, b \in \mathbb{Z}[\sqrt{3}]$ schreiben $p = ab$. Mit $p^2 = N_{\sqrt{3}}(p) = N_{\sqrt{3}}(ab) = N_{\sqrt{3}}(a)N_{\sqrt{3}}(b)$ folgt dann $N(a) = p$, weshalb nach Lemma 34 3 ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist, ein Widerspruch.

Nachdem wir nun gezeigt haben, dass die vier Elemente prim sind, sei $\pi \in \mathbb{Z}[\sqrt{3}]$ ein beliebiges Primelement. Nach Lemma 29 gilt dann $N_{\sqrt{3}}(\pi) \in \{p, p^2\}$. Im Fall $N_{\sqrt{3}}(\pi) = p$ unterscheiden wir

zwischen den Fällen $p = 2$, $p = 3$, sowie $p \in \mathbb{Z}\backslash\{2, 3\}$. Angenommen $p = 2$. Wir können schreiben $2 = (2 + \sqrt{3})(-1 + \sqrt{3})^2$. Mit Bemerkung 30 folgt $\pi \mid 2$ weshalb $\pi\beta = 2$. Mit der Eindeutigkeit der Primfaktorisierung folgt nun $\pi \sim (-1 + \sqrt{3})$. Ähnlich verfahren wir für $p = 3$. In diesem Fall faktorisieren wir $3 = \sqrt{3}^2$ und argumentieren wie oben. Also $\pi \mid 3$, weshalb aus $\pi\beta = 3 = \sqrt{3}^2$ wegen der Eindeutigkeit der Primzerlegung Assoziiertheit folgt. Sei nun $N(\pi) = p \in \mathbb{Z}\backslash\{2, 3\}$. Dann gilt $a^2 - 3b^2 = \pm p$ und mit Lemma 34 folgt ausserdem, dass 3 ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist. Sei nun $N_{\sqrt{3}}(\pi) = p^2$. Mit Bemerkung 30 folgt direkt dass $\pi \sim p$. Es verbleibt zu zeigen, dass 3 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist. Wir nehmen dafür an, dass $3 \equiv c^2 \bmod p$ gilt und führen dies zu einem Widerspruch. Wir haben $N_{\sqrt{3}}(c + \sqrt{3}) = \pm c^2 - 3 \equiv 0 \bmod p$. Wir können nun o.B.d.A $c \in [-\frac{p-1}{2}, \frac{p-1}{2}]$ wählen. In diesem Fall erhalten wir $p^2 \nmid c^2 - 3$ während aber gleichzeitig per Annahme gilt, dass $p \mid (c+\sqrt{3})(c-\sqrt{3}) = c^2 - 3$. Da p prim ist, gilt $p \mid (c+\sqrt{3})$ oder $p \mid (c-\sqrt{3})$. Deshalb folgt $ggT(p, c + \sqrt{3}) \neq \pm 1$ oder $ggT(p, c - \sqrt{3}) \neq \pm 1$. Sei β einer der ggT ungleich ± 1. Unter Verwendung der Multiplikativität der Normfunktion folgt $N_{\sqrt{3}}(\beta) \mid N_{\sqrt{3}}(p) = p^2$ und $N_{\sqrt{3}}(\beta) \mid c^2 - 3 = (c + \sqrt{3})(c - \sqrt{3})$. Es folgt $N_{\sqrt{3}}(\beta) \in \{p, p^2\}$. Da wir aber bereits wissen, dass $p^2 \nmid c^2 - 3$ muss $N_{\sqrt{3}}(\beta) = p$ gelten. Deshalb ist β nach Lemma 27 ein Primelement und es gilt

$$\pi\bar{\pi} = \pm p^2 = \beta\beta\bar{\beta}\bar{\beta}.$$

Weil β prim ist, ist dies ein Widerspruch zur Eindeutigkeit der Primzerlegung im euklidischen Ring $\mathbb{Z}[\sqrt{3}]$, weshalb 3 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ sein kann.

Das Theorem folgt.

□

Wir haben nun sowohl die Einheiten, als auch die Primelemente bis auf Assoziiertheit in den beiden euklidischen Ringen $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{3}]$ bestimmt.

References

[1] J. Neukirch, *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992

[2] A. Schmidt, *Einführung in die algebraische Zahlentheorie*. Springer, Berlin, 2007

Email address: joerans@student.ethz.ch