Bachelorarbeit Mathematik
Elementare Zahlentheorie im Ring $\mathbb{Z}[i]$

Michael Kniely

SS 2010

Inhaltsverzeichnis

Betreuer: Ass.-Prof. Mag. Dr.rer.nat. Florian Kainrath
Institut für Mathematik und Wissenschaftliches Rechnen
Karl-Franzens-Universität Graz

1 Teilbarkeit im Ring $\mathbb{Z}[i]$

Der Ring $\mathbb{Z}[i]$ ist ein Teilring der komplexen Zahlen $\mathbb{C}$ und enthält genau jene Elemente, deren Real- und Imaginärteil ganzzahlig ist; es gilt

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

Außerdem ist $\mathbb{Z}[i]$ als Teilring des Körpers $\mathbb{C}$ sogar ein Integritätsbereich, in dem jedes $x \in \mathbb{Z}[i]$ eine eindeutige Darstellung $x = a + bi$ mit $a, b \in \mathbb{Z}$ besitzt.

Das Ziel dieser Arbeit ist es, die elementare Zahlentheorie - wie wir sie in $\mathbb{Z}$ kennen - auch für den Ring $\mathbb{Z}[i]$ zu entwickeln. Dabei werden in manchen Bereichen Analogien zu bereits Bekanntem auftreten, an anderen Stellen sich wiederum völlig neue Situationen ergeben.

Bemerkung 1.1. Im Folgenden wird mit $\bar{\cdot}$ stets die komplexe Konjugation bezeichnet, dann ist für $z \in \mathbb{Z}[i]$ auch $\overline{z} \in \mathbb{Z}[i]$. Aus den Eigenschaften der komplexen Konjugation folgt, dass $\bar{\cdot} : \mathbb{Z}[i] \to \mathbb{Z}[i]$ ein Ringhomomorphismus ist, der wegen $\bar{\cdot} \circ \bar{\cdot} = id$ sogar ein Ringisomorphismus ist.

Definition 1.2. Sei $x \in \mathbb{C}$, dann ist $N(x) := x\cdot\overline{x}$.

Bemerkung 1.3. Seien $x, y \in \mathbb{C},\ a, b \in \mathbb{R}$ mit $x = a + bi$, dann ist $N(xy) = xy\overline{xy} = xy\bar{x}\bar{y} = x\bar{x}y\bar{y} = N(x)N(y)$ und $N(x) = |x|^2 = a^2 + b^2$.

Lemma 1.4. *Sei $z \in \mathbb{Z}[i]$, dann gelten*

1. $N(z) \in \mathbb{N}$.
2. $N(z) = 0 \iff z = 0$.
3. $N : \begin{cases} \mathbb{Z}[i]\backslash\{0\} & \to \mathbb{N}^+ \\ x & \mapsto N(x) \end{cases}$ *ist ein Halbgruppenhomomorphismus.*
4. $N(z) = 1 \iff z \in \{1, i, -1, -i\} \iff z \in \mathbb{Z}[i]^\times$.

Beweis: Seien $a, b \in \mathbb{Z}$ mit $z = a + bi$.

1. Wegen $N(z) = a^2 + b^2 \in \mathbb{Z}$ und $a^2 + b^2 \geq 0$ erhält man $N(z) \in \mathbb{N}$.
2. $\underline{\Leftarrow}$: Aus $z = 0$ folgt sofort $N(z) = 0\cdot 0 = 0$.

   $\underline{\Rightarrow}$: Umgekehrt ergeben sich aus $N(z) = a^2 + b^2 = 0$ die Gleichungen $a^2 = 0$ und $b^2 = 0$, was schließlich $a = b = 0$ und damit $z = 0 + 0i = 0$ liefert.
3. Zunächst ist die Abblidung N wegen 2. wohldefiniert; es bleibt noch zu zeigen, dass N ein Homomorphismus zwischen $(\mathbb{Z}[i]\backslash\{0\}, \cdot\,)$ und $(\mathbb{N}^+, \cdot\,)$ ist und die Beziehung $N(1) = 1$ erfüllt ist. Ersteres ist wegen Bemerkung 1.3 klar, Letzteres folgt durch Nachrechnen: $N(1) = N(1+0i) = 1^2 + 0^2 = 1$.
4. Setzt man $N(z) = 1$ voraus, so erhält man $a^2 + b^2 = 1$.

   $\underline{\text{Fall 1: } a^2 = 0}$: Dann ist $b^2 = 1$, womit nur mehr $z \in \{i, -i\} \subseteq \{1, i, -1, -i\}$ möglich ist.

   $\underline{\text{Fall 2: } a^2 \neq 0}$: Dann ist erstens einmal $a^2 > 0$ bzw. $a^2 \geq 1$ und wegen $a^2 \leq a^2 + b^2 = 1$ schließlich $a^2 = 1$; weiters muss dann $b^2 = 0$ und somit $z \in \{1, -1\} \subseteq \{1, i, -1, -i\}$ sein.

   Die Inklusion $\{1, i, -1, -i\} \subseteq \mathbb{Z}[i]^\times$ ist klar, da $1 \cdot 1 = 1$, $i(-i) = 1$, und $(-1)(-1) = 1$ ist.

   Gelte nun $z \in \mathbb{Z}[i]^\times$; dann gibt es ein $z' \in \mathbb{Z}[i]^\times$ mit $z\cdot z' = 1$, woraus nun $N(z)N(z') = N(zz') = N(1) = 1$ folgt; damit ist $N(z)$ eine Einheit in $\mathbb{N}$ und daher gilt $N(z) = 1$. □

Korollar 1.5. $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Beweis: Unmittelbar klar nach Punkt *4.* aus Lemma 1.4. □

Proposition 1.6. *Seien $x, y \in \mathbb{Z}[i],\ y \neq 0$, dann gibt es $q, r \in \mathbb{Z}[i]$ mit $x = q\cdot y + r$, wobei $N(r) < N(y)$ ist.*

Beweis: Seien $x, y \in \mathbb{Z}[i],\ y \neq 0$. Damit ist einmal $N(y) > 0$; betrachte nun die folgende komplexe Division:

$$\frac{x}{y} = \frac{x\overline{y}}{y\overline{y}} = \frac{x\overline{y}}{N(y)} = s + ti$$

mit $s, t \in \mathbb{Q}$; wähle nun $m, n \in \mathbb{Z}$ mit der Eigenschaft $|s-m| \leq \frac{1}{2}$ bzw. $|t-n| \leq \frac{1}{2}$ und setze $q := m+ni$; dann gilt

$$N(\frac{x}{y} - q) = N((s-m) + (t-n)i) = (s-m)^2 + (t-n)^2 \leq \frac{1}{4} + \frac{1}{4} < 1.$$

Setzt man nun $r = x - qy$, so ist $N(r) = N(x-qy) = N(y(\frac{x}{y} - q)) = N(y)N(\frac{x}{y} - u) < N(y)$; somit gilt $x = qy + r$ mit $q, r \in \mathbb{Z}[i]$ und $N(r) < N(y)$. □

Proposition 1.7. *Sei I ein Ideal von $\mathbb{Z}[i]$, dann gibt es ein $x \in \mathbb{Z}[i]$ mit $I = \mathbb{Z}[i]x$.*

Beweis: Sei I ein Ideal von $\mathbb{Z}[i]$.

Fall 1: $I = 0$: Dann ist $I = \mathbb{Z}[i]0 = \mathbb{Z}[i]x$ mit $x = 0$.

Fall 2: $I \neq 0$: In diesem Fall ist $I\backslash\{0\}$ nicht leer und somit $M := \{N(u) \mid u \in I\backslash\{0\}\}$ eine nichtleere Teilmenge der natürlichen Zahlen, welche ein Minimum besitzt; sei $v \in I\backslash\{0\}$ mit $N(v) = \min(M)$. Nun wird behauptet, dass $I = \mathbb{Z}[i]v$ ist. Da $\mathbb{Z}[i]v \subseteq I$ klar ist wegen $v \in I$, bleibt noch $I \subseteq \mathbb{Z}[i]v$ zu zeigen. Sei dazu $u \in I$; dann ist $u = vq + r$ mit passenden $q, r \in \mathbb{Z}[i]$ und $N(r) < N(v)$. Es gilt $r = u - vq \in I$ wegen $u, v \in I$ und $q \in \mathbb{Z}[i]$; da aber $N(v) = \min(M)$ kann wegen $N(r) < N(v)$ nicht $r \neq 0$ gelten und daher muss $r = 0$ sein, woraus $u = qv \in \mathbb{Z}[i]v$ folgt. □

Definition 1.8. Seien $x, y \in \mathbb{Z}[i]$.

- y heißt ein **Teiler** von $x :\Longleftrightarrow\ (\exists\ z \in \mathbb{Z}[i])\ x = y \cdot z$.
- x heißt **assoziiert** zu $y :\Longleftrightarrow\ (\exists\ \epsilon \in \mathbb{Z}[i]^\times)\ x = \epsilon \cdot y$.

Schreibweise: Ist y ein Teiler von x, so nennt man x ein Vielfaches von y bzw. teilbar durch y.

- Ist y ein Teiler von x, so schreibt man $y \mid x$, andernfalls $y \nmid x$.
- Ist x assoziiert zu y, so schreibt man $x \sim y$, andernfalls $x \nsim y$.

Lemma 1.9. *Seien $x, y \in \mathbb{Z}[i]$ und $\sim$ die Assoziiertheit von Elementen in $\mathbb{Z}[i]$, dann gelten*

1. *$\sim$ definiert eine Äquivalenzrelation auf $\mathbb{Z}[i]$.*
2. *$x \sim y \iff [x \mid y\ \wedge\ y \mid x]$.*

Beweis: 1. Es ist zu zeigen, dass $\sim$ reflexiv, symmetrisch und transitiv ist. Seien dazu $x, y, z \in \mathbb{Z}[i]$, dann erhält man mittels Einsetzen der Definition: $x \sim x$, da $x = 1 \cdot x$ und $1 \in \mathbb{Z}[i]^\times$; $x \sim y \Rightarrow x = \epsilon y$ mit $\epsilon \in \mathbb{Z}[i]^\times \Rightarrow y = \epsilon^{-1}x \Rightarrow y \sim x$, da $\epsilon^{-1} \in \mathbb{Z}[i]^\times$; $[x \sim y\ \wedge\ y \sim z] \Rightarrow [x = \delta y\ \wedge\ y = \epsilon z$ mit $\delta, \epsilon \in \mathbb{Z}[i]^\times] \Rightarrow x = \delta\epsilon z \Rightarrow x \sim z$, da $\delta\epsilon \in \mathbb{Z}[i]^\times$.

2. $\Rightarrow$: Per Definition gilt $x = \epsilon y$ mit $\epsilon \in \mathbb{Z}[i]^\times$, woraus man sofort $y \mid x$ und $x \mid y$ erhält.

   $\Leftarrow$: Gelte nun $x \mid y$ und $y \mid x$; dann ist $y = xu$ und $x = vy$, insgesamt also $x \cdot (1 - uv) = 0$.

   Fall 1: $x = 0$: Dann ist $y = 0u = 0$ und damit $x = 0 \sim 0 = y$.

   Fall 2: $x \neq 0$: In diesem Fall muss $(1 - uv) = 0$ und damit $uv = 1$ gelten, womit $u \in \mathbb{Z}[i]^\times$ und schließlich $x \sim y$ ist. □

Sprechweise: „x und y sind assoziiert“ statt „x ist zu y assoziiert“. Diese Konvention ist sinnvoll, da die Assoziiertheit als Äquivalenzrelation auf $\mathbb{Z}[i]$ insbesondere symmetrisch ist.

Definition 1.10. Seien $x, y \in \mathbb{Z}[i]$.

- y heißt ein **echter Teiler** von $x :\Longleftrightarrow\ [y \mid x\ \wedge\ y \notin \mathbb{Z}[i]^\times\ \wedge\ y \nsim x]$.

Lemma 1.11. *Seien $x, y \in \mathbb{Z}[i]$, dann gelten*

1. *y ist ein Teiler von x* $\iff \mathbb{Z}[i]x \subseteq \mathbb{Z}[i]y$.

2. $x \sim y \iff \mathbb{Z}[i]x = \mathbb{Z}[i]y$.

3. *y ist ein echter Teiler von x* $\iff \mathbb{Z}[i]x \subsetneq \mathbb{Z}[i]y \subsetneq \mathbb{Z}[i]$.

Beweis: 1. $\underline{\Rightarrow:}$ $y \mid x \Rightarrow (\exists\, z \in \mathbb{Z}[i])\ x = yz \Rightarrow \mathbb{Z}[i]x = \mathbb{Z}[i]zy \subseteq \mathbb{Z}[i]y$.
$\underline{\Leftarrow:}$ $x = 1x \in \mathbb{Z}[i]x \subseteq \mathbb{Z}[i]y \Rightarrow (\exists\, z \in \mathbb{Z}[i])\ x = zy \Rightarrow y \mid x$.

2. $x \sim y \Leftrightarrow [x \mid y \wedge y \mid x] \Leftrightarrow [\mathbb{Z}[i]y \subseteq \mathbb{Z}[i]x \wedge \mathbb{Z}[i]x \subseteq \mathbb{Z}[i]y] \Leftrightarrow \mathbb{Z}[i]x = \mathbb{Z}[i]y$.

3. Per Definition ist y genau dann ein echter Teiler von x, wenn $[y \mid x \wedge y \notin \mathbb{Z}[i]^\times \wedge y \not\sim x]$.
$\underline{\Rightarrow:}$ $[[y \mid x \wedge y \not\sim x] \Rightarrow \mathbb{Z}[i]x \subsetneq \mathbb{Z}[i]y]$ und $[y \notin \mathbb{Z}[i]^\times \Rightarrow 1 \notin \mathbb{Z}[i]y \Rightarrow \mathbb{Z}[i]y \subsetneq \mathbb{Z}[i]]$.
$\underline{\Leftarrow:}$ $[\mathbb{Z}[i]x \subsetneq \mathbb{Z}[i]y \Rightarrow [y \mid x \wedge y \not\sim x]]$ und $[\mathbb{Z}[i]y \subsetneq \mathbb{Z}[i] \Rightarrow 1 \notin \mathbb{Z}[i]y \Rightarrow y \notin \mathbb{Z}[i]^\times]$. □

Definition 1.12. Sei $x \in \mathbb{Z}[i],\ x \neq 0,\ x \notin \mathbb{Z}[i]^\times$.

- x heißt **Primelement** bzw. **prim** $:\iff (\forall\, y \in \mathbb{Z}[i])\ y \mid x \Rightarrow [y \in \mathbb{Z}[i]^\times \vee y \sim x]$.

Lemma 1.13. *Sei $x \in \mathbb{Z}[i],\ x \neq 0,\ x \notin \mathbb{Z}[i]^\times$, dann gilt:*

x ist prim $\iff$ *x hat keine echten Teiler* $\iff (\forall\, y, z \in \mathbb{Z}[i])\ x = yz \Rightarrow [y \in \mathbb{Z}[i]^\times \vee z \in \mathbb{Z}[i]^\times]$.

Beweis: Sei x zunächst prim und $y \in \mathbb{Z}[i]$ ein Teiler von x, dann folgt sofort $y \in \mathbb{Z}[i]^\times$ oder $y \sim x$, also ist y kein echter Teiler von x.

Besitze nun x keine echten Teiler und seien $y, z \in \mathbb{Z}[i]$ mit $x = yz$, dann ist y ein Teiler von x, für den nach Voraussetzung $y \in \mathbb{Z}[i]^\times$ oder $y \sim x$ gilt. Im Falle von $y \sim x$ ist $y \neq 0$ und es gilt $yz = x = \epsilon y$ mit $\epsilon \in \mathbb{Z}[i]^\times$; nach Kürzen von y erhält man damit $z = \epsilon \in \mathbb{Z}[i]^\times$.

Gelte schließlich die letztgenannte Aussage in der obigen Äquivalenzkette und sei $y \in \mathbb{Z}[i]$ mit $y \mid x$, dann gibt es ein $z \in \mathbb{Z}[i]$ mit $x = yz$. Laut Voraussetzung ist nun $y \in \mathbb{Z}[i]^\times$ oder $z \in \mathbb{Z}[i]^\times$; da $z \in \mathbb{Z}[i]^\times$ aber $x \sim y$ impliziert, ist x somit prim. □

Satz 1.14. *Sei $x \in \mathbb{Z}[i]$, dann gilt:* *x ist prim* $\iff (\forall\, y, z \in \mathbb{Z}[i])\ x \mid yz \Rightarrow [x \mid y \vee x \mid z]$.

Beweis: $\underline{\Rightarrow:}$ Seien $x \in \mathbb{Z}[i]$ prim und $y, z \in \mathbb{Z}[i]$ mit $x \mid yz$; es ist zu zeigen, dass y oder z ein Vielfaches von x ist. Setze dazu $I := \mathbb{Z}[i]x + \mathbb{Z}[i]y$; dann ist I ein Ideal in $\mathbb{Z}[i]$ und nach Proposition 1.7 gibt es ein $w \in \mathbb{Z}[i]$ mit $I = \mathbb{Z}[i]w$; außerdem muss $w \neq 0$ sein, da $w = 0 \Rightarrow I = 0 \Rightarrow I \ni x = 0$, was einen Widerspruch darstellt, da x ein Primelement ist. Weiters ist $\mathbb{Z}[i]x \subseteq I = \mathbb{Z}[i]w$ und damit nach Lemma 1.11 w ein Teiler von x; da x jedoch prim ist, muss $w \in \mathbb{Z}[i]^\times$ oder $w \sim x$ gelten.

Fall 1: $w \in \mathbb{Z}[i]^\times$: In diesem Fall ist $1 = ww'$ mit passendem $w' \in \mathbb{Z}[i]^\times$ und folglich $w \sim 1$. Man erhält: $I = \mathbb{Z}[i]w = \mathbb{Z}[i]\cdot 1 = \mathbb{Z}[i] \Rightarrow \mathbb{Z}[i] = \mathbb{Z}[i]x + \mathbb{Z}[i]y$; daher gibt es $u, v \in \mathbb{Z}[i]$ mit $1 = ux + vy$. Damit ist nun auch $z = uxz + vyz = x(uz) + x(vx')$ mit $yz = xx'$ und $x' \in \mathbb{Z}[i]$; aus der letzten Beziehung ergibt sich sofort $x \mid z$.

Fall 2: $w \sim x$: Aus Lemma 1.11 folgt zunächst $\mathbb{Z}[i]w = \mathbb{Z}[i]x$; da weiters $\mathbb{Z}[i]y \subseteq I = \mathbb{Z}[i]w = \mathbb{Z}[i]x$ gilt, ist x somit ein Teiler von y.

Daraus folgt, dass x in jedem Fall y oder z teilt.

$\underline{\Leftarrow:}$ Seien nun $x \in \mathbb{Z}[i]$ und $y \in \mathbb{Z}[i]$ ein beliebiger Teiler von x; dann existiert ein $z \in \mathbb{Z}[i]$ mit $x = yz$. Nach Voraussetzung teilt x nun y oder z.

Fall 1: $x \mid y$: Dann gilt: $[y \mid x \wedge x \mid y] \Rightarrow y \sim x$.

Fall 2: $x \mid z$: Nun erhält man: $[z \mid x \wedge x \mid z] \Rightarrow z \sim x \Rightarrow x = \epsilon z$ mit $\epsilon \in \mathbb{Z}[i]$. Damit folgt: $yz = x = \epsilon z \Rightarrow (y - \epsilon)z = 0 \Rightarrow [y = \epsilon \vee z = 0]$; da aus $z = 0$ sofort $x = 0$ folgen würde, bleibt nur die Möglichkeit $y = \epsilon \in \mathbb{Z}[i]^\times$ übrig.

Somit ist $y \sim x$ oder $y \in \mathbb{Z}[i]^\times$ und x somit prim. □

Satz 1.15. *Sei $x \in \mathbb{Z}[i],\ x \neq 0,\ x \notin \mathbb{Z}[i]^\times$, dann lässt sich x darstellen in der Form*

$$x = \prod_{\nu=1}^{n} p_\nu$$

mit Primelementen $p_1, ..., p_n \in \mathbb{Z}[i]$ und $n \in \mathbb{N}^+$; diese Darstellung ist bis auf Reihenfolge der Faktoren und Assoziiertheit eindeutig.

Beweis: Existenz: Sei $x \in \mathbb{Z}[i],\ x \neq 0,\ x \notin \mathbb{Z}[i]^\times$, dann zeigt man die Existenz einer solchen Darstellung mithilfe eines Induktionsbeweises nach $N(x)$. Wegen $x \neq 0$ und $x \notin \mathbb{Z}[i]^\times$ ist $N(x) \geq 2$. Gebe es nun für alle $x' \in \mathbb{Z}[i]\backslash(\{0\} \cup \mathbb{Z}[i]^\times)$ mit $N(x') < N(x)$ eine Darstellung als Produkt von primen Elementen in der behaupteten Form, dann ist zu zeigen, dass auch x ein Produkt primer Elemente ist. Im Falle, dass x prim ist, ist x ein triviales Produkt über das Primelement x selbst. Falls x nicht prim ist, gibt es $y, z \in \mathbb{Z}[i]\backslash(\{0\} \cup \mathbb{Z}[i]^\times)$ mit $x = yz$; da y und z nicht Null und keine Einheiten sind, erhält man $N(y) > 1$ sowie $N(z) > 1$ und damit aus $N(x) = N(y)N(z)$ die Beziehungen $N(y) < N(x)$ sowie $N(z) < N(x)$. Nach Induktionsvoraussetzung sind nun

$$y = \prod_{\mu_1=1}^{m_1} p_{\mu_1} \quad \text{und} \quad z = \prod_{\mu_2=1}^{m_2} q_{\mu_2}$$

Produkte von primen Elementen $p_1, ..., p_{m_1}, q_1, ..., q_{m_2}$; also ist auch $x = yz = p_1 \cdot ... \cdot p_{m_1} \cdot q_1 \cdot ... \cdot q_{m_2}$ ein Produkt primer Elemente.

Eindeutigkeit: Seien nun $m, n \in \mathbb{N}^+$ und $p_1, ..., p_m, q_1, ..., q_n \in \mathbb{Z}[i]$ Primelemente mit

$$x = \prod_{\mu=1}^{m} p_\mu = \prod_{\nu=1}^{n} p_\nu.$$

Es ist zu zeigen, dass $m = n$ ist und es ein $\sigma : \{1, ..., m\} \to \{1, ..., n\}$ bijektiv gibt, sodass für alle $i \in \{1, ..., n\}$ die Beziehung $p_i \sim q_{\sigma(i)}$ gilt. Dazu führt man einen Induktionsbeweis nach m.

$m = 1$: Dann ist $p_1 = x = q_1 \cdot ... \cdot q_n$, womit $p_1 \mid q_{\nu_0}$ für ein $\nu_0 \in \{1, ..., n\}$ gilt, da p_1 prim ist; damit ist aber sogar $p_1 \sim q_{\nu_0}$, da q_{ν_0} als Primelement keine echten Teiler hat. Nach eventuellem Umnummerieren erhält man $p_1 \sim q_n$ bzw. $q_n = \epsilon p_1$ mit $\epsilon \in \mathbb{Z}[i]^\times$ und nach Kürzen von p_1 schließlich $1 = \epsilon q_1 \cdot ... \cdot q_{n-1}$, was für $n \geq 2$ einen Widerspruch darstellt, da kein q_ν eine Einheit ist. Somit ist $m = n = 1$ und $p_1 = q_1$.

$m > 1$: Sei nun die Aussage für $m - 1$ bereits bewiesen; dann gilt $p_m \mid q_{\nu_0}$ für ein $\nu_0 \in \{1, ..., n\}$, da p_m prim ist, und damit auch $p_m \sim q_{\nu_0}$ analog zum Fall $m = 1$. Eventuelles Umnummerieren liefert $p_m \sim q_n$ bzw. $q_n = \epsilon p_m$ mit $\epsilon \in \mathbb{Z}[i]^\times$ und Kürzen von p_m schließlich $p_1 \cdot ... \cdot p_{m-1} = \epsilon q_1 \cdot ... \cdot q_{n-1}$. Darauf die Induktionsannahme angewandt ergibt $m - 1 = n - 1$ sowie $p_i \sim q_i$ für alle $i \in \{1, ..., n - 1\}$, woraus mit $p_m \sim q_n$ die Behauptung folgt. □

2 Größter gemeinsamer Teiler

Definition 2.1. Seien $A \subseteq \mathbb{Z}[i],\ d \in \mathbb{Z}[i]$.

- d heißt ein **größter gemeinsamer Teiler** von $A :\iff d$ erfüllt die folgenden beiden Bedingungen:
  1. $(\forall\ a \in A)\ d \mid a$.
  2. $(\forall\ d' \in \mathbb{Z}[i])\ [(\forall\ a \in A)\ d' \mid a] \implies d' \mid d$.
- $\mathrm{GGT}(A) := \{d \in \mathbb{Z}[i] \mid d \text{ ist ein größter gemeinsamer Teiler von } A\}$.

Proposition 2.2. *Seien $A \subseteq \mathbb{Z}[i],\ d \in \mathbb{Z}[i]$, dann gilt:*

$$d \in \mathrm{GGT}(A) \iff \sum_{a \in A} \mathbb{Z}[i]a = \mathbb{Z}[i]d.$$

Beweis: Seien also $A \subseteq \mathbb{Z}[i]$ und $d \in \mathbb{Z}[i]$.

$\underline{\Rightarrow}$: Sei einmal $d \in \mathrm{GGT}(A)$; wählt man $a' \in A$ beliebig, dann gilt laut Definition des größten gemeinsamen Teilers $d \mid a'$ und somit auch $\mathbb{Z}[i]a' \subseteq \mathbb{Z}[i]d$, womit man schließlich

$$\bigcup_{a \in A} \mathbb{Z}[i]a \subseteq \mathbb{Z}[i]d$$

und damit

$$\sum_{a \in A} \mathbb{Z}[i]a = \langle \bigcup_{a \in A} \mathbb{Z}[i]a \rangle \subseteq \mathbb{Z}[i]d$$

erhält. Andererseits gibt es wegen Proposition 1.7 ein $d' \in \mathbb{Z}[i]$, sodass $\sum_{a \in A} \mathbb{Z}[i]a = \mathbb{Z}[i]d'$, da $\sum_{a \in A} \mathbb{Z}[i]a$ ein Ideal von $\mathbb{Z}[i]$ ist. Daraus ergibt sich $\mathbb{Z}[i]a' \subseteq \sum_{a \in A} \mathbb{Z}[i]a = \mathbb{Z}[i]d'$ bzw. $d' \mid a'$ für alle $a' \in A$; da d aber ein größter gemeinsamer Teiler von A ist, muss daher auch $d' \mid d$ gelten, woraus schließlich

$$\mathbb{Z}[i]d \subseteq \mathbb{Z}[i]d' = \sum_{a \in A} \mathbb{Z}[i]a$$

folgt.

$\underline{\Leftarrow}$: Gelte nun $\sum_{a \in A} \mathbb{Z}[i]a = \mathbb{Z}[i]d$, dann erhält man zunächst für beliebiges $a' \in A$ die Inklusion

$$\mathbb{Z}[i]a' \subseteq \sum_{a \in A} \mathbb{Z}[i]a = \mathbb{Z}[i]d,$$

woraus $d \mid a'$ für alle $a' \in A$ folgt. Wählt man nun ein $d' \in \mathbb{Z}[i]$, das ebenfalls jedes $a' \in A$ teilt, dann ist $\mathbb{Z}[i]a' \subseteq \mathbb{Z}[i]d'$ für alle $a' \in A$ und somit gilt auch

$$\mathbb{Z}[i]d = \sum_{a \in A} \mathbb{Z}[i]a = \langle \bigcup_{a \in A} \mathbb{Z}[i]a \rangle \subseteq \mathbb{Z}[i]d'$$

bzw. $d' \mid d$, womit gezeigt ist, dass $d \in \mathrm{GGT}(A)$ ist. □

Korollar 2.3. *Sei $A \subseteq \mathbb{Z}[i]$, dann gelten*

1. $(\forall\ d_1, d_2 \in \mathrm{GGT}(A))\ d_1 \sim d_2$.
2. *A besitzt einen größten gemeinsamen Teiler d und* $\mathrm{GGT}(A) = \mathbb{Z}[i]^\times d = \{d, i \cdot d, -d, -i \cdot d\}$.

Beweis: 1. Seien $d_1, d_2 \in \mathrm{GGT}(A)$, dann ist

$$\mathbb{Z}[i]d_1 = \sum_{a \in A} \mathbb{Z}[i]a = \mathbb{Z}[i]d_2,$$

woraus sich mittels Lemma 1.11 schließlich $d_1 \sim d_2$ ergibt.

2. Da $\sum_{a\in A}\mathbb{Z}[i]a$ ein Ideal ist, gibt es ein $d\in\mathbb{Z}[i]$ mit $\sum_{a\in A}\mathbb{Z}[i]a=\mathbb{Z}[i]d$; damit erhält man aus Proposition 2.2, dass d ein größter gemeinsamer Teiler ist. Zusätzlich ergibt sich

$$\begin{aligned}\mathrm{GGT}(A) &= \{d'\in\mathbb{Z}[i] \mid \sum_{a\in A}\mathbb{Z}[i]a=\mathbb{Z}[i]d'\}=\{d'\in\mathbb{Z}[i] \mid \mathbb{Z}[i]d=\mathbb{Z}[i]d'\}=\\ &= \{d'\in\mathbb{Z}[i] \mid d'\sim d\}=\{\epsilon d \mid \epsilon\in\mathbb{Z}[i]^\times\}=\mathbb{Z}[i]^\times d=\{d,i\cdot d,-d,-i\cdot d\}\end{aligned}$$

unter Verwendung der vorherigen Resultate. □

Korollar 2.4. *Seien $A\subseteq\mathbb{Z}[i]$, $d\in\mathbb{Z}[i]$, dann gelten*

1.

$$d\in\mathrm{GGT}(A)\implies d=\sum_{a\in A}r_a\cdot a \text{ mit } r_a\in\mathbb{Z}[i] \text{ für alle } a\in A \text{ und } r_a=0 \text{ für fast alle } a\in A.$$

2.

$$\mathrm{GGT}(A)=\mathbb{Z}[i]^\times\iff 1\in\sum_{a\in A}\mathbb{Z}[i]a.$$

Beweis: 1. Sei $d\in\mathrm{GGT}(A)$, dann folgt $d=1d\in\mathbb{Z}[i]d=\sum_{a\in A}\mathbb{Z}[i]a$ laut Proposition 2.2; daher lässt sich d in der behaupteten Form schreiben.

2. $\underline{\Rightarrow:}$ Ist $\mathrm{GGT}(A)=\mathbb{Z}[i]^\times$, so erhält man $\sum_{a\in A}\mathbb{Z}[i]a=\mathbb{Z}[i]$ aus Proposition 2.2, woraus sich unmittelbar $1\in\sum_{a\in A}\mathbb{Z}[i]a$ ergibt.

$\underline{\Leftarrow:}$ Im Falle von $1\in\sum_{a\in A}\mathbb{Z}[i]a$ ist $\sum_{a\in A}\mathbb{Z}[i]a=\mathbb{Z}[i]$; somit ist $1\in\mathrm{GGT}(A)$ und damit $\mathrm{GGT}(A)=\mathbb{Z}[i]^\times$ nach dem vorigen Korollar. □

Satz 2.5. *Seien $m,n\in\mathbb{N}^+$, $a,b,c,a_1,...,a_m,b_1,...,b_n\in\mathbb{Z}[i]$, dann gelten*

1. Sei $d\in\mathrm{GGT}(a,c)$, dann gilt: $c\mid ab\iff c\mid db$.

2. $[c\mid ab\ \wedge\ \mathrm{GGT}(a,c)=\mathbb{Z}[i]^\times]\implies c\mid b$.

3.

$$[(\forall\ k\in\{1,...,m\},l\in\{1,...,n\})\ \mathrm{GGT}(a_k,b_l)=\mathbb{Z}[i]^\times]\implies \mathrm{GGT}(\prod_{k=1}^m a_k,\prod_{l=1}^n b_l)=\mathbb{Z}[i]^\times.$$

Beweis: 1. $\underline{\Rightarrow:}$ Seien $x,y\in\mathbb{Z}[i]$ nach Korollar 2.4 so gewählt, dass $d=xa+yc$; aus $c\mid ab$ folgt dann $ab=cz$ mit passendem $z\in\mathbb{Z}[i]$, somit ist $db=(ax+cy)b=abx+bcy=cxz+bcy$, woraus sich $c\mid db$ ergibt.

$\underline{\Leftarrow:}$ Umgekehrt erhält man aus $d\mid a\ \Rightarrow\ db\mid ad$ und $c\mid db$ die Beziehung $c\mid ab$.

2. Klar nach 1. mit $d=1\in\mathrm{GGT}(a,c)$.

3. Man führt einen Widerspruchsbeweis, bei dem man annimmt, dass die Voraussetzung auf der linken Seite wahr ist, aber $\mathrm{GGT}(\prod_{k=1}^m a_k,\prod_{l=1}^n b_l)\neq\mathbb{Z}[i]^\times$ ist. Sei $d\in\mathrm{GGT}(\prod_{k=1}^m a_k,\prod_{l=1}^n b_l)$, dann kann nicht $d=0$ gelten, da sonst $\prod_{k=1}^m a_k=\prod_{l=1}^n b_l=0$ und damit $a_{k_0}=b_{l_0}=0$ für bestimmte $k_0\in\{1,...,m\}$ und $l_0\in\{1,...,n\}$ folgen würde. Dies ist aber nicht möglich, weil dann $0\in\mathrm{GGT}(a_{k_0},b_{l_0})=\mathbb{Z}[i]^\times$ wäre - ein Widerspruch. Somit ist $d\notin\{0\}\cup\mathbb{Z}[i]^\times$ und es existiert ein Primelement $p\in\mathbb{Z}[i]$ mit $p\mid d$. Wegen $d\mid\prod_{k=1}^m a_k$ und $d\mid\prod_{l=1}^n b_l$ gilt insbesondere $p\mid\prod_{k=1}^m a_k$ und $p\mid\prod_{l=1}^n b_l$, und da p prim ist sogar $p\mid a_{k_0}$ und $p\mid b_{l_0}$ für bestimmte $k_0\in\{1,...,m\}$ und $l_0\in\{1,...,n\}$. Daraus erhält man nun für ein $d_0\in\mathrm{GGT}(a_{k_0},b_{l_0})=\mathbb{Z}[i]^\times$ die Beziehung $p\mid d_0$ und damit $p\in\mathbb{Z}[i]^\times$ - ein Widerspruch. □

3 Prime Elemente

Notation: Im weiteren Verlauf wird mit $\mathbb{P}$ stets die Menge der Primzahlen in $\mathbb{N}$ bezeichnet.

Lemma 3.1. *Seien $a, b \in \mathbb{Z}$, $x \in \mathbb{Z}[i]$, $\epsilon \in \mathbb{Z}[i]^\times$, dann gelten*

1. *a teilt b in $\mathbb{Z}[i]$ $\iff$ a teilt b in $\mathbb{Z}$.*
2. *a teilt x in $\mathbb{Z}[i]$ $\iff$ a teilt $\overline{x}$ in $\mathbb{Z}[i]$.*
3. *x ist prim in $\mathbb{Z}[i]$ $\iff$ $\overline{x}$ ist prim in $\mathbb{Z}[i]$.*
4. *x ist prim in $\mathbb{Z}[i]$ $\iff$ ϵx ist prim in $\mathbb{Z}[i]$.*

Beweis: Die einzelnen Behauptungen erhält man durch Nachrechnen sowie aus bereits Bekanntem.

1. $\underline{\Leftarrow:}$ $b = qa$ mit $q \in \mathbb{Z} \Rightarrow b = qa$ mit $q \in \mathbb{Z}[i]$.
   $\underline{\Rightarrow:}$ Aus $b = qa = a \cdot q_x + a \cdot q_y \cdot i \in \mathbb{Z}$ mit $q = q_x + q_y \cdot i \in \mathbb{Z}[i]$ und $q_x, q_y \in \mathbb{Z}$ ergibt sich $a \cdot q_y = 0$ und damit $b = a \cdot q_x$. Also wird b von a in $\mathbb{Z}$ geteilt.
2. $\underline{\Rightarrow:}$ Man erhält aus $x = qa$ mit $q \in \mathbb{Z}[i]$ sofort $\overline{x} = \overline{q} \cdot \overline{a} = \overline{q} \cdot a$, womit a auch $\overline{x}$ in $\mathbb{Z}[i]$ teilt.
   $\underline{\Leftarrow:}$ Setzt man a teilt $\overline{x}$ in $\mathbb{Z}[i]$ voraus, so folgt aus der Überlegung zuvor, dass a auch $\overline{\overline{x}}$ und damit x in $\mathbb{Z}[i]$ teilt.
3. Laut Bemerkung 1.1 ist die komplexe Konjugation $\bar{\cdot} : \mathbb{Z}[i] \to \mathbb{Z}[i]$ ein Ringisomorphismus; somit folgt die Behauptung unmittelbar aus dem Isomorphieprinzip.
4. Es reicht Folgendes zu zeigen: x ist prim $\Rightarrow \epsilon x$ ist prim. Sei also x prim und gelte $\epsilon x \mid yz$ mit $y, z \in \mathbb{Z}[i]$, dann folgt aus $x \mid (\epsilon^{-}1y)z$ laut Voraussetzung $x \mid (\epsilon^{-}1y)$ oder $x \mid z$ und damit schließlich $\epsilon x \mid y$ oder $\epsilon x \mid z$. □

Proposition 3.2. *Sei $x \in \mathbb{Z}[i]$, dann gilt: $N(x) \in \mathbb{P} \implies x$ ist ein Primelement.*

Beweis: Sei $x \in \mathbb{Z}[i]$; angenommen $N(x) \in \mathbb{P}$ und x ist kein Primelement, also $x = q_1 q_2$, wobei $q_1, q_2 \in \mathbb{Z}[i]$ echte Teiler von x sind; dann ist $N(q_i) > 1$ für $i \in \{1, 2\}$, da wegen $N(x) \in \mathbb{P}$ auch $x \neq 0$ und damit $q_1, q_2 \neq 0$ sind. Somit erhält man die Beziehung $N(x) = N(q_1)N(q_2)$, die nach den vorigen Überlegungen besagt, dass $N(x)$ nicht prim ist - ein Widerspruch; also muss x ein Primelement sein. □

Satz 3.3. *Für jedes Primelement $x \in \mathbb{Z}[i]$ gibt es genau eine Primzahl $p \in \mathbb{P}$ mit $x \mid p$ in $\mathbb{Z}[i]$; dabei sind genau zwei sich ausschließende Fälle möglich:*

(i) *$p \sim x$ in $\mathbb{Z}[i]$.*

(ii) *$p = x \cdot \overline{x}$.*

Beweis: Sei $x \in \mathbb{Z}[i]$ ein Primelement, dann ist $x \notin \{0\} \cup \mathbb{Z}[i]^\times$ und somit $N(x) > 1$. Mittels Primfaktorzerlegung in $\mathbb{Z}$ erhält man $p_1, ..., p_n \in \mathbb{P}$ mit $n \in \mathbb{N}^+$, sodass

$$x \cdot \overline{x} = N(x) = \prod_{\nu=1}^{n} p_\nu.$$

Da x ein Primelement in $\mathbb{Z}[i]$ ist, gibt es ein $p \in \{p_1, ..., p_n\}$ mit $x \mid p$ in $\mathbb{Z}[i]$. Angenommen es gebe noch ein $p' \in \mathbb{P}$ mit $p' \neq p$ und $x \mid p'$; wegen $\mathrm{ggT}(p, p') = 1$ existieren dann $l, l' \in \mathbb{Z}$ mit $1 = lp + l'p'$. Weiters folgt aus $x \mid p$ sowie $x \mid p'$ die Beziehung $x \mid lp + l'p' = 1$, womit $x \in \mathbb{Z}[i]^\times$ ist - ein Widerspruch, der zeigt, dass es genau ein $p \in \mathbb{P}$ gibt mit $x \mid p$ in $\mathbb{Z}[i]$.

Sei nun $y \in \mathbb{Z}[i]$ mit $p = xy$, dann sind die folgenden zwei Fälle möglich:

Fall 1: $y \in \mathbb{Z}[i]^\times$: $p = xy$ mit $y \in \mathbb{Z}[i]^\times \Rightarrow p \sim x$ in $\mathbb{Z}[i]$.

Fall 2: $y \notin \mathbb{Z}[i]^\times$: $N(x) > 1$ und $N(y) > 1$, da $p \neq 0 \Rightarrow y \neq 0$; somit folgt aus $p^2 = N(p) = N(x)N(y)$ und $p \in \mathbb{P}$, dass $N(x) = N(y) = p$ ist. Es ergibt sich $p \cdot \overline{x} = x \cdot y \cdot \overline{x} = N(x) \cdot y = p \cdot y$ und schließlich durch Kürzen $\overline{x} = y$, woraus man nun $p = xy = x\overline{x}$ erhält.

Es bleibt noch zu zeigen, dass sich die beiden im Satz angegebenen Fälle ausschließen. Gelte also (i) und (ii), dann folgt zunächst $\epsilon x = p = x\overline{x}$ mit $\epsilon \in \mathbb{Z}[i]^\times$ und damit $\overline{x} = \epsilon \in \mathbb{Z}[i]^\times$, womit auch $x \in \mathbb{Z}[i]^\times$ und schließlich $p \in \mathbb{Z}[i]^\times$ ist - ein Widerspruch. □

Satz 3.4. *Für jede Primzahl $p \in \mathbb{P}$ gibt es genau drei sich ausschließende Möglichkeiten für die Primzerlegung von p in $\mathbb{Z}[i]$:*

(i) *p ist ein Primelement in $\mathbb{Z}[i]$.*

(ii) *$p = x \cdot \overline{x}$ mit $x \sim \overline{x}$ und x ist ein Primelement in $\mathbb{Z}[i]$.*

(iii) *$p = x \cdot \overline{x}$ mit $x \nsim \overline{x}$ und x ist ein Primelement in $\mathbb{Z}[i]$.*

Beweis: Sei $p \in \mathbb{P}$, dann ist $N(p) = p^2 > 1$ und damit $p \notin \mathbb{Z}[i]^\times$. Aus Satz 1.15 folgt zunächst, dass es ein Primelement $x \in \mathbb{Z}[i]$ mit $x \mid p$ gibt; laut Satz 3.3 ist nun $p = \epsilon x$ oder $p = x \cdot \overline{x}$ mit $\epsilon \in \mathbb{Z}[i]^\times$. Im ersten Fall ist p laut Lemma 3.1 selbst ein Primelement - Möglichkeit (i); im zweiten Fall ist $p = x \cdot \overline{x}$ - dies entspricht den sich ausschließenden Möglichkeiten (ii) und (iii).

Die Möglichkeiten (ii) und (iii) schließen sich offensichtlich aus. Ebenso können auch (i) und (ii) sowie (i) und (iii) nicht gleichzeitig eintreten, denn ein $p \in \mathbb{P}$ mit $p = x\overline{x}$ und einem Primelement $x \in \mathbb{Z}[i]$ kann nicht prim in $\mathbb{Z}[i]$ sein, da x ein Teiler von p ist, der keine Einheit und wegen $\overline{x} \notin \mathbb{Z}[i]^\times$ auch nicht zu p assoziiert ist. Somit ist x ein echter Teiler von p und p daher kein Primelement in $\mathbb{Z}[i]$. □

Definition 3.5. Sei $p \in \mathbb{P}$ eine Primzahl, dann heißt p

- **träge** in $\mathbb{Z}[i]$ $:\iff$ p erfüllt Bedingung (i) in Satz 3.4.
- **verzweigt** in $\mathbb{Z}[i]$ $:\iff$ p erfüllt Bedingung (ii) in Satz 3.4.
- **unverzweigt** in $\mathbb{Z}[i]$ $:\iff$ p erfüllt Bedingung (iii) in Satz 3.4.

Definition 3.6. Die Menge $\mathbb{P}$ der Primzahlen kann folgendermaßen aufgeteilt werden:

- $\mathcal{T} := \{p \in \mathbb{P} \mid p \text{ ist träge in } \mathbb{Z}[i]\}$.
- $\mathcal{V} := \{p \in \mathbb{P} \mid p \text{ ist verzweigt in } \mathbb{Z}[i]\}$.
- $\mathcal{U} := \{p \in \mathbb{P} \mid p \text{ ist unverzweigt in } \mathbb{Z}[i]\}$.

Proposition 3.7. *Die Beziehung $\mathbb{P} = \mathcal{T} \dot\cup \mathcal{V} \dot\cup \mathcal{U}$ stellt eine disjunkte Zerlegung von $\mathbb{P}$ dar.*

Beweis: Laut Satz 3.4 gibt es für eine Primzahl $p \in \mathbb{P}$ genau die drei sich ausschließenden Möglichkeiten $p \in \mathcal{T}$ oder $p \in \mathcal{V}$ oder $p \in \mathcal{U}$; folglich kann man die obige disjunkte Aufteilung von $\mathbb{P}$ durchführen. □

Proposition 3.8. *Seien $x \in \mathbb{Z}[i]$ prim und $p \in \mathbb{P}$ die nach Satz 3.3 eindeutig bestimmte Primzahl mit $x \mid p$, dann gilt:*

- $p \in \mathcal{T} \implies N(x) = p^2$.
- $p \in \mathcal{V} \cup \mathcal{U} \implies N(x) = p$.

Beweis: Seien $x \in \mathbb{Z}[i]$ prim, $p \in \mathbb{P}$ mit $x \mid p$. Ist $p \in \mathcal{T}$, dann ist p ein Primelement in $\mathbb{Z}[i]$ und besitzt daher keine echten Teiler, also muss $x \sim p$ bzw. $x = \epsilon p$ mit $\epsilon \in \mathbb{Z}[i]^\times$ sein. Damit erhält man $N(x) = N(\epsilon p) = N(p) = p^2$. Falls $p \in \mathcal{V} \cup \mathcal{U}$ ist, gilt $p = x \cdot \overline{x}$ und somit $N(x) = x \cdot \overline{x} = p$. □

Lemma 3.9. *Sei $p \in \mathbb{P}$ eine Primzahl, dann gilt:* $p \in 4\mathbb{Z} + 3 \implies p \in \mathcal{T}$.

Beweis: Sei $p \in \mathbb{P} \cap (4\mathbb{Z} + 3)$.

Schritt 1: Es gilt $(\forall\, a, b \in \mathbb{Z})\ p \neq a^2 + b^2$. Angenommen das ist nicht der Fall, dann gibt es $a, b, k \in \mathbb{Z}$ mit $4k + 3 = p = a^2 + b^2$; dies ist aber ein Widerspruch, wie die folgende Fallunterscheidung zeigt:

Fall 1: $a \in 2\mathbb{Z}, b \in 2\mathbb{Z}$: Dieser Fall liefert wegen $4k + 3 \in 2\mathbb{Z} + 1$ und $a^2 + b^2 \in 2\mathbb{Z}$ einen Widerspruch.

Fall 2: $a \in 2\mathbb{Z} + 1, b \in 2\mathbb{Z} + 1$: Ein Widerspruch, da $4k + 3 \in 2\mathbb{Z} + 1$ und $a^2 + b^2 \in 2\mathbb{Z}$ ist.

Fall 3: $a \in 2\mathbb{Z}, b \in 2\mathbb{Z} + 1$: Es gilt $2 \mid a \Rightarrow 4 \mid a^2$; weiters findet man $b = 2g + 1 \Rightarrow b^2 = 4g^2 + 4g + 1 \equiv 1 \ mod\ 4$ mit $g \in \mathbb{Z}$. Somit ist $4\mathbb{Z} + 3 \ni a^2 + b^2 \equiv 0 + 1 = 1 \ mod\ 4$ - ein Widerspruch.

Fall 4: $a \in 2\mathbb{Z} + 1, b \in 2\mathbb{Z}$: Ein Widerspruch analog zu Fall 3.

Schritt 2: Es gilt: $p \in \mathcal{T}$. Wiederum nimmt man an, das sei nicht der Fall, dann ist $p \in \mathcal{V} \cup \mathcal{U}$ und somit $p = x\overline{x}$ mit $x = a + bi \in \mathbb{Z}[i]$ und $a, b \in \mathbb{Z}$. Daher ist $p = a^2 + b^2$ - ein Widerspruch zu Schritt 1. □

Lemma 3.10. *Es gilt:* $\{2\} = \mathcal{V}$.

Beweis: $\underline{\subseteq}$: $2 = (1+i)(1-i)$, wobei $1+i$ wegen $N(1+i) = 2 \in \mathbb{P}$ ein Primelement in $\mathbb{Z}[i]$ ist. Aus $1+i \sim -i(1+i) = 1-i$ folgt nun $2 \in \mathcal{V}$.

$\underline{\supseteq}$: Seien $p \in \mathcal{V}$ und $x \in \mathbb{Z}[i]$ ein Primelement mit $p = x\overline{x}$ und $x \sim \overline{x}$; dann gilt einmal $x \mid \overline{x}$ in $\mathbb{Z}[i]$ und somit $x \mid x - \overline{x}$. Seien weiters $a, b \in \mathbb{Z}$ mit $x = a + bi$, so erhält man $x - \overline{x} = 2bi$ und $x \mid 2bi$ bzw. $2bi = kx$ mit $k \in \mathbb{Z}[i]$; zusätzlich ergibt sich $4b^2 = N(2bi) = N(k)N(x) = N(k)x\overline{x} = N(k)p$ und somit $p \mid 4b^2$ in $\mathbb{Z}$.

Angenommen $p \mid b$, dann gilt $p = x\overline{x} = a^2 + b^2 \Rightarrow p \mid p - b^2 = a^2$ und, da p prim ist, auch $p \mid a$; seien nun $k_a, k_b \in \mathbb{Z}$ mit $a = k_a p$ und $b = k_b p$, dann ist $p = a^2 + b^2 = p^2(k_a^2 + k_b^2)$ und damit $1 = p(k_a^2 + k_b^2)$, woraus schließlich $p \mid 1$ folgt - ein Widerspruch. Also muss $p \nmid b$ und wegen $p \in \mathbb{P}$ auch $p \nmid b^2$ gelten; aus demselben Grund muss aber wegen $p \mid 4b^2$ daher p ein Teiler von 4 sein, woraus $p = 2$ folgt. □

Lemma 3.11. *Sei $p \in \mathbb{P}$ eine Primzahl, dann gilt:* $p \in 4\mathbb{Z} + 1 \implies p \in \mathcal{U}$.

Beweis: Sei $p \in \mathbb{P} \cap (4\mathbb{Z} + 1)$, dann gibt es ein $m \in \mathbb{N}^+$ mit $p = 4m + 1$.

Schritt 1: Es gilt: $(\exists\, u \in \mathbb{Z})\ p \mid u^2 + 1$. Setze $u = (2m)!$, dann folgt aus dem *Satz von Wilson*

$$\begin{aligned} -1 &\equiv (p-1)! = (4m)! = (2m)! \cdot (2m+1) \cdot \ldots \cdot 4m = u \cdot (p-2m) \cdot \ldots \cdot (p-1) \equiv \\ &\equiv u \cdot (-1) \cdot \ldots \cdot (-2m) = u \cdot (-1)^{2m} \cdot (2m)! = u^2 \ (mod\ p). \end{aligned}$$

Somit erhält man $u^2 + 1 \equiv 0\ (mod\ p)$ bzw. $p \mid u^2 + 1$.

Schritt 2: Es gilt: $p \in \mathcal{U}$. Setze $x := u + i$, dann ist $x\overline{x} = u^2 + 1$ und daher gilt $p \mid x\overline{x}$. Angenommen p teilt x oder $\overline{x}$ in $\mathbb{Z}[i]$: $u \pm i = p(k \pm li)$ mit $k, l \in \mathbb{Z}$ liefert $\pm i = \pm pli$ bzw. $\pm 1 = \pm pl$ mittels Vergleich der Imaginärteile, was schließlich $p \mid 1$ zur Folge hat - ein Widerspruch; somit teilt p weder x noch $\overline{x}$ in $\mathbb{Z}[i]$ und daher kann p kein Primelement in $\mathbb{Z}[i]$ sein. Da ferner $p \in 4\mathbb{Z} + 1$ und damit insbesondere $p \neq 2$ ist kann p auch nicht verzweigt sein; also muss $p \in \mathcal{U}$ sein. □

Satz 3.12. *Es gilt:* $\mathcal{T} = \mathbb{P} \cap (4\mathbb{Z} + 3), \quad \mathcal{V} = \{2\}, \quad \mathcal{U} = \mathbb{P} \cap (4\mathbb{Z} + 1)$.

Beweis: Zunächst gilt einmal $\mathbb{P} \cap 4\mathbb{Z} = \emptyset$ und $\mathbb{P} \cap (4\mathbb{Z} + 2) = \{2\}$, da keine Primzahl von 4 geteilt wird und 2 die einzige gerade Primzahl ist. Somit ergibt sich

$$\begin{aligned} \mathbb{P} &= (\mathbb{P} \cap 4\mathbb{Z}) \,\dot\cup\, (\mathbb{P} \cap (4\mathbb{Z} + 1)) \,\dot\cup\, (\mathbb{P} \cap (4\mathbb{Z} + 2)) \,\dot\cup\, (\mathbb{P} \cap (4\mathbb{Z} + 3)) = \\ &= (\mathbb{P} \cap (4\mathbb{Z} + 1)) \,\dot\cup\, \{2\} \,\dot\cup\, (\mathbb{P} \cap (4\mathbb{Z} + 3)). \end{aligned}$$

Die Inklusionen $\mathcal{T} \supseteq \mathbb{P} \cap (4\mathbb{Z}+3)$ und $\mathcal{U} \supseteq \mathbb{P} \cap (4\mathbb{Z}+1)$ folgen direkt aus Lemma 3.9 und Lemma 3.11, die Gleichheit $\{2\} = \mathcal{V}$ aus Lemma 3.10. Um noch die beiden umgekehrten Inklusionen zu zeigen, sei einmal $p \in \mathcal{T}$, dann ist $p \in \mathbb{P}$ und nach Proposition 3.7 auch $p \notin \mathcal{V}$ und $p \notin \mathcal{U}$, also ist $p \notin (4\mathbb{Z}+1) \cup \{2\}$. Aus der oben betrachteten disjunkten Aufteilung von $\mathbb{P}$ erhält man nun $p \in \mathbb{P} \cap (4\mathbb{Z} + 3)$. Analog findet man die Implikation $p \in \mathcal{U} \ \Rightarrow\ p \notin \mathcal{T} \cup \mathcal{V} \ \Rightarrow\ p \notin (4\mathbb{Z} + 3) \cup \{2\} \ \Rightarrow\ p \in \mathbb{P} \cap (4\mathbb{Z} + 1)$, womit die drei Mengenäquivalenzen gezeigt sind. □

Definition 3.13. Sei $p \in \mathbb{P}$, dann wählt man auf folgende Art ein Primelement $\pi_p \in \mathbb{Z}[i]$. Falls $p \in \mathcal{T}$ ist, wähle $\pi_p := p$; falls $p \in \mathcal{V} \cup \mathcal{U}$ ist, wähle $\pi_p := x$, wobei $p = x \cdot \overline{x}$ ist mit $x \in \mathbb{Z}[i]$. Nun kann die Menge all dieser Primelemente $\pi_p \in \mathbb{Z}[i]$ zu sämtlichen Primzahlen $p \in \mathbb{P}$ folgendermaßen aufgeteilt werden:

- $\mathfrak{T} := \{\pi_p \in \mathbb{Z}[i] \ \mid\ p \in \mathcal{T}\}$.
- $\mathfrak{V} := \{\pi_p \in \mathbb{Z}[i] \ \mid\ p \in \mathcal{V}\}$.
- $\mathfrak{U} := \{\pi_p, \overline{\pi_p} \in \mathbb{Z}[i] \ \mid\ p \in \mathcal{U}\}$.
- $\mathfrak{P} := \mathfrak{T} \cup \mathfrak{V} \cup \mathfrak{U}$.

Proposition 3.14. *Die Beziehung $\mathfrak{P} = \mathfrak{T} \,\dot\cup\, \mathfrak{V} \,\dot\cup\, \mathfrak{U}$ stellt eine disjunkte Zerlegung von $\mathfrak{P}$ dar.*

Beweis: Laut Definition ist $\mathfrak{P} = \mathfrak{T} \cup \mathfrak{V} \cup \mathfrak{U}$; es bleibt noch zu zeigen, dass die Mengen $\mathfrak{T}$, $\mathfrak{V}$ und $\mathfrak{U}$ paarweise disjunkt sind. Angenommen es gibt ein $\pi \in \mathfrak{T} \cap \mathfrak{V}$, dann findet man auch ein $p_1 \in \mathcal{T}$ sowie ein $p_2 \in \mathcal{V}$ mit $\pi \mid p_1$ und $\pi \mid p_2$. Dies hätte laut Satz 3.3 aber $p_1 = p_2$ und damit $\mathcal{T} \cap \mathcal{V} \neq \emptyset$ zur Folge - ein Widerspruch zu Proposition 3.7. Analog findet man $\mathfrak{T} \cap \mathfrak{U} = \emptyset$ und $\mathfrak{V} \cap \mathfrak{U} = \emptyset$.

Satz 3.15. *1. Die Menge $\mathfrak{P}$ ist bezüglich der Assoziiertheit $\sim$ ein Repräsentantensystem der primen Elemente von $\mathbb{Z}[i]$, das heißt* $(\forall\ \pi \in \mathbb{Z}[i]\ prim)(\exists^1\ \pi_0 \in \mathfrak{P})\ \pi \sim \pi_0$.

2. Jedes $a \in \mathbb{Z}[i]\backslash\{0\}$ hat eine eindeutige Darstellung der Form

$$a = \epsilon \prod_{\pi \in \mathfrak{P}} \pi^{\alpha_\pi}$$

mit $\epsilon \in \mathbb{Z}[i]^\times,\ \alpha_\pi \in \mathbb{N}$ für alle $\pi \in \mathfrak{P}$ und $\alpha_\pi = 0$ für fast alle $\pi \in \mathfrak{P}$.

Beweis: 1. Sei $\pi \in \mathbb{Z}[i]$ prim, dann gibt es laut Satz 3.3 eine Primzahl $p \in \mathbb{P}$ mit entweder $p \sim \pi$ oder $p = \pi\overline{\pi}$. Im ersten Fall ist p selbst Primelement in $\mathbb{Z}[i]$; damit ist $p \in \mathcal{T}$ und es gilt $\pi \sim p = \pi_p \in \mathfrak{T} \in \mathfrak{P}$; im zweiten Fall ist p kein Primelement in $\mathbb{Z}[i]$, womit also entweder $p \in \mathcal{V}$ oder $p \in \mathcal{U}$ ist; somit gibt es entweder ein $\pi_p \in \mathfrak{V}$ mit $p = \pi_p\overline{\pi_p}$ und $\pi_p \sim \overline{\pi_p}$, oder es gibt $\pi_p, \overline{\pi_p} \in \mathfrak{U}$ mit $p = \pi_p\overline{\pi_p}$ und $\pi_p \nsim \overline{\pi_p}$. In beiden Fällen gilt jedoch $\pi\overline{\pi} = p = \pi_p\overline{\pi_p}$ und wegen der Eindeutigkeit der Zerlegung von p in Primelemente bis auf Reihenfolge und Assoziiertheit schließlich $\pi \sim \pi_p \in \mathfrak{V} \subseteq \mathfrak{P}$ im ersten bzw. $\pi \sim \pi_p \in \mathfrak{U} \subseteq \mathfrak{P}$ oder $\pi \sim \overline{\pi_p} \in \mathfrak{U} \subseteq \mathfrak{P}$ im zweiten Fall.

Seien nun $\pi_1, \pi_2 \in \mathfrak{P}$ mit $\pi_1 \sim \pi_2$ und $p_1, p_2 \in \mathbb{P}$ die dazugehörigen Primzahlen in $\mathbb{Z}$; es ist zu zeigen, dass $\pi_1 = \pi_2$ ist. Dies beweist man mittels folgender Fallunterscheidung:

Fall 1: $p_1 \in \mathcal{T},\ p_2 \in \mathcal{T}$**:** $p_1^2 = N(\pi_1) = N(\pi_2) = p_2^2 \ \Rightarrow\ p_1 = p_2 \ \Rightarrow\ \pi_1 = \pi_2$.

Fall 2: $p_1 \in \mathcal{T},\ p_2 \in \mathcal{V}$**:** $p_1^2 = N(\pi_1) = N(\pi_2) = p_2$ - Widerspruch zu $p_2 \in \mathbb{P}$ - Fall tritt nicht auf.

Fall 3: $p_1 \in \mathcal{T},\ p_2 \in \mathcal{U}$**:** $p_1^2 = N(\pi_1) = N(\pi_2) = p_2$ - Widerspruch zu $p_2 \in \mathbb{P}$ - Fall tritt nicht auf.

Fall 4: $p_1 \in \mathcal{V},\ p_2 \in \mathcal{V}$**:** $p_1 = N(\pi_1) = N(\pi_2) = p_2 \ \Rightarrow\ \pi_1 = \pi_2$.

Fall 5: $p_1 \in \mathcal{V},\ p_2 \in \mathcal{U}$**:** $\pi_2 \sim \pi_1 \sim \overline{\pi_1} \sim \overline{\pi_2}$ - Widerspruch zu $\pi_2 \nsim \overline{\pi_2}$ - Fall tritt nicht auf.

Fall 6: $p_1 \in \mathcal{U},\ p_2 \in \mathcal{U}$**:** $p_1 = N(\pi_1) = N(\pi_2) = p_2$; sei also $p := p_1 = p_2$. Angenommen es gilt $\pi_1 = \pi_p$ und $\pi_2 = \overline{\pi_p}$, dann ist $\pi_p = \pi_1 \sim \pi_2 = \overline{\pi_p}$ - ein Widerspruch; somit ist entweder $\pi_1 = \pi_2 = \pi_p$ oder $\pi_1 = \pi_2 = \overline{\pi_p}$.

2. Aus Satz 1.15 folgt für ein $a \in \mathbb{Z}[i]\backslash(\{0\} \cup \mathbb{Z}[i]^\times)$ die Existenz und Eindeutigkeit der Darstellung von a als Produkt von Primelementen bis auf Reihenfolge und Assoziiertheit; lässt man nun nur mehr Primzahlen aus $\mathfrak{P}$ zu und verwendet die obige Produktschreibweise, so erhält man die geforderte Eindeutigkeit. Ist $a \in \mathbb{Z}[i]^\times$, so hat a die eindeutige Darstellung $a = a \prod_{\pi \in \mathfrak{P}} \pi^0$, das heißt $\epsilon = a$ und $\alpha_\pi = 0$ für alle $\pi \in \mathfrak{P}$. □

4 Struktur von $\mathbb{Z}[i]/\mathbb{Z}[i]x$

Notation: Für $x \in \mathbb{Z}[i]$ sei $\Pi_x : \mathbb{Z}[i] \to \mathbb{Z}[i]/\mathbb{Z}[i]x$ der kanonische Homomorphismus.

Definition 4.1. Sei $\psi : \begin{cases} \mathbb{Z}[i]\backslash\{0\} & \to \mathbb{N}^+ \cup \{\infty\} \\ x & \mapsto |\mathbb{Z}[i]/\mathbb{Z}[i]x| \end{cases}$

Lemma 4.2. *Seien $x, y \in \mathbb{Z}[i]\backslash\{0\}$, dann ist $\psi(xy) = \psi(x)\psi(y)$.*

Beweis: Seien $x, y \in \mathbb{Z}[i]\backslash\{0\}$. Da $\mathbb{Z}[i]xy$ ein Ideal von $\mathbb{Z}[i]$ und $\mathbb{Z}[i]xy \subseteq \mathbb{Z}[i]x = ker(\Pi_x)$ ist, folgt aus der *„universellen Eigenschaft des Restklassenhomomorphismus“*, dass es einen Ringhomomorphismus $f : \mathbb{Z}[i]/\mathbb{Z}[i]xy \to \mathbb{Z}[i]/\mathbb{Z}[i]x$ gibt, sodass $f \circ \Pi_{xy} = \Pi_x$; weiters folgt aus der Surjektivität von Π_x die Surjektivität von f und es gilt $ker(f) = \Pi_{xy}(ker(\Pi_x)) = \Pi_{xy}(\mathbb{Z}[i]x)$.

Seien $z_1, z_2 \in \mathbb{Z}[i]$, dann gilt: $\Pi_y(z_1) = \Pi_y(z_2) \Rightarrow \Pi_y(z_1 - z_2) = 0 \Rightarrow z_1 - z_2 \in \mathbb{Z}[i]y \Rightarrow (z_1 - z_2)x \in \mathbb{Z}[i]yx = \mathbb{Z}[i]xy \Rightarrow \Pi_{xy}((z_1 - z_2)x) = \Pi_{xy}(z_1x - z_2x) = 0 \Rightarrow \Pi_{xy}(z_1x) = \Pi_{xy}(z_2x)$. Also kann man eine Abbildung $g : \mathbb{Z}[i]/\mathbb{Z}[i]y \to \Pi_{xy}(\mathbb{Z}[i]x)$ via $g(\Pi_y(z)) = \Pi_{xy}(zx)$ definieren, wobei bereits die Surjektivität von Π_y ausgenützt wurde und $z \in \mathbb{Z}[i]$ ist.

g ist ein Homomorphismus von $(\mathbb{Z}[i]/\mathbb{Z}[i]y, +)$ nach $(\Pi_{xy}(\mathbb{Z}[i]x), +)$: Seien $u_1, u_2 \in \mathbb{Z}[i]/\mathbb{Z}[i]y$ und $z_1, z_2 \in \mathbb{Z}[i]$ mit $u_j = \Pi_y(z_j)$ für $j \in \{1, 2\}$; dann ist $g(u_1 + u_2) = g(\Pi_y(z_1) + \Pi_y(z_2)) = g(\Pi_y(z_1 + z_2)) = \Pi_{xy}((z_1 + z_2)x) = \Pi_{xy}(z_1x + z_2x) = \Pi_{xy}(z_1x) + \Pi_{xy}(z_2x) = g(\Pi_y(z_1)) + g(\Pi_y(z_2)) = g(u_1) + g(u_2)$.

g ist surjektiv: Sei $v \in \Pi_{xy}(\mathbb{Z}[i]x)$ und $z \in \mathbb{Z}[i]$ mit $v = \Pi_{xy}(zx)$, dann ist $g(\Pi_y(z)) = \Pi_{xy}(zx) = v$.

g ist injektiv: Seien $u_1, u_2 \in \mathbb{Z}[i]/\mathbb{Z}[i]y$ und $z_1, z_2 \in \mathbb{Z}[i]$ mit $u_j = \Pi_y(z_j)$ für $j \in \{1, 2\}$ und gelte $g(u_1) = g(u_2)$. Dann ist $0 = g(u_1 - u_2) = g(\Pi_y(z_1 - z_2)) = \Pi_{xy}((z_1 - z_2)x)$, also ist $(z_1 - z_2)x \in ker(\Pi_{xy}) = \mathbb{Z}[i]xy$ und da $x \neq 0$ kein Nullteiler ist, gilt weiters $z_1 - z_2 \in \mathbb{Z}[i]y = ker(\Pi_y)$; daraus ergibt sich $\Pi_y(z_1 - z_2) = 0$ bzw. $u_1 = \Pi_y(z_1) = \Pi_y(z_2) = u_2$.

Somit ist $g : \mathbb{Z}[i]/\mathbb{Z}[i]y \to \Pi_{xy}(\mathbb{Z}[i]x)$ ein Gruppenisomorphismus und

$$\mathbb{Z}[i]/\mathbb{Z}[i]y \cong \Pi_{xy}(\mathbb{Z}[i]x) = ker(f),$$

woraus insbesondere $|ker(f)| = |\mathbb{Z}[i]/\mathbb{Z}[i]y| = \psi(y)$ folgt. Andererseits erhält man aus dem Homomorphiesatz der Gruppentheorie

$$(\mathbb{Z}[i]/\mathbb{Z}[i]xy)/ker(f) \cong f(\mathbb{Z}[i]/\mathbb{Z}[i]xy) = \mathbb{Z}[i]/\mathbb{Z}[i]x$$

und damit $|(\mathbb{Z}[i]/\mathbb{Z}[i]xy)/ker(f)| = |\mathbb{Z}[i]/\mathbb{Z}[i]x| = \psi(x)$. Mittels *Satz von Lagrange* und der Tatsache, dass $ker(f)$ eine Untergruppe von $\mathbb{Z}[i]/\mathbb{Z}[i]xy$ ist, ergibt sich schließlich $\psi(xy) = |\mathbb{Z}[i]/\mathbb{Z}[i]xy| = |(\mathbb{Z}[i]/\mathbb{Z}[i]xy)/ker(f)| \cdot |ker(f)| = \psi(x)\psi(y)$. □

Lemma 4.3. *Sei $m \in \mathbb{N}^+$, dann ist $\psi(m) = m^2$.*

Beweis: Seien $m \in \mathbb{N}^+$ und

$$S := \{a + bi \in \mathbb{Z}[i] \mid 0 \leq a, b < m\},$$

dann ist $\Pi_m|_S : S \to \mathbb{Z}[i]/\mathbb{Z}[i]m$ bijektiv, wie die folgenden Überlegungen zeigen.

$\Pi_m|_S$ ist surjektiv: Sei $z \in \mathbb{Z}[i]/\mathbb{Z}[i]m$, wähle $y \in \mathbb{Z}[i]$ mit $z = \Pi_m(y)$ und $u, v \in \mathbb{Z}$ mit $y = u + vi$; mittels Division mit Rest erhält man $u = mq + r$ und $v = ms + t$ mit $q, r, s, t \in \mathbb{Z}$ und $0 \leq r, t < m$. Dann gilt $z = \Pi_m(y) = \Pi_m(u + vi) = \Pi_m(mq + r + msi + ti) = \Pi_m(m(q + si) + r + ti) = \Pi_m(m)\Pi_m(q + si) + \Pi_m(r + ti) = 0 + \Pi_m(r + ti) = (\Pi_m|_S)(r + ti)$, somit ist $\Pi_m|_S$ surjektiv.

$\Pi_m|_S$ ist injektiv: Seien $y_1, y_2 \in S$ und $u_1, u_2, v_1, v_2 \in \{w \in \mathbb{Z} \mid 0 \leq w < m\}$ mit $y_1 = u_1 + v_1i$, $y_2 = u_2 + v_2i$ und $(\Pi_m|_S)(y_1) = (\Pi_m|_S)(y_2)$. Dann ist $(\Pi_m|_S)(u_1 + v_1i) = (\Pi_m|_S)(u_2 + v_2i)$ bzw. $\Pi_m((u_1 - u_2) + (v_1 - v_2)i) = 0$, das heißt es gibt ein $q \in \mathbb{Z}[i]$, sodass $(u_1 - u_2) + (v_1 - v_2)i = qm$ ist. Nach Lemma 3.1 folgt daraus sowohl $m \mid u_1 - u_2$ in $\mathbb{Z}$ als auch $m \mid v_1 - v_2$ in $\mathbb{Z}$, und da $-m + 1 \leq u_1 - u_2 \leq m - 1$ sowie $-m + 1 \leq v_1 - v_2 \leq m - 1$ ist, müssen $u_1 = u_2$ und $v_1 = v_2$ sein, womit gezeigt ist, dass $\Pi_m|_S$ auch injektiv ist.

Da nun $\Pi_m|_S$ eine Bijektion zwischen S und $\mathbb{Z}[i]/\mathbb{Z}[i]m$ darstellt, gilt $\psi(m) = |\mathbb{Z}[i]/\mathbb{Z}[i]m| = |S| = m^2$. □

Satz 4.4. *Sei $x \in \mathbb{Z}[i]\backslash\{0\}$, dann ist $\psi(x) = N(x)$.*

Beweis: Sei $x \in \mathbb{Z}[i]$, $x \neq 0$. Laut Bemerkung 1.1 ist $\bar{\cdot} : \mathbb{Z}[i] \to \mathbb{Z}[i]$ ein Ringisomorphismus; weiters ist $\mathbb{Z}[i]x$ ein Ideal von $\mathbb{Z}[i]$ mit $\overline{\mathbb{Z}[i]x} = \mathbb{Z}[i]\overline{x}$. Nach dem Isomorphieprinzip induziert $\bar{\cdot}$ einen Ringisomorphismus $f : \mathbb{Z}[i]/\mathbb{Z}[i]x \to \overline{\mathbb{Z}[i]}/\overline{\mathbb{Z}[i]x} = \mathbb{Z}[i]/\mathbb{Z}[i]\overline{x}$; somit ist $\mathbb{Z}[i]/\mathbb{Z}[i]\overline{x} \cong \mathbb{Z}[i]/\mathbb{Z}[i]x$, woraus sich $\psi(\overline{x}) = \psi(x)$ ergibt.

Aus den vorhergehenden Lemmata zusammen mit $\psi(x), N(x) > 0$ folgt nun $\psi(x)^2 = \psi(x)\psi(x) = \psi(x)\psi(\overline{x}) = \psi(x\overline{x}) = \psi(N(x)) = N(x)^2$ und damit schließlich $\psi(x) = N(x)$. □

Satz 4.5. *Seien $x \in \mathbb{Z}[i]\backslash\{0\}$, $y \in \mathbb{Z}[i]$, dann gelten*

1. *$\Pi_x(y)$ ist ein Nullteiler von $\mathbb{Z}[i]/\mathbb{Z}[i]x \iff \mathrm{GGT}(x,y) \neq \mathbb{Z}[i]^\times$.*
2. *$\Pi_x(y)$ ist eine Einheit von $\mathbb{Z}[i]/\mathbb{Z}[i]x \iff \mathrm{GGT}(x,y) = \mathbb{Z}[i]^\times$.*
3. *$\mathbb{Z}[i]/\mathbb{Z}[i]x$ ist ein Körper $\iff$ $\mathbb{Z}[i]/\mathbb{Z}[i]x$ ist ein Bereich $\iff$ x ist ein Primelement.*

Beweis: 1. $\underline{\Rightarrow:}$ Sei $\Pi_x(y)$ ein Nullteiler von $\mathbb{Z}[i]/\mathbb{Z}[i]x$, dann gibt es ein $w \in (\mathbb{Z}[i]/\mathbb{Z}[i]x)\backslash\{0\}$, sodass $\Pi_x(y)w = 0$ ist; sei weiters $u \in \mathbb{Z}[i]$ mit $w = \Pi_x(u)$. Da $w \neq 0$ ist, erhält man $u \notin ker(\Pi_x) = \mathbb{Z}[i]x$, woraus $x \nmid u$ folgt; andererseits ist aber $0 = \Pi_x(y)w = \Pi_x(y)\Pi_x(u) = \Pi_x(uy)$, was nun $x \mid uy$ impliziert. Angenommen $\mathrm{GGT}(x,y) = \mathbb{Z}[i]^\times$, dann ergibt sich zusammen mit Satz 2.5 der Widerspruch $x \mid u$; also ist $\mathrm{GGT}(x,y) \neq \mathbb{Z}[i]^\times$.

$\underline{\Leftarrow:}$ Seien $\mathrm{GGT}(x,y) \neq \mathbb{Z}[i]^\times$ und $d \in \mathrm{GGT}(x,y)$; dann ist auch $d \notin \mathbb{Z}[i]^\times$ und man erhält $x \nmid \frac{x}{d}$, da $x \mid \frac{x}{d} \Rightarrow xd \mid x \Rightarrow d \mid 1 \Rightarrow d \in \mathbb{Z}[i]^\times$ - ein Widerspruch. Somit ist also $\frac{x}{d} \notin ker(\Pi_x)$ bzw. $\Pi_x(\frac{x}{d}) \neq 0$; schließlich folgt aus $\Pi_x(y)\Pi_x(\frac{x}{d}) = \Pi_x(\frac{yx}{d}) = \Pi_x(\frac{y}{d})\Pi_x(x) = 0$, dass $\Pi_x(y)$ ein Nullteiler von $\mathbb{Z}[i]/\mathbb{Z}[i]x$ ist.

2. $\underline{\Rightarrow:}$ Sei $\Pi_x(y) \in (\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times$, dann gibt es ein $w \in \mathbb{Z}[i]/\mathbb{Z}[i]x$ und ein $u \in \mathbb{Z}[i]$, sodass $\Pi_x(y)w = 1$ und $w = \Pi_x(u)$ ist. Weiters gilt $\Pi_x(1) = 1 = \Pi_x(y)\Pi_x(u) = \Pi_x(uy)$ und damit $\Pi_x(uy - 1) = 0$, woraus nun $x \mid uy - 1$ folgt; daher gibt es ein $z' \in \mathbb{Z}[i]$ mit $uy - 1 = xz'$ bzw. ein $z \in \mathbb{Z}[i]$ mit $zx + uy = 1$; folglich ist $1 \in \mathbb{Z}[i]x + \mathbb{Z}[i]y$ und damit $\mathrm{GGT}(x,y) = \mathbb{Z}[i]^\times$ laut Korollar 2.4.

   $\underline{\Leftarrow:}$ Sei jetzt $\mathrm{GGT}(x,y) = \mathbb{Z}[i]^\times$, dann ist $1 = ux + vy$ mit passenden $u, v \in \mathbb{Z}[i]$ laut Korollar 2.4; somit ist $1 = \Pi_x(1) = \Pi_x(ux + vy) = \Pi_x(u)\Pi_x(x) + \Pi_x(v)\Pi_x(y) = 0 + \Pi_x(v)\Pi_x(y) = \Pi_x(v)\Pi_x(y)$ und daher $\Pi_x(y) \in (\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times$.

3. Ist $\mathbb{Z}[i]/\mathbb{Z}[i]x$ ein Körper, so ist $\mathbb{Z}[i]/\mathbb{Z}[i]x$ klarerweise auch ein Bereich.

   Sei also $\mathbb{Z}[i]/\mathbb{Z}[i]x$ einmal ein Bereich und $y \in \mathbb{Z}[i]$ ein Teiler von x. Dann gibt es ein $z \in \mathbb{Z}[i]$ mit $x = yz$; folglich ist dann $0 = \Pi_x(x) = \Pi_x(yz) = \Pi_x(y)\Pi_x(z)$ und nach Voraussetzung muss damit $\Pi_x(y) = 0$ oder $\Pi_x(z) = 0$ sein; im ersten Fall folgt $y \in \mathbb{Z}[i]x$ und damit $x \mid y$ und schließlich $y \sim x$; im zweiten Fall erhält man analog $x \mid z$ und damit $z \sim x$, woraus sich $y \in \mathbb{Z}[i]^\times$ ergibt. Somit besitzt x keine echten Teiler und ist daher ein Primelement in $\mathbb{Z}[i]$.

   Sei nun x ein Primelement in $\mathbb{Z}[i]$; dann ist $x \notin \{0\} \cup \mathbb{Z}[i]^\times$ und deshalb $|\mathbb{Z}[i]/\mathbb{Z}[i]x| = N(x) \geq 2$ nach Satz 4.4; also ist $\mathbb{Z}[i]/\mathbb{Z}[i]x$ nicht der Nullring. Seien $u \in (\mathbb{Z}[i]/\mathbb{Z}[i]x)\backslash\{0\}$ und $y \in \mathbb{Z}[i]$ mit $u = \Pi_x(y)$; wegen $u \neq 0$ erhält man $y \notin ker(\Pi_x) = \mathbb{Z}[i]x$ bzw. $x \nmid y$. Sei $d \in \mathrm{GGT}(x,y)$; wegen $d \mid x$ muss $d \in \mathbb{Z}[i]^\times$ oder $d \sim x$ sein, da x ein Primelement ist; im letzteren Fall folgt auch $x \mid d$, was wegen $d \mid y$ schließlich $x \mid y$ impliziert - ein Widerspruch. Somit muss $d \in \mathbb{Z}[i]^\times$ und damit $\mathrm{GGT}(x,y) = \mathbb{Z}[i]^\times$ gelten, womit $u = \Pi_x(y) \in (\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times$ gezeigt ist; also ist jedes $u \in (\mathbb{Z}[i]/\mathbb{Z}[i]x)\backslash\{0\}$ invertierbar, und $\mathbb{Z}[i]/\mathbb{Z}[i]x$ daher ein Körper. □

5 Struktur der primen Restklassengruppen $(\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times$

Notation: Für $x \in \mathbb{Z}[i]$ sei $\Pi_x : \mathbb{Z}[i] \to \mathbb{Z}[i]/\mathbb{Z}[i]x$ der kanonische Homomorphismus.

Bemerkung 5.1. Sei $x \in \mathbb{Z}[i]\backslash\{0\}$; aus Satz 4.4 folgt dann unmittelbar $|(\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times| \leq |\mathbb{Z}[i]/\mathbb{Z}[i]x| = \psi(x) = N(x) < \infty$.

Definition 5.2. Sei $\phi_{\mathbb{Z}[i]} : \begin{cases} \mathbb{Z}[i]\backslash\{0\} & \to \mathbb{N}^+ \\ x & \mapsto |(\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times| \end{cases}$

Satz 5.3. *Seien $x, y \in \mathbb{Z}[i]\backslash\{0\}$ mit $\mathrm{GGT}(x, y) = \mathbb{Z}[i]^\times$, dann ist $\phi_{\mathbb{Z}[i]}(xy) = \phi_{\mathbb{Z}[i]}(x)\phi_{\mathbb{Z}[i]}(y)$.*

Beweis: Seien $x, y \in \mathbb{Z}[i]$ und $d \in \mathrm{GGT}(x, y) = \mathbb{Z}[i]^\times$; da $\mathbb{Z}[i]x + \mathbb{Z}[i]y = \mathbb{Z}[i]d = \mathbb{Z}[i]$ ist, sind die Ideale $\mathbb{Z}[i]x$ und $\mathbb{Z}[i]y$ teilerfremd und man erhält aus dem *chinesischen Restsatz*

$$\mathbb{Z}[i]/\mathbb{Z}[i]xy = \mathbb{Z}[i]/(\mathbb{Z}[i]x \cap \mathbb{Z}[i]y) \cong \mathbb{Z}[i]/\mathbb{Z}[i]x \times \mathbb{Z}[i]/\mathbb{Z}[i]y;$$

folglich gilt auch $(\mathbb{Z}[i]/\mathbb{Z}[i]xy)^\times \cong (\mathbb{Z}[i]/\mathbb{Z}[i]x \times \mathbb{Z}[i]/\mathbb{Z}[i]y)^\times = (\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times \times (\mathbb{Z}[i]/\mathbb{Z}[i]y)^\times$. Insgesamt ist also $\phi_{\mathbb{Z}[i]}(xy) = |(\mathbb{Z}[i]/\mathbb{Z}[i]xy)^\times| = |(\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times \times (\mathbb{Z}[i]/\mathbb{Z}[i]y)^\times| = |(\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times| \cdot |(\mathbb{Z}[i]/\mathbb{Z}[i]y)^\times| = \phi_{\mathbb{Z}[i]}(x)\phi_{\mathbb{Z}[i]}(y)$. □

Satz 5.4. *Seien $x \in \mathbb{Z}[i]\backslash\{0\}$ prim und $n \in \mathbb{N}^+$, dann ist $\phi_{\mathbb{Z}[i]}(x^n) = N(x)^{n-1}(N(x) - 1)$.*

Beweis: Sei $x \in \mathbb{Z}[i]$. Da $\mathbb{Z}[i]x^n$ ein Ideal von $\mathbb{Z}[i]$ und $\mathbb{Z}[i]x^n \subseteq \mathbb{Z}[i]x = ker(\Pi_x)$ ist, erhält man aus der *„universellen Eigenschaft des Restklassenhomomorphismus“*, dass es einen Ringhomomorphismus $f : \mathbb{Z}[i]/\mathbb{Z}[i]x^n \to \mathbb{Z}[i]/\mathbb{Z}[i]x$ gibt mit $f \circ \Pi_{x^n} = \Pi_x$; dieses f ist wegen der Surjektivität von Π_x ebenfalls surjektiv. Setze $f' := f|_{(\mathbb{Z}[i]/\mathbb{Z}[i]x^n)^\times} : (\mathbb{Z}[i]/\mathbb{Z}[i]x^n)^\times \to (\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times$; da das Bild unter f jeder Einheit in $\mathbb{Z}[i]/\mathbb{Z}[i]x^n$ eine Einheit in $\mathbb{Z}[i]/\mathbb{Z}[i]x$ ist, ist f' mit diesem Wertebereich wohldefiniert.

Sei nun $w \in (\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times$ beliebig und $u \in \mathbb{Z}[i]$ mit $w = \Pi_x(u)$; aus Satz 4.5 erhält man damit $\mathrm{GGT}(u, x) = \mathbb{Z}[i]^\times$ und mithilfe von Satz 2.5 auch $\mathrm{GGT}(u, x^n) = \mathbb{Z}[i]^\times$. Nochmalige Verwendung von Satz 4.5 liefert nun $\Pi_{x^n}(u) \in (\mathbb{Z}[i]/\mathbb{Z}[i]x^n)^\times$; insgesamt gilt also $w = \Pi_x(u) = (f \circ \Pi_{x^n})(u) = f(\Pi_{x^n}(u)) = f'(\Pi_{x^n}(u))$, womit gezeigt ist, dass f' auch surjektiv ist.

Aus dem Homomorphiesatz der Gruppentheorie ergibt sich $(\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times/ker(f') \cong (\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times$ und folglich $|(\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times/ker(f')| = |(\mathbb{Z}[i]/\mathbb{Z}[i]x)^\times| = N(x) - 1$, da x ein Primelement und $\mathbb{Z}[i]/\mathbb{Z}[i]x$ somit ein Körper ist.

Sei $u \in \mathbb{Z}[i]$, dann ist $\mathrm{GGT}(x^n, 1 + ux) = \mathbb{Z}[i]^\times$, da jeder gemeinsame Teiler von x^n und $1 + ux$ eine Potenz von x sein muss - weil x prim ist - aber $1 + ux$ nicht von x geteilt wird. Daher ist $\Pi_{x^n}(1 + ux) \in (\mathbb{Z}[i]/\mathbb{Z}[i]x^n)^\times$ und wegen $f'(\Pi_{x^n}(1 + ux)) = f(\Pi_{x^n}(1 + ux)) = \Pi_x(1 + ux) = \Pi_x(1) = 1$ ist $\Pi_{x^n}(1 + ux) \in ker(f')$.

Seien $u_1, u_2 \in \mathbb{Z}[i]$, dann gilt $\Pi_{x^n}(1 + u_1x) = \Pi_{x^n}(1 + u_2x) \Leftrightarrow x^n \mid u_1x - u_2x = (u_1 - u_2)x \Leftrightarrow x^{n-1} \mid u_1 - u_2 \Leftrightarrow \Pi_{x^{n-1}}(u_1) = \Pi_{x^{n-1}}(u_2)$.

Definiere nun $g : \mathbb{Z}[i]/\mathbb{Z}[i]x^{n-1} \to ker(f')$ via $g(\Pi_{x^{n-1}}(u)) = \Pi_{x^n}(1 + ux)$, dann ist g nach den Überlegungen zuvor wohldefiniert. Aus der Beziehung $\Pi_{x^n}(1 + u_1x) = \Pi_{x^n}(1 + u_2x) \Leftrightarrow \Pi_{x^{n-1}}(u_1) = \Pi_{x^{n-1}}(u_2)$ folgt außerdem die Injektivität von g. Um auch noch die Surjektivität von g zu zeigen, wähle man ein $y \in ker(f')$ beliebig, dann gibt es ein $v \in \mathbb{Z}[i]$ mit $y = \Pi_{x^n}(v)$; zusätzlich folgt aus $f'(y) = 1$ noch $\Pi_x(v) = f(\Pi_{x^n}(v)) = f'(\Pi_{x^n}(v)) = 1 = \Pi_x(1)$ und damit $x \mid 1 - v$ bzw. $x(-u) = 1 - v$ bzw. $v = 1 + ux$ mit $u \in \mathbb{Z}[i]$. Somit ist $g(\Pi_{x^{n-1}}(u)) = \Pi_{x^n}(1 + ux) = \Pi_{x^n}(v) = y$ und g daher surjektiv.

Also ist g bijektiv und folglich $|ker(f')| = |\mathbb{Z}[i]/\mathbb{Z}[i]x^{n-1}| = N(x^{n-1}) = N(x)^{n-1}$. Da $ker(f')$ eine Untergruppe von $(\mathbb{Z}[i]/\mathbb{Z}[i]x^n)^\times$ ist, ergibt sich das Ergebnis

$$\phi_{\mathbb{Z}[i]}(x^n) = |(\mathbb{Z}[i]/\mathbb{Z}[i]x^n)^\times| = |(\mathbb{Z}[i]/\mathbb{Z}[i]x^n)^\times/ker(f')| \cdot |ker(f')| = (N(x) - 1) \cdot N(x)^{n-1}$$

als Folgerung aus dem *Satz von Lagrange*. □

Satz 5.5. *Seien $p \in \mathcal{T}$ sowie $n \in \mathbb{N}^+$, dann gilt:*

$(\mathbb{Z}[i]/\mathbb{Z}[i]p^n)^\times$ *ist zyklisch* $\iff n = 1$.

Beweis: $\underline{n=1:}$ Da p ein Primelement in $\mathbb{Z}[i]$ ist, erhält man aus Satz 4.5, dass $\mathbb{Z}[i]/\mathbb{Z}[i]p$ ein Körper mit $N(p)$ Elementen ist. Also ist insbesondere $(\mathbb{Z}[i]/\mathbb{Z}[i]p)^\times$ endlich, woraus nun folgt, dass die Einheitengruppe $(\mathbb{Z}[i]/\mathbb{Z}[i]p)^\times$ zyklisch ist. [2, Kapitel 2, Satz 3.4]

$\underline{n \geq 2:}$ Laut Satz 5.4 gilt $\phi_{\mathbb{Z}[i]}(p^{n-1}) = |(\mathbb{Z}[i]/\mathbb{Z}[i]p^{n-1})^\times| = N(p)^{n-2}(N(p)-1) = p^{2(n-2)}(p^2-1)$; da die Gruppenordnung von $(\mathbb{Z}[i]/\mathbb{Z}[i]p^{n-1})^\times$ Vielfaches der Ordnung eines jeden Elements ist, ergibt sich folgende Aussage:

$$(\forall\ x \in (\mathbb{Z}[i]/\mathbb{Z}[i]p^{n-1})^\times)\ x^{p^{2(n-2)}(p^2-1)} = 1.$$

Sei nun $a \in \mathbb{Z}[i]$ mit $\mathrm{GGT}(p,a) = \mathbb{Z}[i]^\times$, dann ist auch $\mathrm{GGT}(p^{n-1},a) = \mathbb{Z}[i]^\times$, woraus mittels Satz 4.5 nun $\Pi_{p^{n-1}}(a) \in (\mathbb{Z}[i]/\mathbb{Z}[i]p^{n-1})^\times$ folgt. Zusammen mit der Überlegung zuvor erhält man

$$\Pi_{p^{n-1}}(a^{p^{2(n-2)}(p^2-1)}) = \Pi_{p^{n-1}}(a)^{p^{2(n-2)}(p^2-1)} = 1$$

bzw. äquivalent dazu

$$a^{p^{2(n-2)}(p^2-1)} \equiv 1\ (mod\ p^{n-1}).$$

Diese Kongruenz lässt sich auch in der Form

$$a^{p^{2n-4}(p^2-1)} = 1 + bp^{n-1}$$

mit $b \in \mathbb{Z}[i]$ anschreiben, woraus man durch Potenzieren mit p die Gleichung

$$a^{p^{2n-3}(p^2-1)} = (1+bp^{n-1})^p$$

erhält. Mittels binomischem Lehrsatz ergibt sich

$$\begin{aligned}(1+bp^{n-1})^p &= \sum_{k=0}^{p}\binom{p}{k}b^k p^{k(n-1)} = 1 + pbp^{n-1} + \sum_{k=2}^{p}\binom{p}{k}b^k p^{k(n-1)} = \\ &= 1 + bp^n + p^{2(n-1)}\sum_{k=2}^{p}\binom{p}{k}b^k p^{(k-2)(n-1)} \equiv 1 + p^{2(n-1)}\sum_{k=2}^{p}\binom{p}{k}b^k p^{(k-2)(n-1)} \equiv \\ &\equiv 1\ (mod\ p^n),\end{aligned}$$

da $n \geq 2 \Rightarrow 2(n-1) = n + n - 2 \geq n$. Insgesamt folgt daraus also die Aussage

$$(\forall\ a \in \mathbb{Z}[i],\ \mathrm{GGT}(p,a) = \mathbb{Z}[i]^\times)\ a^{p^{2n-3}(p^2-1)} \equiv 1\ (mod\ p^n).$$

Sei jetzt $x \in (\mathbb{Z}[i]/\mathbb{Z}[i]p^n)^\times$ und $a \in \mathbb{Z}[i]$ mit $x = \Pi_{p^n}(a)$; dann gilt $\mathrm{GGT}(p^n,a) = \mathbb{Z}[i]^\times$ nach Satz 4.5 und damit klarerweise auch $\mathrm{GGT}(p,a) = \mathbb{Z}[i]^\times$. Zusammen mit der letzten Kongruenz folgt dann

$$x^{p^{2n-3}(p^2-1)} = \Pi_{p^n}(a)^{p^{2n-3}(p^2-1)} = \Pi_{p^n}(a^{p^{2n-3}(p^2-1)}) = 1,$$

was schließlich

$$ord(x) \leq p^{2n-3}(p^2-1) < p^{2n-2}(p^2-1) = N(p)^{n-1}(N(p)-1) = |(\mathbb{Z}[i]/\mathbb{Z}[i]p^n)^\times|$$

liefert. Damit kann also $(\mathbb{Z}[i]/\mathbb{Z}[i]p^n)^\times$ nicht zyklisch sein, da sonst ein $x_0 \in (\mathbb{Z}[i]/\mathbb{Z}[i]p^n)^\times$ mit $\langle x_0\rangle = (\mathbb{Z}[i]/\mathbb{Z}[i]p^n)^\times$ existieren müsste, für das dann aber $ord(x_0) = |\langle x_0\rangle| = |(\mathbb{Z}[i]/\mathbb{Z}[i]p^n)^\times|$ gelten würde - ein Widerspruch zur Ungleichung zuvor. □

Satz 5.6. *Seien $\pi \in \mathfrak{V}$ sowie $n \in \mathbb{N}^+$, dann gilt:*

$(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times$ *ist zyklisch* $\iff n \leq 3$.

Beweis: Seien $\pi \in \mathfrak{V}$ und $n \in \mathbb{N}^+$, dann ist zunächst einmal $\pi\overline{\pi} \in \mathcal{V} = \{2\}$; weiters kann wegen $(1+i)(1-i) = 2$, $1-i = \overline{1+i}$ und $1+i \sim 1-i$ ohne Einschränkung $\pi = 1+i$ angenommen werden.

$\underline{n=1:}$ Mit Satz 5.4 erhält man $|(\mathbb{Z}[i]/\mathbb{Z}[i]\pi)^\times| = \phi_{\mathbb{Z}[i]}(\pi) = N(\pi) - 1 = 2 - 1 = 1$; es folgt sofort $(\mathbb{Z}[i]/\mathbb{Z}[i]\pi)^\times = \{1\} = \langle\Pi_\pi(1)\rangle$. Also ist $(\mathbb{Z}[i]/\mathbb{Z}[i]\pi)^\times$ zyklisch.

$\underline{n=2}$: Aus $\phi_{\mathbb{Z}[i]}(\pi^2) = N(\pi)^1(N(\pi)-1) = 2$ folgt, dass $(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^2)^\times$ eine Gruppe mit 2 Elementen ist; diese wird vom Element $x \neq 1$ erzeugt - wegen $x^1 = x$ und $x^2 = 1$ - und ist daher zyklisch.

$\underline{n=3}$: Hier ist $\pi^n = (1+i)^3 = -2+2i$ und $|(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times| = \phi_{\mathbb{Z}[i]}(\pi^n) = 2^{3-1}(2-1) = 4$; es muss also ein $x \in (\mathbb{Z}[i]/(-2+2i)\mathbb{Z}[i])^\times$ mit $ord(x) = 4$ gefunden werden.

Betrachtet man das Element $\Pi_{\pi^n}(2+i) \in \mathbb{Z}[i]/\mathbb{Z}[i]\pi^n$, so sieht man, dass $1 = (-1)(-2+2i)+i(2+i)$ ist. Nach Korollar 2.4 ist damit $\mathrm{GGT}(-2+2i, 2+i) = \mathbb{Z}[i]^\times$ und somit $\Pi_{\pi^n}(2+i) \in (\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times$ laut Satz 4.5.

Nun wird behauptet, dass $ord(\Pi_{\pi^n}(2+i)) = 4$ gilt, wie man durch Nachrechnen bestätigt:

$$\frac{(2+i)^2-1}{-2+2i} = \frac{(2+4i)(-2-2i)}{8} = \frac{1}{2} - \frac{3}{2}i \notin \mathbb{Z}[i] \;\Rightarrow$$

$$\Rightarrow\; (2+i)^2 - 1 \notin (-2+2i)\mathbb{Z}[i] = ker(\Pi_{\pi^n}) \;\Rightarrow$$

$$\Rightarrow\; \Pi_{\pi^n}(2+i)^2 \neq \Pi_{\pi^n}(1) = 1 \;\Rightarrow$$

$$\Rightarrow\; ord(\Pi_{\pi^n}(2+i)) \neq 2.$$

Insbesondere gilt damit $ord(\Pi_{\pi^n}(2+i)) > 1$, da sonst $\Pi_{\pi^n}(2+i)^2 = 1$ wäre. Da jedoch $ord(\Pi_{\pi^n}(2+i))$ ein Teiler von $|(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times| = 4$ ist, bleibt nur mehr die zuvor behauptete Möglichkeit übrig.

$\underline{n \geq 4}$: Es ist $|(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^{n-2})^\times| = \phi_{\mathbb{Z}[i]}(\pi^{n-2}) = N(\pi)^{n-3}(N(\pi)-1) = 2^{n-3}$ und

$$(\forall\; x \in (\mathbb{Z}[i]/\mathbb{Z}[i]\pi^{n-2})^\times)\; x^{2^{n-3}} = 1,$$

da die Ordnung eines jeden Elements die Gruppenordnung von $(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^{n-2})^\times$ teilt.

Sei $a \in \mathbb{Z}[i]$ beliebig mit $\mathrm{GGT}(\pi, a) = \mathbb{Z}[i]^\times$, dann ist auch $\mathrm{GGT}(\pi^{n-2}, a) = \mathbb{Z}[i]^\times$ und damit $\Pi_{\pi^{n-2}}(a) \in (\mathbb{Z}[i]/\mathbb{Z}[i]\pi^{n-2})^\times$. Zusammen mit dem vorigen Ergebnis ergibt sich

$$\Pi_{\pi^{n-2}}(a^{2^{n-3}}) = \Pi_{\pi^{n-2}}(a)^{2^{n-3}} = 1$$

oder anders formuliert

$$a^{2^{n-3}} \equiv 1\ (mod\ \pi^{n-2}).$$

Das nochmals anders notiert liefert

$$a^{2^{n-3}} = 1 + b\pi^{n-2}$$

mit $b \in \mathbb{Z}[i]$; daraus folgt mittels Potenzieren mit 2 $(= -i\pi^2)$ die Beziehung

$$a^{2^{n-2}} = (1+b\pi^{n-2})^2,$$

aus der man durch Ausquadrieren und der Wahl $b' = -ib \in \mathbb{Z}[i]$ Folgendes erhält:

$$\begin{aligned}(1+b\pi^{n-2})^2 &= 1 + 2b\pi^{n-2} + b^2\pi^{2(n-2)} = \\ &= 1 + b'\pi^n + b^2\pi^{2(n-2)} \equiv \\ &\equiv 1 + b^2\pi^{2(n-2)} \equiv \\ &\equiv 1\ (mod\ \pi^n),\end{aligned}$$

wobei die letzte Kongruenz wegen $n \geq 4 \;\Rightarrow\; 2(n-2) = n+n-4 \geq n$ wahr ist. Somit sieht man die Gültigkeit der folgenden Behauptung:

$$(\forall\; a \in \mathbb{Z}[i],\ \mathrm{GGT}(\pi, a) = \mathbb{Z}[i]^\times)\; a^{2^{n-2}} \equiv 1\ (mod\ \pi^n).$$

Wählt man jetzt $x \in (\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times$ und $a \in \mathbb{Z}[i]$ mit $x = \Pi_{\pi^n}(a)$, so ist $\mathrm{GGT}(\pi^n, a) = \mathbb{Z}[i]^\times$ und damit auch $\mathrm{GGT}(\pi, a) = \mathbb{Z}[i]^\times$, woraus sich zusammen mit der vorigen Behauptung schließlich

$$x^{2^{n-2}} = \Pi_{\pi^n}(a)^{2^{n-2}} = \Pi_{\pi^n}(a^{2^{n-2}}) = 1$$

ergibt. Insgesamt liefert das

$$ord(x) \leq 2^{n-2} < 2^{n-1} = N(\pi)^{n-1}(N(\pi)-1) = |(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times|,$$

womit gezeigt ist, dass $(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times$ nicht zyklisch sein kann, da für ein erzeugendes Element $x_0 \in (\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times$ die Beziehung $\langle x_0\rangle = (\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times$ und damit auch $ord(x_0) = |\langle x_0\rangle| = |(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times|$ gelten müsste, was nach obiger Ungleichung aber nicht möglich ist. $\square$

Satz 5.7. *Seien $\pi \in \mathfrak{U}$ sowie $n \in \mathbb{N}^+$, dann gilt:*

$(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times$ *ist zyklisch.*

Beweis: Da $\pi \in \mathfrak{U}$ ist, gilt $\pi \sim \overline{\pi}$. Seien nun $p \in \mathcal{U}$ mit $p = \pi\overline{\pi}$ und $j : \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ die Inklusion. Definiere $f : \mathbb{Z} \to \mathbb{Z}[i]/\mathbb{Z}[i]\pi^n$ mit $f(a) := \Pi_{\pi^n}(j(a))$, dann ist f ein Ringhomomorphismus, da j und Π_{π^n} Ringhomomorphismen sind; weiters gilt

$$\begin{aligned} ker(f) &= \{a \in \mathbb{Z} \mid \Pi_{\pi^n}(j(a)) = 0\} = \{a \in \mathbb{Z} \mid j(a) \in ker(\Pi_{\pi^n}) = \mathbb{Z}[i]\pi^n\} = \\ &= \{a \in \mathbb{Z} \mid a \in \mathbb{Z}[i]\pi^n\} = \mathbb{Z} \cap \mathbb{Z}[i]\pi^n. \end{aligned}$$

Außerdem ist $\mathbb{Z} \cap \mathbb{Z}[i]\pi^n = p^n\mathbb{Z}$ und daher auch $ker(f) = p^n\mathbb{Z}$, wie im Folgenden gezeigt wird.

$\underline{\supseteq}$: Wegen $p^n\mathbb{Z} \subseteq \mathbb{Z}$ und $p^n\mathbb{Z} = \pi^n\overline{\pi}^n\mathbb{Z} \subseteq \mathbb{Z}[i]\pi^n$, gilt $p^n\mathbb{Z} \subseteq \mathbb{Z} \cap \mathbb{Z}[i]\pi^n$.

$\underline{\subseteq}$: Sei $a \in \mathbb{Z} \cap \mathbb{Z}[i]\pi^n$, dann ist insbesondere $a \in \mathbb{Z}$, weshalb $a = \epsilon \cdot p^k \cdot q_1 \cdot ... \cdot q_m = \epsilon \cdot \pi^k \cdot \overline{\pi}^k \cdot q_1 \cdot ... \cdot q_m$ mit $\epsilon \in \{-1, 1\}$, $k, m \in \mathbb{N}$ und $q_1, ..., q_m \in \mathbb{P}\backslash\{p\}$ ist. Wegen $\pi \mid p$ ergibt sich zusammen mit Satz 3.3 die Aussage $\pi \nmid q_l$ in $\mathbb{Z}[i]$ für alle $l \in \{1, ..., m\}$ und da $\pi \sim \overline{\pi}$ ist, folgt weiters $\pi \nmid \overline{\pi}$ in $\mathbb{Z}[i]$; damit gilt aber auch $\pi \nmid \overline{\pi}^k$ in $\mathbb{Z}[i]$ und klarerweise auch $\pi \nmid \epsilon$ in $\mathbb{Z}[i]$, da π prim in $\mathbb{Z}[i]$ ist. Nach Voraussetzung ist zusätzlich $a \in \mathbb{Z}[i]\pi^n$, womit man $\pi^n \mid a$ in $\mathbb{Z}[i]$ erhält; aus der Überlegung vorhin und der Eindeutigkeit der Primfaktorzerlegung ergibt sich nun $k \geq n$, da sonst $\pi^n \mid a$ in $\mathbb{Z}[i]$ nicht möglich wäre. Somit gilt also $p^n \mid p^k \mid a$ in $\mathbb{Z}$ und damit $a \in p^n\mathbb{Z}$.

Aus dem Homomorphiesatz der Ringtheorie folgt nun die Existenz eines injektiven Ringhomomorphismus $\overline{f} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}[i]/\mathbb{Z}[i]\pi^n$, da ja $p^n\mathbb{Z} = ker(f)$ ist; beachtet man, dass $|\mathbb{Z}/p^n\mathbb{Z}| = p^n = N(\pi)^n = N(\pi^n) = |\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n|$ ist, so ergibt sich aus der Injektivität von $\overline{f}$ auch sofort die Surjektivität und damit die Bijektivität von $\overline{f}$; somit ist $\overline{f}$ ein Ringisomorphismus und folglich

$$\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Dieses $\overline{f}$ induziert nun auch einen Gruppenisomorphismus $f^* : (\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times$; damit gilt also auch

$$(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times \cong (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Da nun mit $p \in \mathcal{U}$ insbesondere $p > 2$ ist, ist $(\mathbb{Z}/p^n\mathbb{Z})^\times$ nach dem *Satz von Gauß* eine zyklische Gruppe, womit auch $(\mathbb{Z}[i]/\mathbb{Z}[i]\pi^n)^\times$ zyklisch ist. □

Lemma 5.8. *Seien $n \in \mathbb{N}^+$, $G_1, ...G_n$ endliche Gruppen, dann sind die folgenden Aussagen äquivalent:*

1. *$G_1 \times ... \times G_n$ ist zyklisch.*
2. *$(\forall\ \nu \in \{1, ..., n\})$ G_ν ist zyklisch und $(\forall\ \nu_1, \nu_2 \in \{1, ..., n\}, \nu_1 \neq \nu_2)$ $\mathrm{ggT}(|G_{\nu_1}|, |G_{\nu_2}|) = 1$.*

Beweis: $\underline{1. \Rightarrow 2.}$: Angenommen *2.* ist falsch, dann ist die Negation von *1.* zu zeigen.

Fall 1: Sei $\nu \in \{1, ..., n\}$, sodass G_ν nicht zyklisch ist; ohne Einschränkung sei $\nu = 1$, das heißt

$$(\forall\ \overline{g} \in G_1)(\exists\ \overline{h} \in G_1)(\forall\ k \in \mathbb{N}^+)\ \overline{h} \neq \overline{g}^k.$$

Sei nun $g = (g_1, ..., g_n) \in G_1 \times ... \times G_n$ beliebig, dann gibt es ein $h_1 \in G_1$, sodass $h_1 \neq g_1^k$ ist für alle $k \in \mathbb{N}^+$ und somit ist (mit komponentenweiser Verknüpfung) $(h_1, 1, ..., 1) \neq g^k$ für alle $k \in \mathbb{N}^+$, womit g kein erzeugendes Element von $G_1 \times ... \times G_n$ ist. Da $g \in G_1 \times ... \times G_n$ beliebig gewählt war, kann $G_1 \times ... \times G_n$ daher nicht zyklisch sein.

Fall 2: Seien jetzt $n \geq 2$ und $\nu_1, \nu_2 \in \{1, ..., n\}$, $\nu_1 \neq \nu_2$ mit $\mathrm{ggT}(|G_{\nu_1}|, |G_{\nu_2}|) > 1$; ohne Einschränkung seien $\nu_1 = 1$ und $\nu_2 = 2$. Wählt man nun $g = (g_1, g_2) \in G_1 \times G_2$ beliebig, dann ist $g_1^{|G_1|} = 1_{G_1}$ und $g_2^{|G_2|} = 1_{G_2}$ und folglich $g^{\mathrm{kgV}(|G_1|,|G_2|)} = (g_1^{\mathrm{kgV}(|G_1|,|G_2|)}, g_2^{\mathrm{kgV}(|G_1|,|G_2|)}) = (1, 1) = 1$; wegen $\mathrm{ggT}(|G_1|, |G_2|) > 1$ ergibt sich aber

$$ord(g) \leq \mathrm{kgV}(|G_1|, |G_2|) = \frac{|G_1| \cdot |G_2|}{\mathrm{ggT}(|G_1|, |G_2|)} < |G_1| \cdot |G_2| = |G_1 \times G_2|.$$

Damit kann g kein erzeugendes Element sein, denn sonst müsste $ord(g) = |\langle g \rangle| = |G_1 \times G_2|$ gelten; da $g \in G_1 \times G_2$ beliebig gewählt war, kann $G_1 \times G_2$ somit nicht zyklisch sein, was für $n = 2$ den Fall erledigt.

Für $n \geq 3$ gilt zunächst klarerweise

$$G_1 \times ... \times G_n \cong (G_1 \times G_2) \times G_3 \times ... \times G_n$$

und da nun die erste Gruppe des Produktes auf der rechten Seite nicht zyklisch ist, folgt mittels Fall 1, dass $(G_1 \times G_2) \times G_3 \times ... \times G_n$ nicht zyklisch und schließlich auch $G_1 \times ... \times G_n$ nicht zyklisch ist.

2. $\Rightarrow$ 1.: Diese Implikation wird mittels vollständiger Induktion nach n bewiesen.

$n = 1$: Dann gilt *2. $\Rightarrow$ 1.* trivialerweise.

$n = 2$: Seien $m_1, m_2 \in \mathbb{N}^+$ mit $m_1 = |G_1|$ und $m_2 = |G_2|$. Aus dem *Struktursatz für zyklische Gruppen* erhält man $G_1 \cong \mathbb{Z}/m_1\mathbb{Z}$ sowie $G_2 \cong \mathbb{Z}/m_2\mathbb{Z}$ und mittels *chinesischem Restsatz* auch $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \cong \mathbb{Z}/m_1m_2\mathbb{Z}$ wegen $\mathrm{ggT}(m_1, m_2) = 1$. Insgesamt heißt das also

$$G_1 \times G_2 \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \cong \mathbb{Z}/m_1m_2\mathbb{Z},$$

womit gezeigt ist, dass $G_1 \times G_2$ zyklisch ist, da ja $\mathbb{Z}/m_1m_2\mathbb{Z}$ zyklisch ist.

$n \geq 3$: Sei die Implikation *2. $\Rightarrow$ 1.* für $n-1$ gezeigt. Aus der Voraussetzung folgt insbesondere, dass jedes G_ν zyklisch ist mit $\nu \in \{1, ..., n-1\}$ und $\mathrm{ggT}(|G_{\nu_1}|, |G_{\nu_2}|) = 1$ ist für alle $\nu_1, \nu_2 \in \{1, ..., n-1\},\ \nu_1 \neq \nu_2$; also erhält man nach Induktionsannahme, dass $G_1 \times ... \times G_{n-1}$ zyklisch ist. Da

$$G_1 \times ... \times G_n \cong (G_1 \times ... \times G_{n-1}) \times G_n$$

ist und wegen $\mathrm{ggT}(|G_\nu|, |G_n|) = 1$ für alle $\nu \in \{1, ..., n-1\}$ auch $\mathrm{ggT}(|G_1 \times ... \times G_{n-1}|, |G_n|) = \mathrm{ggT}(|G_1| \cdot ... \cdot |G_{n-1}|, |G_n|) = 1$ gilt, folgt mithilfe des Falles $n = 2$ die Zyklizität von $(G_1 \times ... \times G_{n-1}) \times G_n$ und damit jene von $G_1 \times ... \times G_n$, was den Induktionsbeweis abschließt. □

Satz 5.9. *Sei $a \in \mathbb{Z}[i]$, dann ist $(\mathbb{Z}[i]/\mathbb{Z}[i]a)^\times$ genau in den folgenden Fällen zyklisch:*

1. $a \in \{0, 1, i, -1, -i\}$.
2. $a \sim (1+i)^n$ *mit* $n \in \mathbb{N}^+$ *und* $n \leq 3$.
3. $a \sim \pi$ *mit* $\pi \in \mathfrak{T}$.
4. $a \sim \pi^n$ *mit* $\pi \in \mathfrak{U}$ *und* $n \in \mathbb{N}^+$.
5. $a \sim (1+i)\pi$ *mit* $\pi \in \mathfrak{T}$.
6. $a \sim (1+i)\pi^n$ *mit* $\pi \in \mathfrak{U}$ *und* $n \in \mathbb{N}^+$.

Beweis: Sei $a \in \mathbb{Z}[i]$, dann sind die folgenden 3 Fälle möglich.

Fall 1: $a = 0$: Wegen $\mathbb{Z}[i]/\mathbb{Z}[i]a \cong \mathbb{Z}[i]$ ist $(\mathbb{Z}[i]/\mathbb{Z}[i]a)^\times \cong \mathbb{Z}[i]^\times = \langle i \rangle$ und damit zyklisch.

Fall 2: $a \in \mathbb{Z}[i]^\times$: Aus $\mathbb{Z}[i]/\mathbb{Z}[i]a = \mathbb{Z}[i]/\mathbb{Z}[i] \cong \{0\}$ folgt, dass $(\mathbb{Z}[i]/\mathbb{Z}[i]a)^\times \cong \{0\}^\times = \{0\} = \langle 0 \rangle$ ist; also ist $(\mathbb{Z}[i]/\mathbb{Z}[i]a)^\times$ auch in diesem Fall zyklisch.

Fall 3: $a \notin \{0\} \cup \mathbb{Z}[i]^\times$: Nach Satz 3.15 besitzt a eine eindeutige Darstellung in der Form

$$a = \epsilon \cdot \pi_1^{\alpha_1} \cdot ... \cdot \pi_m^{\alpha_m}$$

mit $\epsilon \in \mathbb{Z}[i]^\times, m \in \mathbb{N}^+,\ \pi_1, ..., \pi_m \in \mathfrak{P}$ und $\alpha_1, ..., \alpha_m \in \mathbb{N}^+$.

Seien nun $\pi, \pi' \in \mathfrak{P}$ mit $\pi \neq \pi'$ und $k, l \in \mathbb{N}^+$, dann ist $\mathrm{GGT}(\pi, \pi') = \mathbb{Z}[i]^\times$, da π und π' prim und nicht assoziiert sind; damit ist nun auch $\mathrm{GGT}(\pi^k, \pi'^l) = \mathbb{Z}[i]^\times$ laut Satz 2.5. Weiters erhält man daraus mit Korollar 2.4 die Beziehung $1 \in \mathbb{Z}[i]\pi^k + \mathbb{Z}[i]\pi'^l$ und schließlich $\mathbb{Z}[i]\pi^k + \mathbb{Z}[i]\pi'^l = \mathbb{Z}[i]$, was gleichbedeutend damit ist, dass die Ideale $\mathbb{Z}[i]\pi^k$ und $\mathbb{Z}[i]\pi'^l$ teilerfremd sind. Mit dieser Überlegung ergibt sich zusammen mit dem *chinesischen Restsatz*

$$\mathbb{Z}[i]/\mathbb{Z}[i]a = \mathbb{Z}[i]/\mathbb{Z}[i]\ \epsilon \cdot \pi_1^{\alpha_1} \cdot ... \cdot \pi_m^{\alpha_m} = \mathbb{Z}[i]/\mathbb{Z}[i]\pi_1^{\alpha_1} \cdot ... \cdot \mathbb{Z}[i]\pi_m^{\alpha_m} \cong \mathbb{Z}[i]/\mathbb{Z}[i]\pi_1^{\alpha_1} \times ... \times \mathbb{Z}[i]/\mathbb{Z}[i]\pi_m^{\alpha_m}$$

und damit auch

$$(\mathbb{Z}[i]/\mathbb{Z}[i]a)^\times \cong (\mathbb{Z}[i]/\mathbb{Z}[i]\pi_1^{\alpha_1} \times ... \times \mathbb{Z}[i]/\mathbb{Z}[i]\pi_m^{\alpha_m})^\times = (\mathbb{Z}[i]/\mathbb{Z}[i]\pi_1^{\alpha_1})^\times \times ... \times (\mathbb{Z}[i]/\mathbb{Z}[i]\pi_m^{\alpha_m})^\times.$$

Fall 3.1: $m = 1$: Gemäß den Sätzen 5.5, 5.6 und 5.7 ist $(\mathbb{Z}[i]/\mathbb{Z}[i]a)^\times$ genau dann zyklisch, wenn einer der Punkte *2.*, *3.* oder *4.* eintritt; die Einheit ϵ spielt dabei keine Rolle.

Fall 3.2: $m \geq 2$: Da

$$(\mathbb{Z}[i]/\mathbb{Z}[i]a)^\times \cong (\mathbb{Z}[i]/\mathbb{Z}[i]\pi_1^{\alpha_1})^\times \times ... \times (\mathbb{Z}[i]/\mathbb{Z}[i]\pi_m^{\alpha_m})^\times$$

ist, muss als notwendige Voraussetzung für die Zyklizität von $(\mathbb{Z}[i]/\mathbb{Z}[i]a)^\times$ jedes einzelne $(\mathbb{Z}[i]/\mathbb{Z}[i]\pi_\mu^{\alpha_\mu})^\times$ zyklisch sein; damit bleiben für $\mu \in \{1, ..., m\}$ nur mehr die Möglichkeiten $\pi_\mu \in \mathfrak{T} \ \wedge \ \alpha_\mu = 1$, $\pi_\mu \in \mathfrak{V} \ \wedge \ \alpha_\mu \leq 3$ und $\pi_\mu \in \mathfrak{U} \ \wedge \ \alpha_\mu \in \mathbb{N}^+$. Weiters müssen für die Zyklizität von $(\mathbb{Z}[i]/\mathbb{Z}[i]a)^\times$ auch die Gruppenordnungen $\phi_{\mathbb{Z}[i]}(\pi_\mu^{\alpha_\mu})$ aller Gruppen $(\mathbb{Z}[i]/\mathbb{Z}[i]\pi_\mu^{\alpha_\mu})^\times$ paarweise teilerfremd sein; für $\mu \in \{1, ..., m\}$ sei $p_\mu \in \mathbb{P}$ die nach Satz 3.3 eindeutig bestimmte Primzahl mit $\pi_\mu \mid p_\mu$, dann erhält man zusammen mit Proposition 3.8:

- $\pi_\mu \in \mathfrak{T} \ \Rightarrow \ \phi_{\mathbb{Z}[i]}(\pi_\mu^{\alpha_\mu}) = N(\pi_\mu)^{\alpha_\mu - 1}(N(\pi_\mu) - 1) = p_\mu^{2(\alpha_\mu - 1)}(p_\mu^2 - 1) \in 2\mathbb{N}^+$, wegen $p_\mu \neq 2$.
- $\pi_\mu \in \mathfrak{V} \ \Rightarrow \ \phi_{\mathbb{Z}[i]}(\pi_\mu^{\alpha_\mu}) = N(\pi_\mu)^{\alpha_\mu - 1}(N(\pi_\mu) - 1) = p_\mu^{\alpha_\mu - 1}(p_\mu - 1) = 2^{\alpha_\mu - 1}$, wegen $p_\mu = 2$.
- $\pi_\mu \in \mathfrak{U} \ \Rightarrow \ \phi_{\mathbb{Z}[i]}(\pi_\mu^{\alpha_\mu}) = N(\pi_\mu)^{\alpha_\mu - 1}(N(\pi_\mu) - 1) = p_\mu^{\alpha_\mu - 1}(p_\mu - 1) \in 2\mathbb{N}^+$, wegen $p_\mu \neq 2$.

Man erkennt, dass in der Primfaktorzerlegung von a höchstens ein träges oder unverzweigtes Primelement auftreten kann; als zweites Primelement ist dazu nur $1 + i$ möglich, da sowohl $\phi_{\mathbb{Z}[i]}((1 + i)^2)$ als auch $\phi_{\mathbb{Z}[i]}((1 + i)^3)$ gerade ist, womit die Ordnungen der beiden auftretenden Gruppen nicht mehr teilerfremd wären. Dies entspricht den Punkten *5.* und *6.* und ist laut Lemma 5.8 auch eine hinreichende Bedingung für die Zyklizität von $(\mathbb{Z}[i]/\mathbb{Z}[i]a)^\times$. □

Literatur

[1] Bundschuh, Peter: *Einführung in die Zahlentheorie.* 6., überarb. und aktualisierte Aufl. Berlin, Heidelberg : Springer, 2008

[2] Frey, Gerhard: *Elementare Zahlentheorie.* Braunschweig, Wiesbaden : Vieweg, 1984

[3] Remmert, Reinhold ; Ullrich, Peter: *Elementare Zahlentheorie.* 2., korrigierte Aufl. Basel, Boston, Berlin : Birkhäuser, 1995