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

Stefan Rosenberger

Betreuer: Dr.rer.nat. Florian Kainrath

3. November 2010

Inhaltsverzeichnis

1 Grundlegende Eigenschaften von $\mathbb{Z}[\omega]$

Der Ring $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$, mit $\omega = \frac{-1+i\sqrt{3}}{2}$, ist ein Unterring der komplexen Zahlen $\mathbb{C}$. Als solcher ist $\mathbb{Z}[\omega]$ sogar ein Integritätsbereich, in dem jedes $x \in \mathbb{Z}[\omega]$ eine eindeutige Darstellung $x = a+b\omega$ mit $a, b \in \mathbb{Z}$ hat.
Speziell ist ω eine Nullstelle des Polynoms $P(X) = X^2 + X + 1$. Für ein $z \in \mathbb{C}$ sei wie üblich $\overline{z}$ das Komplex-konjungierte von z.

Lemma 1.1. *Es gilt:*

1. $\omega^2 = -\omega - 1 = \overline{\omega}$
2. $\omega \cdot \overline{\omega} = 1$

Beweis. 1. Wegen $\omega^2 + \omega + 1 = 0$ folgt unmittelbar: $\omega^2 = -\omega - 1 = \frac{+1-i\sqrt{3}}{2} - 1 = \frac{-1-i\sqrt{3}}{2} = \overline{\omega}$.

2. $\omega \cdot \overline{\omega} = (\frac{-1+i\sqrt{3}}{2})\overline{(\frac{-1+i\sqrt{3}}{2})} = (\frac{-1+i\sqrt{3}}{2})(\frac{-1-i\sqrt{3}}{2}) = \frac{1}{4}(1 - i\sqrt{3} + i\sqrt{3} + 3) = 1$

□

Lemma 1.2. *Sei* $D = \{r + s\omega | r, s \in \mathbb{Q}\}$ *und*

$$N : \begin{cases} D \to \mathbb{Q}_{\geq 0} \\ x \mapsto x \cdot \overline{x} \end{cases}$$

dann gelten:

1. $N(x) = 0 \iff x = 0$
2. *Für die Abbildung* N *gilt* $N(1) = 1$*, und für alle* $x, y \in D$ *gilt* $N(xy) = N(x)N(y)$.
   Für die Einschränkung von N *auf* $\mathbb{Z}[\omega]$ *gilt dass*

   $$N|_{\mathbb{Z}[\omega]} : \begin{cases} \mathbb{Z}[\omega] \to \mathbb{N} \\ x \mapsto x \cdot \overline{x} \end{cases}$$

   ein Halbgruppenhomomorphismus ist.
3. *Für* $x \in \mathbb{Z}[\omega]$ *gilt:* $N(x) = 1 \iff x \in \mathbb{Z}[\omega]^\times$.
4. *Es gibt kein* $x \in \mathbb{Z}[\omega]$ *sodass* $N(x) = 2$ *gilt.*

Beweis. Für $x \in D$ seien $r, s \in \mathbb{Q}$ sodass $x = r + s\omega$ gilt. Dann folgt $N(x) = x\overline{x} = (r + s\omega)\overline{(r + s\omega)} = (r + s\omega)(r + s\overline{\omega}) = r^2 + rs\overline{\omega} + rs\omega + s^2\overline{\omega}\omega = r^2 + rs(\omega^2 + \omega) + s^2 = r^2 - sr + s^2$, womit $N(x) \in \mathbb{Q}$ folgt. Wegen $N(x) = x\overline{x} = |x| \geq 0$ folgt dass $N(x) \in \mathbb{Q}_{\geq 0}$.

1. Sei $x \in D$.
   $N(x) = x\overline{x} = 0 \iff x = 0$ oder $\overline{x} = 0 \iff x = 0$
2. $N(1) = \overline{1} \cdot 1 = 1$
   Seien nun $x, y \in D$. Dann gilt $N(xy) = (xy)\overline{(xy)} = xy\overline{x}\overline{y} = x\overline{x}y\overline{y} = N(x)N(y)$.
   Sei nun $x \in \mathbb{Z}[\omega]$, sodass $x = a + b\omega$ mit $a, b \in \mathbb{Z}$ gilt. Dann folgt $N(x) = a^2 - ab + b^2 \in \mathbb{N}$, und damit die Behauptung.
3. " $\Rightarrow$ " Sei $x \in \mathbb{Z}[\omega]$ mit $N(x) = 1$, dann folgt $x\overline{x} = \overline{x}x = 1$
   Somit ist $\overline{x}$ inverses Element von x, und daher gilt $x \in \mathbb{Z}[\omega]^\times$.
   " $\Leftarrow$ " Sei nun $x \in \mathbb{Z}[\omega]^\times$. Dann gibt es ein $y \in \mathbb{Z}[\omega]^\times$ sodass gilt: $xy = 1 \Rightarrow x\overline{x}\overline{y}y = 1 \Rightarrow N(x)N(y) = 1$.
   Wie in 2 gezeigt, ist $N(y)$ eine positive natürliche Zahl, womit $N(x) = 1$ gilt.
4. Angenommen es gibt ein $x \in \mathbb{Z}[\omega]$, sodass $N(x) = 2$ und $x = a + b\omega$, mit $a, b \in \mathbb{Z}$, gilt.
   Dann folgt $2 = a^2 - ab + b^2$. Das ist gleichbedeutend mit $8 = 4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2$.
   Falls $|b| \geq 2$ gelten würde, so folgt $3b^2 > 8$, was nicht sein kann. Also bleiben die Fälle $b = \pm 1$ und $b = 0$ zu betrachten.

1.Fall) Sei $b = 0$ so folgt $(2a)^2 = 8$. Da 8 in $\mathbb{Z}$ jedoch kein Quadrat ist, kann das nicht sein.

2.Fall) Sei $b = \pm 1$ so folgt $(2a \pm 1)^2 + 3 = 8$ und daher $(2a \pm 1)^2 = 5$. Auch 5 ist in $\mathbb{Z}$ kein Quadrat, womit dieser Fall nicht zutreffend sein kann.

Widerspruch.

□

Lemma 1.3. *Sei $x \in \mathbb{Z}[\omega]$, sodass $x = a + b\omega$ mit $a, b \in \mathbb{Z}$ gilt. Dann gelten*

1. $\overline{x} = a - b - b\omega \in \mathbb{Z}[\omega]$.
2. $\mathbb{Z}[\omega]^\times = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.
3. $\mathbb{Z}[\omega]^\times$ *ist zyklisch.*
4. *Die Abbildung*

$$g : \begin{cases} \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega] \\ x \longmapsto \overline{x} \end{cases}$$

ist ein Ringisomorphismus.

Beweis. 1. Sei $x \in \mathbb{Z}[\omega]$ sodass $x = a + b\omega$ mit $a, b \in \mathbb{Z}$. Dann gilt:
$\overline{x} = \overline{a + b\omega} = a + b\overline{\omega} = a + b(-\omega - 1) = a - b - b\omega \in \mathbb{Z}[\omega]$.

2. z.z.: $\mathbb{Z}[\omega]^\times \subset \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$
Sei $x = a + b\omega \in \mathbb{Z}[\omega]^\times$. Dann gilt: $1 = a^2 - ab + b^2$ bzw. $4 = 4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2$.
Hierfür gibt es zwei mögliche Lösungen:
(a) $2a - b = \pm 1$ und $b = \pm 1$
(b) $2a - b = \pm 2$ und $b = 0$
(denn würde $|b| > 1$ gelten so würde $3b^2 > 4$ folgen)
Somit sind sechs Fälle zu betrachten, welche einfach nachzurechnen sind:

1.Fall Sei $2a - b = 1$ und $b = 1 \Rightarrow 2a - 1 = 1 \Rightarrow a = 1$
$\Rightarrow x = 1 + \omega$ und mit $\omega^2 + \omega + 1 = 0$ folgt $x = -\omega^2$.

2.Fall Sei $2a - b = 1$ und $b = -1$
$\Rightarrow 2a + 1 = 1 \Rightarrow 2a = 0 \Rightarrow a = 0 \Rightarrow x = -\omega$.

3.Fall Sei $2a - b = -1$ und $b = 1$
$\Rightarrow 2a - 1 = -1 \Rightarrow 2a = 0 \Rightarrow a = 0 \Rightarrow x = \omega$.

4.Fall Sei $2a - b = -1$ und $b = -1$
$\Rightarrow 2a + 1 = -1 \Rightarrow 2a = -2 \Rightarrow a = -1 \Rightarrow x = -1 - \omega = \omega^2$.

5.Fall Sei $2a - b = 2$ und $b = 0$
$\Rightarrow 2a = 2 \Rightarrow a = 1 \Rightarrow x = 1$.

6.Fall Sei $2a - b = -2$ und $b = 0$
$\Rightarrow 2a = -2 \Rightarrow a = -1 \Rightarrow x = -1$.

Womit folgt $\mathbb{Z}[\omega]^\times \subset \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.

z.z.: $\{1, -1, \omega, -\omega, \omega^2, -\omega^2\} \subset \mathbb{Z}[\omega]^\times$
$\mathbb{Z}[\omega]^\times$ ist eine Gruppe, und nach 1.1 gilt: $-1, \omega \in \mathbb{Z}[\omega]^\times$. Daher folgt die Behauptung.

Und somit gilt $\mathbb{Z}[\omega]^\times = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.

3. z.z.: $\mathbb{Z}[\omega]^\times = \langle -\omega \rangle$
Für $-\omega \in \mathbb{Z}[\omega]^\times$ gilt mit 1.1

- $(-\omega)^2 = \omega^2$.
- $(-\omega)^3 = -\omega \cdot \omega^2 = -1$.
- $(-\omega)^4 = -1 \cdot (-\omega) = \omega$.
- $(-\omega)^5 = \omega \cdot (-\omega) = -\omega^2$.
- $(-\omega)^6 = (-\omega^2) \cdot (-\omega) = 1$.

Somit wird $\mathbb{Z}[\omega]^\times$ von $-\omega$ erzeugt.

4. Aus den bekannten Eigenschaften von $\bar{\cdot}$ folgt, dass g ein Ringhomomorphismus ist mit $g \circ g = id$. Daraus resultiert die Behauptung.

□

Definition 1.4. Seien $n, m \in \mathbb{Z}[\omega]$

1. m heißt **assoziiert** zu n falls es ein $\nu \in \mathbb{Z}[\omega]^\times$ gibt sodass $\nu m = n$ gilt. Dann schreiben wir $m \sim n$.
2. m heißt **Teiler** von n falls es ein $x \in \mathbb{Z}[\omega]$ gibt sodass $mx = n$ gilt. In diesem Fall sagen wir m teilt n und schreiben $m|n$.
3. m heißt **echter Teiler** von n, falls m Teiler von n ist, und m weder Einheit noch zu n assoziiert ist.
4. Sei $n \in \mathbb{Z}[\omega] \setminus (\mathbb{Z}[\omega]^\times \cup \{0\})$.
   n heißt **Primelement** falls n keinen echten Teiler hat.

Lemma 1.5. *Assoziiertheit ist eine Äquivalenzrelation auf $\mathbb{Z}[\omega]$.*
Insbesondere gilt für $x \in \mathbb{Z}[\omega]$ genau dann $x \sim 1$, wenn $x \in \mathbb{Z}[\omega]^\times$ ist.

Beweis. Seien $x, y, z \in \mathbb{Z}[\omega]$.

reflexiv: Es gilt $1 \in \mathbb{Z}[\omega]^\times$, und somit $1 \cdot x = x$ womit $x \sim x$ gilt.

symmetrisch: Sei $x \sim y$, dann existiert ein $\nu \in \mathbb{Z}[\omega]^\times$ sodass $\nu x = y$. Das ist gleichbedeutend mit $x = \nu^{-1} y$, und wegen $\nu^{-1} \in \mathbb{Z}[\omega]^\times$ folgt $y \sim x$.

transitiv: Sei $x \sim y$ und $y \sim z$ dann existieren $\nu, \eta \in \mathbb{Z}[\omega]^\times$ sodass $\nu x = y$ und $\eta y = z$. Womit $\nu x = \eta^{-1} z$ folgt und daher $\eta \nu x = z$ gilt. Wegen $\eta\nu \in \mathbb{Z}[\omega]^\times$ folgt $x \sim z$.

Sei nun $x \in \mathbb{Z}[\omega]$ sodass $x \sim 1$ gilt. Dann existiert ein $\nu \in \mathbb{Z}[\omega]^\times$ sodass $x\nu = 1$. Womit $x \in \mathbb{Z}[\omega]^\times$ folgt. Andererseits ist $x \in \mathbb{Z}[\omega]^\times$, so ist auch $x^{-1} \in \mathbb{Z}[\omega]^\times$ und es gilt $xx^{-1} = 1$. Und daher folgt $x \sim 1$. □

Lemma 1.6. *Seien $a, b \in \mathbb{Z}[\omega]$. Dann gelten:*

1. *$b|a \iff a\mathbb{Z}[\omega] \subset b\mathbb{Z}[\omega]$*
2. *$a \sim b \iff a|b$ und $b|a \iff a\mathbb{Z}[\omega] = b\mathbb{Z}[\omega]$*
3. *b ist ein echter Teiler von $a \iff a\mathbb{Z}[\omega] \subsetneq b\mathbb{Z}[\omega] \subsetneq \mathbb{Z}[\omega]$*
4. *Sei a prim und $b|a$ dann gilt $b \sim a$ oder $b \sim 1$.*

Beweis. Seien $a, b \in \mathbb{Z}[\omega]$.

1. **"⇒"** Gelte $b|a$, dann gibt es ein $q \in \mathbb{Z}[\omega]$ sodass $a = bq$ gilt.
   Sei nun $x \in a\mathbb{Z}[\omega]$, dann existiert ein $p \in \mathbb{Z}[\omega]$ sodass $x = ap = bqp \in b\mathbb{Z}[\omega]$. Damit folgt $a\mathbb{Z}[\omega] \subset b\mathbb{Z}[\omega]$.

   "⇐" Es gelte nun $a\mathbb{Z}[\omega] \subset b\mathbb{Z}[\omega]$.
   Dann folgt $a \in b\mathbb{Z}[\omega]$ also gibt es ein $q \in \mathbb{Z}[\omega]$ sodass $a = bq$. Womit b teilt a gilt.

2. Falls $a = 0$ oder $b = 0$ gilt ist die Aussage klar, seien also nun $a \neq 0$ und $b \neq 0$.

   $a \sim b \Rightarrow a|b$ **und** $b|a$**:**
   Sei $a \sim b$. Dann gibt es ein $x \in \mathbb{Z}[\omega]^\times$ sodass $bx = a$. Womit $b = ax^{-1}$ folgt und daher $a|b$ und $b|a$ gilt.

   $a|b$ und $b|a \Rightarrow a\mathbb{Z}[\omega] = b\mathbb{Z}[\omega]$:
   Folgt unmittelbar aus 1.

$a\mathbb{Z}[\omega] = b\mathbb{Z}[\omega] \Rightarrow a \sim b$:
Sei $a\mathbb{Z}[\omega] = b\mathbb{Z}[\omega]$. Da $a \in b\mathbb{Z}[\omega]$ und $b \in a\mathbb{Z}[\omega]$ gilt, gibt es $c, d \in \mathbb{Z}[\omega]$ sodass $a = cb$ und $b = da$. Damit folgt $a = cb = cda$. Wegen $a \in \mathbb{C} \setminus \{0\}$ gilt $1 = cd = dc$, und daher $c, d \in \mathbb{Z}[\omega]^\times$ gilt. Womit $a \sim b$ folgt.

3. Da b ein echter Teiler von a ist gilt insbesondere $b \neq 0$, $b \neq 1$ und $a \nsim b$.
Nach 2 folgt dass $a \nsim b \Leftrightarrow a\mathbb{Z}[\omega] \neq b\mathbb{Z}[\omega]$.
Nach 1 gilt auch $a\mathbb{Z}[\omega] \subset b\mathbb{Z}[\omega]$. Wegen $1 \in \mathbb{Z}[\omega]$ folgt nun $b\mathbb{Z}[\omega] \subsetneq \mathbb{Z}[\omega]$.
Damit folgt die Aussage.

4. Da a prim ist und $b|a$ gilt, folgt $b \in \mathbb{Z}[\omega]^\times$ oder $b \sim a$. Falls $b \in \mathbb{Z}[\omega]^\times$ ist, so folgt die Behauptung mit 1.5.

□

Lemma 1.7. *Seien $x, y \in \mathbb{Z}[\omega]$ und $y \neq 0$. Dann existieren $\gamma, \rho \in \mathbb{Z}[\omega]$ mit $x = \gamma y + \rho$ und $N(\rho) < N(y)$. Dabei ist N die eingeschränkte Abbildung aus 1.2.*

Beweis. Seien $x, y \in \mathbb{Z}[\omega]$ mit $y \neq 0$ womit $N(y) > 0$ gilt, und $D = \{r + s\omega | r, s \in \mathbb{Q}\}$. Dann folgt

$$\frac{x}{y} = \frac{x\overline{y}}{y\overline{y}} = \frac{x\overline{y}}{N(y)} =: r + s\omega \in D.$$

Dabei sind r, s rationale Zahlen. Insbesondere existieren $m, n \in \mathbb{Z}$ mit $|r - m| \leq \frac{1}{2}$ und $|s - n| \leq \frac{1}{2}$.
Setze nun $\gamma = m + n\omega \in \mathbb{Z}[\omega]$. Dann gilt $N(\frac{x}{y} - \gamma) = (r-m)^2 - (r-m)(s-n) + (s-n)^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1$.
Sei nun $\rho = x - \gamma y \in \mathbb{Z}[\omega]$. Dann folgt $N(\rho) = N(x - \gamma y) = N(y(\frac{x}{y} - \gamma)) = N(y)N(\frac{x}{y} - \gamma) < N(y)$. □

Proposition 1.8. *$\mathbb{Z}[\omega]$ ist ein Hauptidealring.*

Beweis. Sei $I \subset \mathbb{Z}[\omega]$ ein Ideal. Da $\{0\}$ in jedem Ring ein Hauptideal ist, sei ohne Einschränkung $I \neq \{0\}$.
Damit gilt $I \setminus \{0\} \neq \emptyset$. Daher gibt es ein $x \in I$ sodass $N(x) = \min\{N(a) | a \in I \setminus \{0\}\}$ ist.
Behauptung: $I = x\mathbb{Z}[\omega]$.
Zeige zuerst $x\mathbb{Z}[\omega] \subset I$. Dies ist jedoch klar, denn I ist ein Ideal und $x \in I$. Daher gilt für alle $y \in \mathbb{Z}[\omega]$ dass $xy \in I$ ist. Woraus $x\mathbb{Z}[\omega] \subset I$ folgt.
Sei nun umgekehrt $y \in I$. Wie in 1.7 gezeigt existieren $a, b \in \mathbb{Z}[\omega]$, sodass $y = ax + b$ und $N(b) < N(x)$ gilt. Damit folgt $b = y - ax \in I$ denn $x, y \in I$.
Falls $b \neq 0$ gilt, so ist $N(x)$ nicht das Minimum von $\{N(a) | a \in I \setminus \{0\}\}$ (wegen $b \in I$), was nicht sein kann.
Daher gilt $b = 0$, womit folgt $y = ax \in x\mathbb{Z}[\omega]$, und daher $I \subset x\mathbb{Z}[\omega]$.

□

Satz 1.9. *Für jedes prime Element $n \in \mathbb{Z}[\omega]$ gilt, falls $n|n_1n_2$ mit $n_1, n_2 \in \mathbb{Z}[\omega]$ so folgt $n|n_1$ oder $n|n_2$.*

Beweis. Sei $n \in \mathbb{Z}[\omega]$ ein primes Element und $n_1, n_2 \in \mathbb{Z}[\omega]$ sodass $n|n_1n_2$.
Betrachte das Ideal $J := n\mathbb{Z}[\omega] + n_1\mathbb{Z}[\omega]$.
Da $\mathbb{Z}[\omega]$ nach 1.8 ein Hauptidealring ist, gibt es ein $d \in \mathbb{Z}[\omega]$ sodass $J = d\mathbb{Z}[\omega]$. Da n prim ist gilt $n \neq 0$ und damit $d \neq 0$.
Somit folgt $J = d\mathbb{Z}[\omega] = n\mathbb{Z}[\omega] + n_1\mathbb{Z}[\omega]$. Daher gilt $n\mathbb{Z}[\omega] \subset d\mathbb{Z}[\omega]$, und mit 1.6 folgt $d|n$.
Da n prim ist hat n keinen echten Teiler, womit gilt $d \sim n$ oder $d \sim 1$.

1.Fall $d \sim n$
Dann gilt $n\mathbb{Z}[\omega] = d\mathbb{Z}[\omega] \supset n_1\mathbb{Z}[\omega]$. Mit 1.6 folgt $n|n_1$.

2.Fall $d \sim 1$
Dann gilt $\mathbb{Z}[\omega] = n\mathbb{Z}[\omega] + n_1\mathbb{Z}[\omega]$. Daher gibt es $x, y \in \mathbb{Z}[\omega]$ sodass $1 = nx + n_1y$.
Daraus folgt $n_2 = n(n_2x) + (n_1n_2)y$, und wegen $n|n_1n_2$ folgt $n|n_2$.

Womit schließlich gilt $n|n_1$ oder $n|n_2$. □

Satz 1.10. *Jedes Element $x \in \mathbb{Z}[\omega] \setminus (\mathbb{Z}[\omega]^\times \cup \{0\})$ besitzt eine bis auf Assoziiertheit und Reihenfolge eindeutige Darstellung als Produkt endlich vieler Primelemente.*

Beweis.

Existenz

Sei $x \in \mathbb{Z}[\omega] \setminus (\mathbb{Z}[\omega]^\times \cup \{0\})$. Mit 1.2 folgt $N(x) \geq 3$, und es gilt $N(1-\omega) = 3$. Beweis durch Induktion nach $N(x)$.
Sei die Behauptung für alle $x' \in \mathbb{Z}[\omega] \setminus (\mathbb{Z}[\omega]^\times \cup \{0\})$, mit $N(x') < N(x)$ wahr.
Falls $x \in \mathbb{Z}[\omega]$ prim ist, so folgt die Behauptung. Sei nun $x \in \mathbb{Z}[\omega]$ nicht prim.
Dann existieren $x', x'' \in \mathbb{Z}[\omega] \setminus (\mathbb{Z}[\omega]^\times \cup \{0\})$ sodass $x = x'x''$ gilt. Es folgt $N(x) = N(x'x'') = N(x')N(x'')$, und wegen $N(\mathbb{Z}[\omega]) \subset \mathbb{N}$ folgt $0 < N(x') < N(x)$ und $0 < N(x'') < N(x)$. Nach Vorraussetzung besitzen daher x' und x'' eine Darstellung von endlich vielen Primelementen, somit folgt die Behauptung.

Eindeutigkeit

Seien hierfür $p_1, ..., p_n, q_1, ..., q_m \in \mathbb{Z}[\omega]$ prime Elemente und $n, m \in \mathbb{N}$ sodass

$$x = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$$

gilt. Somit ist zu zeigen dass es eine bijektive Abbildung $\sigma : \{1, ..., n\} \to \{1, ..., m\}$ gibt sodass p_i assoziiert zu $q_{\sigma(i)}$ für alle $i \in \{1, ..., n\}$ ist. Induktion über m:

"$m = 1$" .
Sei $x = q_1 := q = p_1...p_n$. Da q prim ist gibt es ein p_i mit $i \in \{1, .., n\}$ sodass $q|p_i$, ohne Einschränkung sei $i = 1$. Es folgt unmittelbar dass $p_1|q$. Somit gilt $q \sim p_1$. Damit existiert ein $\nu \in \mathbb{Z}[\omega]^\times$ sodass $q = p_1\nu$. Daher gilt $q = p_1\nu = p_1p_2...p_n$, womit $\nu = p_2...p_n \in \mathbb{Z}[\omega]^\times$ folgt. Da p_i prim ist für alle $i \in \{1, ..., n\}$ folgt $n = 1$. Und daher gilt $q = p_1$.

"$m > 1$" .
Sei nun die Aussage wahr für alle $k \leq m - 1$.
Dann gilt $p_1...p_n = q_1...q_m$. Da q_m prim ist gibt es ein $i \in \{1, .., n\}$ sodass $q_m|p_i$ gilt. Ohne Einschränkung sei $i = n$. Wegen q_m und p_n prim in $\mathbb{Z}[\omega]$ folgt $q_m \sim p_n$. Sei daher $\nu \in \mathbb{Z}[\omega]^\times$ sodass $\nu q_m = p_n$ gilt. Dann folgt $p_1...p_{n-1}\nu q_m = q_1...q_{m-1}p_m$, und damit gilt $p_1...p_{n-1}\nu = q_1...q_{m-1}$. Nach Induktionsvorraussetzung folgt $n - 1 = m - 1$ und daher $n = m$. Da $q_m \sim p_n$ gilt folgt die Behauptung.

□

2 Prime Elemente in $\mathbb{Z}[\omega]$

Definition 2.1. Sei $A \subset \mathbb{Z}[\omega]$.

- Ein Element $d \in \mathbb{Z}[\omega]$ heißt **größter gemeinsamer Teiler** von A falls
  1. $d|a$ für alle $a \in A$.
  2. Für alle $\tilde{d} \in \mathbb{Z}[\omega] \setminus \{0\}$, mit $\tilde{d}|a$ für alle $a \in A$, gilt $\tilde{d}|d$.

  gelten.
- $GGT(A)$ ist die **Menge aller größten gemeinsamen Teiler von** A.

Proposition 2.2. *Sei $\emptyset \neq A \subset \mathbb{Z}[\omega]$ und $d \in \mathbb{Z}[\omega]$ dann gilt*

1. $$d \in GGT(A) \iff \sum_{a \in A} \mathbb{Z}[\omega]a = \mathbb{Z}[\omega]d.$$
2. *$GGT(A) \neq \emptyset$.*
3. *Für alle $d, \tilde{d} \in GGT(A)$ gilt $d \sim \tilde{d}$.*
4. *Für $d \in GGT(A)$ gilt $GGT(A) = d\mathbb{Z}[\omega]^\times$.*
5. *Es gilt $GGT(A) = \mathbb{Z}[\omega]^\times \iff 1 \in \sum_{a \in A} \mathbb{Z}[\omega]a$.*
6. *Seien $m \in \mathbb{N}, a \in A$ und $b_1, ..., b_m \in \mathbb{Z}[\omega]$. Falls für alle $k \in \{1, ..., m\}$ gilt $GGT(a, b_k) = \mathbb{Z}[\omega]^\times$, so folgt $GGT(a, \prod_{i=1}^{m} b_i) = \mathbb{Z}[\omega]^\times$.*

Beweis.

1. "$\Leftarrow$" Sei $\sum_{a \in A} \mathbb{Z}[\omega]a = \mathbb{Z}[\omega]d$. Für alle $a \in A$ gilt dann $\mathbb{Z}[\omega]a \subset \mathbb{Z}[\omega]d$. Mit 1.6 folgt $d|a$ für alle $a \in A$.
   Sei nun $\tilde{d} \in \mathbb{Z}[\omega]$, sodass $\tilde{d}|a$ für jedes $a \in A$ gilt.
   Mit 1.6 folgt für jedes $a \in A$, dass $\mathbb{Z}[\omega]a \subset \mathbb{Z}[\omega]\tilde{d}$ ist. Damit gilt $\sum_{a \in A} \mathbb{Z}[\omega]a \subset \mathbb{Z}[\omega]\tilde{d}$. Somit gilt $\mathbb{Z}[\omega]d = \sum_{a \in A} \mathbb{Z}[\omega]a \subset \mathbb{Z}[\omega]\tilde{d}$, womit man mit 1.6 $\tilde{d}|d$ erhält.

   "$\Rightarrow$" Sei $d \in GGT(A)$, dann gilt für alle $a \in A$ dass $d|a$. Daher folgt $\mathbb{Z}[\omega]a \subset \mathbb{Z}[\omega]d$. Damit gilt $\sum_{a \in A} \mathbb{Z}[\omega]a \subset \mathbb{Z}[\omega]d$.
   Nach 1.8 ist $\mathbb{Z}[\omega]$ ist ein Hauptidealring. Daher gibt es ein $\tilde{d} \in \mathbb{Z}[\omega]$ sodass $\sum_{a \in A} \mathbb{Z}[\omega]a = \mathbb{Z}[\omega]\tilde{d}$.
   Mit 1.6 folgt für alle $a \in A$ dass $\tilde{d}|a$. Wegen $d \in GGT(A)$ gilt $\tilde{d}|d$. Damit folgt $\mathbb{Z}[\omega]d \subset \mathbb{Z}[\omega]\tilde{d} = \sum_{a \in A} \mathbb{Z}[\omega]a \subset \mathbb{Z}[\omega]d$.
   Womit folgt dass $\mathbb{Z}[\omega]d = \sum_{a \in A} \mathbb{Z}[\omega]a$.
2. Da $\mathbb{Z}[\omega]$ ein Hauptidealring ist gibt es ein $d \in \mathbb{Z}[\omega]$ sodass
   $$\mathbb{Z}[\omega]d = \sum_{a \in A} \mathbb{Z}[\omega]a$$
   und mit 1. folgt dass $d \in GGT(A)$.
3. Sein $d, \tilde{d} \in GGT(A)$. Dann gilt mit 1. dass
   $$\mathbb{Z}[\omega]d = \sum_{a \in A} \mathbb{Z}[\omega]a = \mathbb{Z}[\omega]\tilde{d}.$$
   Somit gilt $d|\tilde{d}$ und $\tilde{d}|d$. Dann folgt mit 1.6 dass $d \sim \tilde{d}$ ist.

4. Sei $d \in GGT(A)$. Dann gelten folgende Äquivalenzen:
   $d' \in GGT(A) \iff d'\mathbb{Z}[\omega] = \sum\limits_{a\in A} \mathbb{Z}[\omega]a = d\mathbb{Z}[\omega] \iff d' \sim d.$
   Daher gilt $GGT(A) = d\mathbb{Z}[\omega]^\times$.

5. "$\Leftarrow$" Sei $1 \in \sum\limits_{a\in A} \mathbb{Z}[\omega]a$. Dann folgt, wegen $\sum\limits_{a\in A} \mathbb{Z}[\omega]a = \mathbb{Z}[\omega]$, mit 1., dass $1 \in GGT(A)$ gilt. Nun folgt mit 4., dass $GGT(A) = \mathbb{Z}[\omega]^\times$ gilt.
   "$\Rightarrow$" Sei $GGT(A) = \mathbb{Z}[\omega]^\times$. Dann folgt mit 4., dass $1 \in GGT(A)$ gilt. Und mit 1. folgt $1 \in \sum\limits_{a\in A} \mathbb{Z}[\omega]a$.

6. Seien $m \in \mathbb{N}, a \in A$ und $b_1, ..., b_m \in \mathbb{Z}[\omega]$. Beweis durch Widerspruch. Angenommen es gilt für alle $k \in \{1, ..., m\}$ dass $GGT(a, b_k) = \mathbb{Z}[\omega]^\times$ und $GGT(a, \prod\limits_{i=1}^{m} b_i) \neq \mathbb{Z}[\omega]^\times$.
   Sei $d \in GGT(a, \prod\limits_{i=1}^{m} b_i)$, dann gilt $d \neq 0$. (Denn sonst würde $a = \prod\limits_{i=1}^{m} b_i = 0$ gelten. Daher gibt es ein $k \in \{1, ..., m\}$ sodass $b_k = 0$ gilt, und somit würde $0 \in GGT(a, b_k) = \mathbb{Z}[\omega]^\times$ folgen, Widerspruch.)
   Somit gilt $d \notin \mathbb{Z}[\omega]^\times \cup \{0\}$, womit es ein Primelement $p \in \mathbb{Z}[\omega]$ gibt mit $p|d$. Somit folgt $p| \prod\limits_{i=1}^{m} b_i$ und $p|a$. Da p prim ist, gibt es ein $k \in \{1, ..., m\}$, sodass $p|b_k$ gilt. Deshalb existiert ein $d_0 \in GGT(a, b_k) = \mathbb{Z}[\omega]^\times$ mit $p|d_0$. Womit $p \in \mathbb{Z}[\omega]^\times$ folgt, Widerspruch.

□

Bemerkung 2.3. Die Menge der Primelemente von $\mathbb{Z}$ sei wie üblich mit $\mathbb{P}$ bezeichnet.

Satz 2.4. *Sei $x \in \mathbb{Z}[\omega]$ ein primes Element, dann existiert genau ein $p \in \mathbb{P}$, sodass $x|p$ gilt. Für dieses p gilt:*

1. *$N(x) = p$ und x ist nicht assoziiert zu p,*
   oder

2. *$N(x) = p^2$ und x ist assoziiert zu p.*

Beweis. Sei $x \in \mathbb{Z}[\omega]$ prim, sodass $N(x) = n \in \mathbb{N}$ gilt.

Existenz: Falls $n := p \in \mathbb{P}$ gilt, so folgt $x\overline{x} = N(x) = p$. Daher gilt $x|p$.
Sei nun $n \notin \mathbb{P}$. Dann existieren $p_1, ..., p_n \in \mathbb{P}$ und $r_1, ...r_n \in \mathbb{N}$ sodass $n = \prod\limits_{i=1}^{n} p_i^{r_i}$ gilt.
Daraus folgt $N(x) = x\overline{x} = n = \prod\limits_{i=1}^{n} p_i^{r_i}$. Daher gilt $x| \prod\limits_{i=1}^{n} p_i^{r_i}$ in $\mathbb{Z}[\omega]$. Da x prim in $\mathbb{Z}[\omega]$ ist, existiert ein $i \in \{1, ..., n\}$ sodass $x|p_i := p \in \mathbb{P}$.

Eindeutigkeit: Angenommen es existieren $p, q \in \mathbb{P}$ sodass $x|p$ und $x|q$ gilt. Dann folgt $N(x)|p^2$ und $N(x)|q^2$. Da x prim in $\mathbb{Z}[\omega]$ ist gilt $N(x) \neq 1$.
Wegen $p, q \in \mathbb{P}$ gilt $N(x) = p$ und $N(x) = q$, oder $N(x) = p^2$ und $N(x) = q^2$.
Aus der Eindeutigkeit der Primelemente von $\mathbb{Z}$ folgt nun $p = q$.

Sei nun $p \in \mathbb{P}$ sodass $x|p$ gilt. Daher gilt $x\overline{x} = N(x)|p^2$, womit wegen $p \in \mathbb{P}$ gilt: $N(x) = p$ oder $N(x) = p^2$. Falls nun $N(x) = p$ und angenommen $x \sim p$ gilt. Dann existiert ein $\nu \in \mathbb{Z}[\omega]^\times$ sodass $p\nu = x$ gilt. Somit folgt $p = N(x) = N(p\nu) = N(p)N(\nu) = N(p) = p^2$, was im Widerspruch zu $p \in \mathbb{P}$ steht. Daraus folgt $x \nsim p$.
Sei nun $N(x) = p^2$. Dann gilt $x|p$. Sei daher $\gamma \in \mathbb{Z}[\omega]$ sodass $x\gamma = p$ gilt. Dann folgt $N(x)N(\gamma) = N(x\gamma) = N(p) = p^2$. Wegen $N(x) \in \mathbb{N}$ und $N(x) \notin \mathbb{P}$ gilt $N(x) = p^2$ und $N(\gamma) = 1$. Also folgt mit 1.2 $\gamma \in \mathbb{Z}[\omega]^\times$. Daher gilt: $x \sim p$. □

Satz 2.5. *Ist $x \in \mathbb{Z}[\omega]$ sodass $N(x) = p \in \mathbb{P}$ gilt, dann ist x ein primes Element von $\mathbb{Z}[\omega]$.*

Beweis. Angenommen x ist nicht prim in $\mathbb{Z}[\omega]$ und $N(x) = p \in \mathbb{P}$. Da x nicht prim in $\mathbb{Z}[\omega]$ und $N(x) \neq 0$ ist, existieren $\rho, \gamma \in \mathbb{Z}[\omega] \setminus (\mathbb{Z}[\omega]^\times \cup \{0\})$, sodass $x = \rho\gamma$ gilt. Aus $\rho, \gamma \notin \mathbb{Z}[\omega]^\times \cup \{0\}$ folgt mit 1.2 dass $N(\rho) > 1$ und $N(\gamma) > 1$ gilt.
Daraus folgt $p = N(x) = N(\rho)N(\gamma)$ womit p keine Primelement von $\mathbb{Z}$ sein kann. Widerspruch.
Damit gilt x ist prim in $\mathbb{Z}[\omega]$. □

Definition 2.6. Sei $p \in \mathbb{P}$, dann heißt

- p **träge** in $\mathbb{Z}[\omega] \iff p$ ist ein Primelement von $\mathbb{Z}[\omega]$.
- p **unverzweigt** in $\mathbb{Z}[\omega] \iff p = x\overline{x}$ wobei x prim in $\mathbb{Z}[\omega]$ und $x \nsim \overline{x}$ gilt.
- p **verzweigt** in $\mathbb{Z}[\omega] \iff p = x\overline{x}$ wobei x prim in $\mathbb{Z}[\omega]$ und $x \sim \overline{x}$ gilt.

Definition 2.7. Seien die Teilmengen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C} \subset \mathbb{P}$ wie folgt definiert:

- $\mathfrak{A} := \{p \in \mathbb{P} \mid p \text{ ist träge in } \mathbb{Z}[\omega]\}$
- $\mathfrak{B} := \{p \in \mathbb{P} \mid p \text{ ist unverzweigt in } \mathbb{Z}[\omega]\}$
- $\mathfrak{C} := \{p \in \mathbb{P} \mid p \text{ ist verzweigt in } \mathbb{Z}[\omega]\}$

Proposition 2.8. *Für jedes $p \in \mathbb{P}$ gibt es genau eine der folgenden drei Möglichkeiten der Primzerlegung in $\mathbb{Z}[\omega]$.*

1. *p ist träge in $\mathbb{Z}[\omega]$.*
2. *p ist unverzweigt in $\mathbb{Z}[\omega]$.*
3. *p ist verzweigt in $\mathbb{Z}[\omega]$.*

Beweis. Sei $p \in \mathbb{P}$, dann folgt $N(p) = p^2 > 1$. Mit 1.2 folgt $p \notin \mathbb{Z}[\omega]^\times \cup \{0\}$. Nach 1.10 gibt es eine Darstellung der Form $p = \prod_{i=1}^{n} x_i$ mit $x_1, ..., x_n \in \mathbb{Z}[\omega]$ prim. Daher existiert ein Primelement $x \in \mathbb{Z}[\omega]$ sodass $x|p$ gilt. Mit 2.4 folgt $x \sim p$ oder $N(x) = \overline{x}x = p$.
Falls $x \sim p$ gilt, so ist p prim in $\mathbb{Z}[\omega]$. Daher ist p träge in $\mathbb{Z}[\omega]$, was 1 entspricht.
Falls $x\overline{x} = p$ gilt so trifft entweder 2 oder 3 zu.
Die Eindeutigkeit folgt unmittelbar aus der Eindeutigkeit der Primfaktorzerlegung (also nach 1.10). □

Definition 2.9. Von nun an sei für $p \in \mathbb{P}$ stets $\pi_p \in \mathbb{Z}[\omega]$ ein Primelement, sodass gilt

- ist $p \in \mathfrak{A}$, so folgt $p = \pi_p$.
- ist $p \in \mathfrak{B} \cup \mathfrak{C}$, so folgt $p = \overline{\pi}_p \pi_p$.

Proposition 2.10. *Für $\pi_p \in \mathbb{Z}[\omega]$ gilt:*

- *ist $p \in \mathfrak{A} \Longrightarrow N(\pi_p) = p^2$.*
- *Ist $p \in \mathfrak{B} \cup \mathfrak{C} \Longrightarrow N(\pi_p) = p$.*

Beweis. Sei $p \in \mathfrak{A}$. Dann folgt $p = \pi_p$, womit $p \sim \pi_p$ gilt. Daher folgt mit 2.4 dass $N(\pi_p) = p^2$ gilt.
Sei nun $p \in \mathfrak{B} \cup \mathfrak{C}$. Dann folgt $p \nsim \pi_p$ und $\pi_p | p$, womit mit 2.4 folgt: $N(\pi_p) = p$. □

Definition 2.11. Seien

- $\mathcal{A} := \{\pi_p \in \mathbb{Z}[\omega] | p \in \mathfrak{A}\}$
- $\mathcal{B} := \{\pi_p, \overline{\pi_p} \in \mathbb{Z}[\omega] | p \in \mathfrak{B}\}$
- $\mathcal{C} := \{\pi_p \in \mathbb{Z}[\omega] | p \in \mathfrak{C}\}$
- $\mathcal{P} := \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$

Bemerkung 2.12. Nach 2.4 und 2.8 folgt unmittelbar dass $\mathcal{A} \cap \mathcal{B} = \emptyset$, $\mathcal{B} \cap \mathcal{C} = \emptyset$, und $\mathcal{A} \cap \mathcal{C} = \emptyset$ gilt. Daher ist $\mathcal{P}$ die disjunkte Vereinigung von $\mathcal{A}, \mathcal{B}$ und $\mathcal{C}$.

Satz 2.13. *Die Menge $\mathcal{P}$ ist bezüglich der Assoziiertheit ein Repräsentantensystem der primen Elemente von $\mathbb{Z}[\omega]$. (d.h.: Für jedes Primelement $x \in \mathbb{Z}[\omega]$ gibt es ein $\pi \in \mathcal{P}$ mit $x \sim \pi$. Und falls für $\pi_1, \pi_2 \in \mathcal{P}$ gilt $\pi_1 \sim \pi_2$, so folgt $\pi_1 = \pi_2$.)*

Beweis. Sei $x \in \mathbb{Z}[\omega]$ ein Primelement. Nach 2.4 existiert ein $p \in \mathbb{P}$ sodass $p \sim x$ ist oder $p = N(x)$ gilt.
Falls $p \sim x$ gilt, folgt dass $p \in \mathcal{A}$ ein Repräsentant von x ist.
Falls $p = N(x)$ ist, folgt dass p kein Primelement in $\mathbb{Z}[\omega]$ ist. Daher gilt $p \in \mathfrak{B}$ oder $p \in \mathfrak{C}$.
Womit entweder $\pi_p \in \mathcal{B}$, oder $\pi_p \in \mathcal{C}$ gilt.
Für beide Fälle gilt $x\overline{x} = p = \pi_p\overline{\pi_p}$. Nach 1.10 folgt, falls $\pi_p \in \mathcal{B}$ gilt $x \sim \pi_p$ oder $x \sim \overline{\pi}_p$. Falls $\pi_p \in \mathcal{C}$ ist, folgt $x \sim \pi_p$.
Seien nun $\pi, \pi' \in \mathcal{P}$ sodass $\pi \sim \pi'$ gilt. Dann gibt es $p, q \in \mathbb{P}$, sodass $\pi | p$ und $\pi' | q$ gilt. Wegen $\pi \sim \pi'$ folgt $\pi | q$. Mit 2.4 folgt $p = q$.

1.Fall Falls $p \in \mathfrak{A}$ ist, so folgt $\pi = \pi_p$ und $\pi' = \pi_p$. Daher gilt $\pi = \pi'$.

2.Fall Falls $p \in \mathfrak{B}$ ist, so folgt $\pi, \pi' \in \{\pi_p, \overline{\pi}_p\}$. Wegen $\pi \sim \pi'$ und $\pi_p \nsim \overline{\pi}_p$ folgt $\pi = \pi'$.

3.Fall Falls $\pi_p \in \mathfrak{C}$ ist, so folgt $\pi, \pi' \in \{\pi_p\}$. Daher folgt unmittelbar $\pi = \pi'$.

□

Satz 2.14. *Sei $p \in \mathbb{P}$, dann gilt $p \in \mathfrak{B} \cup \mathfrak{C}$ genau dann, wenn es $a, b \in \mathbb{Z}$ gibt, sodass $p = a^2 - ab + b^2$ gilt.*

Beweis.

"⇒" Nach 2.8 ist $p = N(\pi_p)$. Sei $\pi_p = a + b\omega$ mit $a, b \in \mathbb{Z}$, dann folgt $p = \pi_p\overline{\pi}_p = a^2 - ab + b^2$.

"⇐" Seien nun $a, b \in \mathbb{Z}$ sodass $p = a^2 - ab + b^2$ gilt. Setzte $x = a + b\omega \in \mathbb{Z}[\omega]$, dann folgt $p = x\overline{x} = N(x)$. Mit 2.5 folgt, dass x prim in $\mathbb{Z}[\omega]$ ist. Somit ist $p \in \mathfrak{B} \cup \mathfrak{C}$.

□

Satz 2.15. *Sei $p \in \mathbb{P}$, dann gelten:*

1. $p \in \mathfrak{A} \iff p \equiv 2 \mod 3$
2. $p \in \mathfrak{B} \iff p \equiv 1 \mod 3$
3. $p \in \mathfrak{C} \iff p = 3$

Beweis.

3. "⇒" Sei $p \in \mathfrak{C}$, dann gilt $p = N(\pi_p) = \pi_p\overline{\pi_p}$ und $\pi_p \sim \overline{\pi_p}$. Daher folgt $\pi_p | \overline{\pi_p}$ und somit $\pi_p | \pi_p - \overline{\pi_p}$.
Seien $a, b \in \mathbb{Z}$ sodass $\pi_p = a + b\omega$ gilt. Dann folgt $\pi_p | \pi_p - \overline{\pi}_p = a + b\omega - (a - b - b\omega) = b + 2b\omega = b(1 + 2\omega)$, womit $\pi_p | b(1 + 2\omega)$ gilt.
Sei daher $y \in \mathbb{Z}[\omega]$ sodass $\pi_p y = b(1 + 2\omega)$ gilt. Dann gilt:

$$pN(y) = \pi_p\overline{\pi}_p N(y) = N(\pi_p)N(y) = N(\pi_p y) = N(b(1 + 2\omega)) = N(b)N(1 + 2\omega)$$

$$= b^2((1 + 2\omega)(1 - 2 - 2\omega)) = b^2(1 - 2 - 4\omega - 4\omega^2) = b^2(-1 - 4(\omega^2 + \omega)) = b^2(-1 + 4) = 3b^2$$

Damit erhält man $p | 3b^2$, womit wegen $p \in \mathbb{P}$ folgt $p | b$ oder $p | 3$.
Angenommen $p | b$. Dann folgt $p = \pi_p\overline{\pi}_p = a^2 - ab + b^2$, womit $p | p - b(a - b) = a^2$ gilt. Daher gilt $p | a$. Seien daher $c, d \in \mathbb{Z}$ sodass $pc = a$ und $pd = b$ gilt. Dann folgt $p = a^2 - ab + b^2 = p^2c^2 - p^2cd + bp^2d^2 = p^2(c^2 - cd + d^2)$.
Damit folgt $1 = p(c^2 - cd + d^2)$ und daher $p | 1$ in $\mathbb{Z}$. Das kann jedoch wegen $p \in \mathbb{P}$ nicht gelten. Daher gilt $p | 3$ in $\mathbb{Z}$, und somit $p = 3$.

"$\Leftarrow$" Sei $p = 3$, für $x \in \mathbb{Z}[\omega]$ mit $x = 1 - \omega$ gilt $N(x) = (1-\omega)(2+\omega) = 3$. Womit nach 2.5 gilt x ist prim in $\mathbb{Z}[\omega]$. Es bleibt zu zeigen $x \sim \overline{x}$.
Wegen $-\omega^2 \in \mathbb{Z}[\omega]^\times$ und $(1-\omega)(-\omega^2) = (1-\omega)(1+\omega) = 1-\omega^2 = 2+\omega$ folgt $x \sim \overline{x}$.

1. "$\Leftarrow$" Sei $p \in \mathbb{P}$ sodass $p \equiv 2 \mod 3$ gilt. Zu zeigen ist $p \in \mathfrak{A}$. Es genügt zu zeigen dass $p \notin \mathfrak{B} \cup \mathfrak{C}$ gilt.
Angenommen $p \equiv 2 \mod 3$ und $p \in \mathfrak{B} \cup \mathfrak{C}$. Dann gibt es $a, b \in \mathbb{Z}$ sodass $p = N(\pi_p) = a^2 - ab + b^2$ gilt. Womit $4p = (2a-b)^2 + 3b^2$ gilt.
Sei $\pi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ der kanonische Homomorphismus. Dann gilt $\pi(p) = \pi(4p) = \pi((2a-b)^2 + 3b^2) = \pi(2a-b)^2 + \pi(3b^2) = \pi(2a-b)^2$. Daher gibt es ein $x \in \mathbb{Z}$ sodass $\pi(p) = \pi(x^2)$ gilt, womit $x^2 \equiv 2 \mod (3)$ gilt. Da jedoch in $0^2 \equiv 0 \mod (3)$, $1^2 \equiv 1 \mod (3)$ und $2^2 \equiv 1 \mod (3)$ gilt, kann ein solches x nicht existieren, Widerspruch.
Somit gilt $p \notin \mathfrak{B} \cup \mathfrak{C}$.

2. "$\Leftarrow$" Sei $p \in \mathbb{P}$ sodass $p \equiv 1 \mod 3$ gilt. Es folgt unmittelbar dass $p \neq 2$ und $p \neq 3$ gilt. Mit dem Quadratischen Reziprozitätsgesetz folgt

$$\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}.$$

Damit folgt

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Daher gibt es ein $u \in \mathbb{Z}$ sodass $u^2 \equiv -3 \mod p$ gilt, womit $\sqrt{-3} \in \mathbb{Z}/p\mathbb{Z}$ folgt. Da $p \neq 2$ ist, folgt $2 \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\} = (\mathbb{Z}/p\mathbb{Z})^\times$. Daher ist $v := \frac{1-\sqrt{-3}}{2} \in \mathbb{Z}/p\mathbb{Z}$, und v ist eine Nullstelle von $P(x) = x^2 - x + 1$ in $\mathbb{Z}/p\mathbb{Z}$. Sei $\pi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ der kanonische Homomorphismus, und sei $u \in \mathbb{Z}$, sodass $v = \pi(u)$ gilt. Dann gilt $p | u^2 - u + 1$. Sei $x = u + \omega$, dann gilt $N(x) = x\overline{x} = (u+\omega)(u-1-\omega) = u^2 - u - \omega - \omega^2 = u^2 - u + 1$, also $p | x\overline{x}$. Wegen $p \neq 3$ folgt mit 3. $p \notin \mathfrak{C}$, daher ist zu zeigen: p ist nicht prim in $\mathbb{Z}[\omega]$.
Angenommen p ist prim in $\mathbb{Z}[\omega]$. Dann gilt $p | x$, oder $p | \overline{x}$.

"$p|x$" Dann existieren $a, b \in \mathbb{Z}$ sodass $p(a + b\omega) = u + \omega$ und daher $pa + pb\omega = u + \omega$ womit $pb = 1$ folgt, was wegen $p \in \mathbb{P}$ nicht sein kann.

"$p|\overline{x}$" Dann existieren $a, b \in \mathbb{Z}$ sodass $p(a + b\omega) = pa + pb\omega = u - 1 - \omega$ womit $pb = -1$ gilt, was wiederum wegen $p \in \mathbb{P}$ nicht sein kann.

Somit ist p nicht prim in $\mathbb{Z}[\omega]$, und daher gilt $p \in \mathfrak{B}$.

Die Implikationen " $\Rightarrow$ " für 1 und 2 folgen nun unmittelbar mit 2.12. □

Bemerkung 2.16. Aus dem letzten Satz folgt $\mathfrak{C} = \{3\}$ und $\mathcal{C} = \{1 - \omega\}$.

3 Mächtigkeit von $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$

Definition 3.1. Sei

$$\rho : \begin{cases} \mathbb{Z}[\omega] \setminus \{0\} \to \mathbb{N}^+ \cup \infty \\ x \mapsto |\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x| \end{cases}$$

Lemma 3.2. *Seien $x, y \in \mathbb{Z}[\omega] \setminus \{0\}$, dann gilt $\rho(xy) = \rho(x)\rho(y)$.*

Beweis. Seien $x, y \in \mathbb{Z}[\omega]$ und

- $\pi_x : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$
- $\pi_y : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]y$
- $\pi_{xy} : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]xy$

die kanonischen Homomorphismen. Es ist $\mathbb{Z}[\omega]xy$ ein Ideal in $\mathbb{Z}[\omega]$ und $\mathbb{Z}[\omega]xy \subset \mathbb{Z}[\omega]x = \ker(\pi_x)$. Aus der ***universellen Eigenschaft des Restklassenhomomorphisums*** folgt, dass es einen Ringhomomorphismus $f : \mathbb{Z}[\omega]/\mathbb{Z}[\omega]xy \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ gibt, sodass $f \circ \pi_{xy} = \pi_x$ gilt.
Wegen der Surjektivität von π_x folgt dass f surjektiv ist, und es gilt $\ker(f) = \pi_{xy}(ker(\pi_x)) = \pi_{xy}(\mathbb{Z}[\omega]x)$. Sei

$$\tilde{g} : \begin{cases} \mathbb{Z}[\omega] \to \pi_{xy}(\mathbb{Z}[\omega]x) \\ a \mapsto \pi_{xy}(ax) \end{cases}$$

ein Ringhomomorphismus. Es gelten folgende Äquivalenzen:

$$a \in \ker(\tilde{g}) \iff \pi_{xy}(ax) = 0 \iff xy|ax \iff y|a \iff a \in \mathbb{Z}[\omega]y.$$

Daher gilt $\ker(\tilde{g}) = \mathbb{Z}[\omega]y$. Somit folgt aus der ***universellen Eigenschaft des Restklassenhomomorphisums*** dass es einen Ringhomomorphismus $g : \mathbb{Z}[\omega]/\mathbb{Z}[\omega]y \to \pi_{xy}(\mathbb{Z}[\omega]x)$ gibt, sodass $g \circ \pi_y = \tilde{g}$ gilt. Wegen der Surjektivität von $\tilde{g}$ folgt dass g surjektiv ist.
Seien nun $u_1, u_2 \in \mathbb{Z}[\omega]/\mathbb{Z}[\omega]y$ und $a_1, a_2 \in \mathbb{Z}[\omega]$ sodass $u_i = \pi_y(a_i)$, für $i \in \{1, 2\}$, gilt. Gilt nun $g(u_1) = g(u_2)$ so folgt $0 = g(u_1 - u_2) = g(\pi_y(a_1 - a_2)) = \pi_{xy}((a_1 - a_2)x)$. Daher ist $(a_1 - a_2)x \in \ker(\pi_{xy}) = \mathbb{Z}[\omega]xy$. Da $x \neq 0$ kein Nullteiler ist, gilt $a_1 - a_2 \in \mathbb{Z}[\omega]y = \ker(\pi_y)$. Somit folgt $\pi_y(a_1 - a_2) = 0$ und daher $u_1 = \pi_y(a_1) = \pi_y(a_2) = u_2$.
Daher ist g ein Gruppenisomorphismus, womit $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]y \cong \pi_{xy}(\mathbb{Z}[\omega]x) = \ker(f)$ gilt. Insbesondere folgt $|\ker(f)| = |\mathbb{Z}[\omega]/\mathbb{Z}[\omega]y| = \rho(y)$.
Aus dem ***Homomorphiesatz der Gruppentheorie*** folgt $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]xy)/\ker(f) \cong f(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]xy) = \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$. Womit $|(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]xy)/\ker(f)| = |\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x| = \rho(x)$ folgt. Da der $\ker(f)$ eine Untergruppe von $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]xy$ ist, folgt mit dem ***Satz von Lagrange***:

$$\rho(xy) = |\mathbb{Z}[\omega]/\mathbb{Z}[\omega]xy| = |(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]xy)/\ker(f)| \cdot |\ker(f)| = \rho(x) \cdot \rho(y).$$

□

Lemma 3.3. *Sei $n \in \mathbb{N}^+$, dann gilt $\rho(n) = n^2$.*

Beweis. Sei $n \in \mathbb{N}^+$ und $S := \{a + b\omega \in \mathbb{Z}[\omega] | 0 \leq a, b < n\}$. Sei $\pi : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]n$ der kanonische Homomorphismus und $\pi_S : S \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]n$ dessen Einschränkung auf S. Dann ist π_S bijektiv.

surjektiv: Sei $z \in \mathbb{Z}[\omega]/\mathbb{Z}[\omega]n$, $y \in \mathbb{Z}[\omega]$ und $a, b \in \mathbb{Z}$ mit $y = a + b\omega$, sodass $z = \pi(y)$ gilt. Mittels Divison mit Rest gibt es $q, r, s, t \in \mathbb{Z}$ mit $0 \leq r, t < n$ sodass $a = nq + r$ und $b = ns + t$ gilt. Dann folgt $z = \pi(y) = \pi(a + b\omega) = \pi(nq + r + ns\omega + t\omega) = \pi(n(q + s\omega) + r + t\omega) = \pi(n)(\pi(q + s\omega)) + \pi(r + t\omega) = \pi(r + t\omega) = \pi_S(r + t\omega)$. Somit ist π_S surjektiv.

injektiv: Seien $y_1, y_2 \in S$ mit $\pi_S(y_1) = \pi_S(y_2)$. Seien $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ sodass $y_i = a_i + b_i\omega$ und $0 \leq a_i, b_i < n$, für $i \in \{1, 2\}$ gilt. Dann gilt $\pi_S(a_1 + b_1\omega) = \pi_S(a_2 + b_2\omega)$, womit $\pi(a_1 - a_2 + (b_1 - b_2)\omega) = 0$ folgt. Daher existiert ein $q \in \mathbb{Z}[\omega]$ sodass $a_1 - a_2 + (b_1 - b_2)\omega = qn$ gilt. Seien $u, v \in \mathbb{Z}$ sodass $q = u + v\omega$. Dann folgt $a_1 - a_2 - nu + (b_1 - b_2 - nv)\omega = 0$. Daher folgt $nu = a_1 - a_2$ und $nv = b_1 - b_2$. Somit gilt $n|a_1 - a_2$ in $\mathbb{Z}$, und $n|b_1 - b_2$ in $\mathbb{Z}$. Wegen $-n + 1 \leq a_1 - a_2 \leq n - 1$ und $-n + 1 \leq b_1 - b_2 \leq n - 1$ folgt $a_1 = a_2$ und $b_1 = b_2$. Daher folt $y_1 = y_2$.

Da π_S ein Bijektion zwischen S und $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]n$ ist folgt $\rho(n) = |\mathbb{Z}[\omega]/\mathbb{Z}[\omega]n| = |S| = n^2$. □

Satz 3.4. *Sei $x \in \mathbb{Z}[\omega] \setminus \{0\}$, dann ist $\rho(x) = N(x)$.*

Beweis. Sei $x \in \mathbb{Z}[\omega] \setminus \{0\}$. Nach 1.3 ist $\bar{\cdot} : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]$ ein Ringisomorphismus. $\mathbb{Z}[\omega]x$ ist ein Ideal von $\mathbb{Z}[\omega]$ mit $\overline{\mathbb{Z}[\omega]x} = \mathbb{Z}[\omega]\overline{x}$. Nach dem Isomorphieprinzip induziert $\bar{\cdot}$ einen Ringisomorphismus $\kappa : \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x \to \overline{\mathbb{Z}[\omega]}/\overline{\mathbb{Z}[\omega]x} = \mathbb{Z}[\omega]/\mathbb{Z}[\omega]\overline{x}$. Somit gilt $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x \cong \mathbb{Z}[\omega]/\mathbb{Z}[\omega]\overline{x}$. Somit gilt $\rho(x) = \rho(\overline{x})$. Mit 3.3 erhalten wir $N(x)^2 = \rho(N(x)) = \rho(x\overline{x}) = \rho(x)\rho(\overline{x}) = \rho(x)^2$. Daher gilt $N(x) = \rho(x)$. □

Satz 3.5. *Seien $x \in \mathbb{Z}[\omega] \setminus \{0\}, \pi : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ der kanonische Homomorphismus, $y \in \mathbb{Z}[\omega]$ und $n(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)$ die Menge aller Nullteiler von $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$. Dann gelten:*

1. *$\pi(y) \in n(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x) \iff GGT(x,y) \cap \mathbb{Z}[\omega]^\times = \emptyset$*
2. *$\pi(y) \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times \iff GGT(x,y) = \mathbb{Z}[\omega]^\times$*
3. *$\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ ist ein Körper $\iff$ $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ ist ein Bereich $\iff$ x ist ein Primelement.*

Beweis.

1. "⇒" Sei $\pi(y) \in n(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)$. Dann gibt es ein $w \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x) \setminus \{0\}$ sodass $\pi(y)w = 0$ ist. Sei $u \in \mathbb{Z}[\omega]$ mit $w = \pi(u)$. Wegen $w \neq 0$ folgt $u \notin \ker(\pi) = \mathbb{Z}[\omega]x$, womit $x \nmid u$ gilt. Jedoch ist $0 = \pi(y)\pi(u) = \pi(yu)$ womit $x|yu$ folgt.
   Angenommen $GGT(x,y) \cap \mathbb{Z}[\omega]^\times \neq \emptyset$. Dann existiert ein $d \in GGT(x,y) \cap \mathbb{Z}[\omega]^\times$, ohne Einschränkung sei $d = 1$. Dann gibt es $a, b \in \mathbb{Z}[\omega]$ mit $1 = ax + by$. Wegen $x|yu$ existiert ein $z \in \mathbb{Z}[\omega]$ sodass $yu = zx$. Somit folgt nun dass $u = axu + byu = aux + bzx$. Daher folgt $x|u$, was jedoch nicht sein kann.
   Somit folgt $GGT(x,y) \cap \mathbb{Z}[\omega]^\times = \emptyset$.
   "⇐" Sei $GGT(x,y) \cap \mathbb{Z}[\omega]^\times = \emptyset$ und $d \in GGT(x,y)$. Dann gilt $d \notin \mathbb{Z}[\omega]^\times$ und daher folgt $x \nmid \frac{x}{d}$. (Denn falls $x|\frac{x}{d} \Rightarrow xd|x \Rightarrow d|1 \Rightarrow d \in \mathbb{Z}[\omega]^\times$, was nicht sein kann.)
   Somit ist also $\frac{x}{d} \notin \ker(\pi)$ und daher $\pi(\frac{x}{d}) \neq 0$. Damit folgt nun $\pi(y)\pi(\frac{x}{d}) = \pi(\frac{yx}{d}) = \pi(\frac{y}{d})\pi(x) = 0$ und daher $\pi(y) \in n(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)$.

2. "⇒" Sei $\pi(y) \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times$. Dann gibt es ein $w \in \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ und $u \in \mathbb{Z}[\omega]$ sodass $\pi(y)w = 1$ und $w = \pi(u)$ gilt. Weiters gilt $\pi(1) = 1 = \pi(y)\pi(u) = \pi(yu)$ und damit $\pi(yu - 1) = 0$. Damit folgt $x|yu - 1$.
   Daher existiert ein $z' \in \mathbb{Z}[\omega]$ mit $uy - 1 = xz'$ und ein $z \in \mathbb{Z}[\omega]$ mit $zx + uy = 1$. Somit ist $1 \in \mathbb{Z}[\omega]x + \mathbb{Z}[\omega]y$ und daher gilt $GGT(x,y) = \mathbb{Z}[\omega]^\times$.
   "⇐" Sei $GGT(x,y) = \mathbb{Z}[\omega]^\times$, dann gilt $1 = ux + vy$ mit geeigneten $u, v \in \mathbb{Z}[\omega]$. Dann folgt $1 = \pi(1) = \pi(ux + vy) = \pi(u)\pi(x) + \pi(v)\pi(y) = 0 + \pi(v)\pi(y) = \pi(v)\pi(y)$. Daher ist $\pi(y) \in \mathbb{Z}[\omega]^\times$.

3. - $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ ist ein Körper $\Longrightarrow$ $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ ist ein Bereich.
     Ist eine unmittelbare Konsequenz der Definition.
   - $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ ist ein Bereich $\Longrightarrow$ x ist ein Primelement.
     Sei also $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ ein Bereich und $y \in \mathbb{Z}[\omega]$ ein Teiler von x. Dann gibt es ein $z \in \mathbb{Z}[\omega]$ mit $x = yz$. Somit gilt $0 = \pi(x) = \pi(yz) = \pi(y)\pi(z)$. Daher folgt $\pi(y) = 0$ oder $\pi(z) = 0$.
     Falls $\pi(y) = 0$, so gilt $y \in \mathbb{Z}[\omega]x$ und damit $x|y$. Wegen $y|x$, ist x assoziiert zu y.
     Falls $\pi(z) = 0$, so folgt analog dass x assoziiert zu z ist.
     Womit y eine Einheit ist. Somit besitzt x keine echten Teiler, somit ist x prim in $\mathbb{Z}[\omega]$.
   - x ist ein Primelement $\Longrightarrow$ $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ ist ein Körper.
     Sei nun x ein Primelement in $\mathbb{Z}[\omega]$. Dann gilt $x \notin \mathbb{Z}[\omega]^\times \cup \{0\}$ und daher $|\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x| = N(x) \geq 2$.
     Somit ist $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ nicht der Nullring. Seien $u \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x) \setminus \{0\}$ und $y \in \mathbb{Z}[\omega]$ mit $u = \pi(y)$. Wegen $u \neq 0$ folgt $y \notin \ker(\pi) = \mathbb{Z}[\omega]x$, womit $x \nmid y$ gilt. Sei $d \in GGT(x,y)$. Da x prim ist folgt $x \sim d$ oder $d \in \mathbb{Z}[\omega]^\times$. Falls $x \sim d$ gilt so folgt $x|d$. Wegen $d|y$ folgt $x|y$, ein Widerspruch. Somit muss $d \in \mathbb{Z}[\omega]^\times$ und damit $GGT(x,y) = \mathbb{Z}[\omega]^\times$ gelten.
     Daher folgt $u = \pi(y) \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times$. Somit ist jedes Element von $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x) \setminus \{0\}$ invertierbar, und daher ist $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ ein Körper.

□

Definition 3.6. Sei $x \in \mathbb{Z}[\omega] \setminus \{0\}$ dann ist $\phi_{\mathbb{Z}[\omega]}(x) := |(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times|$.

Satz 3.7. *Seien $x, y \in \mathbb{Z}[\omega]$. Dann gilt, falls $GGT(x,y) = \mathbb{Z}[\omega]^\times$ ist, so folgt $\phi_{\mathbb{Z}[\omega]}(x \cdot y) = \phi_{\mathbb{Z}[\omega]}(x) \cdot \phi_{\mathbb{Z}[\omega]}(y)$.*

Beweis. Seien $x, y \in \mathbb{Z}[\omega]$ und $d \in GGT(x,y) = \mathbb{Z}[\omega]^\times$.
Mit $\mathbb{Z}[\omega]x + \mathbb{Z}[\omega]y = \mathbb{Z}[\omega]d = \mathbb{Z}[\omega]$ folgt, dass die Ideale $\mathbb{Z}[\omega]x$ und $\mathbb{Z}[\omega]y$ teilerfremd sind. Mit dem ***Chinesischen Restsatz*** folgt

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

Somit gilt $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]xy)^\times \cong (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x \times \mathbb{Z}[\omega]/\mathbb{Z}[\omega]y)^\times = (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times \times (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]y)^\times$.
Womit schließlich folgt $\phi_{\mathbb{Z}[\omega]}(x \cdot y) = |(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]xy)^\times| = |(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times \times (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]y)^\times| = |(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times| \cdot |(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]y)^\times| = \phi_{\mathbb{Z}[\omega]}(x) \cdot \phi_{\mathbb{Z}[\omega]}(y)$. □

Satz 3.8. *Seien $x \in \mathbb{Z}[\omega], n \in \mathbb{N}^+$.*
Falls $x \in \mathbb{Z}[\omega]$ ein Primelement ist so folgt $\phi_{\mathbb{Z}[\omega]}(x^n) = N(x)^{n-1}(N(x)-1)$.

Beweis. Seien

- $\pi_x : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$
- $\pi_{x^{n-1}} : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^{n-1}$
- $\pi_{x^n} : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^n$

die kanonischen Homomorphismen. Es ist $\mathbb{Z}[\omega]x^n$ ein Ideal von $\mathbb{Z}[\omega]$ und $\mathbb{Z}[\omega]x^n \subset \mathbb{Z}[\omega]x = \ker(\pi_x)$. Somit folgt mit der ***universellen Eigenschaft des Restklassenhomomorphisums***, dass es einen Ringhomomorphismus $f : \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^n \longrightarrow \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x$ gibt sodass $f \circ \pi_{x^n} = \pi_x$.
Sei $\tilde{f} := f|_{(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^n)^\times} : (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^n)^\times \longrightarrow (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times$.
Wegen $f((\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^n)^\times) \subset f((\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times)$ ist $\tilde{f}$ wohldefiniert.
Sei nun $a \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times$ beliebig, und $u \in \mathbb{Z}[\omega]$ ein Repräsentant bezüglich π_x also $\pi_x(u) = a$. Somit ist $GGT(u,x) = \mathbb{Z}[\omega]^\times$, und mit 2.2 folgt $GGT(u,x^n) = \mathbb{Z}[\omega]^\times$. Daher gilt $\pi_{x^n}(u) \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^n)^\times$.
Womit man $a = \pi_x(u) = (f \circ \pi_{x^n})(u) = f(\pi_{x^n}(u)) = \tilde{f}(\pi_{x^n}(u))$ erhählt. Daher ist $\tilde{f}$ surjektiv.
Aus dem ***Homomorphiesatz der Gruppentheorie*** ergibt sich $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times / \ker(f) \cong (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times$.
Wegen x prim in $\mathbb{Z}[\omega]$ folgt mit 3.5 dass $|(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times / \ker(f)| = |(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times| = N(x) - 1$.
Sei $u \in \mathbb{Z}[\omega]$. Weil x prim ist folgt: jeder Teiler von x^n muss eine Potenz von x sein. Da $x \nmid 1 + ux$ gilt, folgt nun $GGT(x^n, 1+ux) = \mathbb{Z}[\omega]^\times$. Daher ist $\pi_{x^n}(1+ux) \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^n)^\times$. Wegen $\tilde{f}(\pi_{x^n}(1+ux)) = f(\pi_{x^n}(1+ux)) = \pi_x(1+ux) = \pi_x(1) = 1$ folgt $\pi_{x^n}(1+ux) \in \ker(\tilde{f})$.
Seien $u_1, u_2 \in \mathbb{Z}[\omega]$, dann gelten folgende Äquivalenzen:

$$\pi_{x^n}(1+u_1x) = \pi_{x^n}(1+u_2x) \Leftrightarrow x^n | u_1x - u_2x = (u_1-u_2)x \Leftrightarrow x^{n-1} | u_1 - u_2 \Leftrightarrow \pi_{x^{n-1}}(u_1) = \pi_{x^{n-1}}(u_2).$$

Sei daher $g : \mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^{n-1} \to \ker(\tilde{f})$ definiert durch $g(\pi_{x^{n-1}}(u)) = \pi_{x^n}(1+ux)$. Durch die eben gezeigten Äquivalenzen ist g injektiv. g ist auch surjektiv, denn:
sei $x \in \ker(\tilde{f})$, dann existiert ein $v \in \mathbb{Z}[\omega]$ mit $y = \pi_{x^n}(v)$. Falls nun $\tilde{f}(y) = 1$ gilt, so folgt $\pi_x(v) = f(\pi_{x^n}(v)) = \tilde{f}(\pi_{x^n}(v)) = 1 = \pi_x(1)$. Somit gilt $x | 1 - v$, daher gibt es ein $u \in \mathbb{Z}[\omega]$ sodass $x(-u) = 1 - v$ bzw. $v = 1 + ux$. Somit folgt $g(\pi_{x^{n-1}}(u)) = \pi_{x^n}(1+ux) = \pi_{x^n}(v) = y$, womit g surjektiv ist.
Daher ist g eine Bijektion.
Somit folgt $\left|\ker(\tilde{f})\right| = \left|\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^{n-1}\right| = N(x^{n-1}) = N(x)^{n-1}$. Da der $\ker(\tilde{f})$ eine Untergruppe von $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^n)^\times$ ist folgt mit dem ***Satz von Lagrange*** dass

$$\phi_{\mathbb{Z}[\omega]}(x^n) = \left|(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^n)^\times\right| = \left|(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x^n)^\times / \ker(\tilde{f})\right| \cdot \left|\ker(\tilde{f})\right| = (N(x)-1) \cdot N(x)^{n-1}.$$

□

4 Zyklizität der Restklassengruppe $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]x)^\times$

Satz 4.1. *Seien $\eta \in \mathcal{A}$ und $n \in \mathbb{N}^+$. Dann gilt:*
$(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n)^\times$ ist zyklisch $\iff$ $n = 1$.

Beweis.

"$\Leftarrow$" Sei $n = 1$. Da $\eta \in \mathbb{Z}[\omega]$ prim ist folgt mit 3.5 $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta$ ist ein Körper, wobei $|\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta| = N(\eta)$ gilt. Daher ist $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta)^\times$ endlich, und somit ist mit [2, Kapitel 2, Satz 3.4] die Einheitengruppe $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta)^\times$ zyklisch.

"$\Rightarrow$" Falls $n \geq 2$, so gilt $\phi_{\mathbb{Z}[\omega]}(\eta^{n-1}) = \left|(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^{n-1})^\times\right| = N(\eta)^{n-2}(N(\eta)-1) = p^{2(n-2)}(p^2-1)$.
Die Ordnung von $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^{n-1})^\times$ ist ein Vielfaches der Ordnung eines jeden $d \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^{n-1})^\times$, womit für jedes $x \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^{n-1})^\times$ gilt $x^{p^{2(n-2)}(p^2-1)} = 1$.
Sei nun $a \in \mathbb{Z}[\omega]$ mit $GGT(\eta, a) = \mathbb{Z}[\omega]^\times$, und seien

- $\pi_{\eta^{n-1}} : \mathbb{Z}[\omega] \longrightarrow (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^{n-1})^\times$
- $\pi_{\eta^n} : \mathbb{Z}[\omega] \longrightarrow (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n)^\times$

die kanonischen Homomorphismen. Dann folgt $GGT(\eta^{n-1}, a) = \mathbb{Z}[\omega]^\times$ und daher gilt $\pi_{\eta^{n-1}}(a) \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^{n-1})^\times$. Somit folgt $\pi_{\eta^{n-1}}(a^{p^{2(n-2)}(p^2-1)}) = \pi_{\eta^{n-1}}(a)^{p^{2(n-2)}(p^2-1)} = 1$.
Womit $a^{p^{2(n-2)}(p^2-1)} \equiv 1 \mod \eta^{n-1}$ folgt. Daher gibt es ein $b \in \mathbb{Z}[\omega]$ mit $a^{p^{2n-4}(p^2-1)} = 1 + b\eta^{n-1}$.
Somit gilt $a^{p^{2n-3}(p^2-1)} = (1 + b\eta^{n-1})^p$.
Damit gilt nun

$$(1 + b\eta^{n-1})^p = \sum_{i=0}^{p} \binom{p}{i} b^i \eta^{i(n-1)} = 1 + pb\eta^{n-1} + \sum_{i=2}^{p} \binom{p}{i} b^i \eta^{i(n-1)} =$$

$$1 + b\eta^n + \eta^{2(n-1)} \sum_{i=2}^{p} \binom{p}{i} b^i \eta^{(i-2)(n-1)} \equiv 1 + \eta^{2(n-1)} \sum_{i=2}^{p} \binom{p}{i} b^i \eta^{(k-2)(n-1)} \equiv 1 \mod \eta^n.$$

Wegen $n \geq 2$ gilt $2(n-1) = n + n - 2 \geq n$. Womit für jedes $a \in \mathbb{Z}[\omega]$ mit $GGT(\eta, a) = \mathbb{Z}[\omega]^\times$ folgt $a^{p^{2n-3}(p^2-1)} \equiv 1 \mod \eta^n$.
Sei nun $x \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n)^\times$ und $a \in \mathbb{Z}[\omega]$ mit $x = \pi_{\eta^n}(a)$. Dann gilt $GGT(\eta^n, a) = \mathbb{Z}[\omega]^\times$, und somit $GGT(\eta, a) = \mathbb{Z}[\omega]^\times$. Daher folgt nun

$$x^{p^{2n-3}(p^2-1)} = \pi_{\eta^n}(a)^{p^{2n-3}(p^2-1)} = \pi_{\eta^n}(a^{p^{2n-3}(p^2-1)}) = 1.$$

womit man

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

erhält.
Daher kann $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n)^\times$ nicht zyklisch sein.
(Denn sonst existiert ein $q \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n)^\times$ sodass $\langle q \rangle = (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n)^\times$. Wobei dann $ord(q) = |\langle q \rangle| = |(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n)^\times|$ gilt, was jedoch nach den eben Gezeigen nicht sein kann.)

□

Satz 4.2. *Für $\pi_3 \in \mathcal{C}$ und $n \in \mathbb{N}$ gilt: $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^n)^\times$ ist zyklisch $\iff$ $n \leq 2$.*

Beweis. Aus 2.15 folgt $\pi_3 \sim (1 - \omega)$. Sei $\Pi_{\pi_3^n} : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/\pi_3^n\mathbb{Z}[\omega]$ der kanonische Homomorphismus.

"$n = 1$" Wegen $|(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3)^\times| = \phi_{\mathbb{Z}[\omega]}(\pi_3) = N(\pi_3) - 1 = 2$ ist $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3)^\times$ eine Gruppe mit zwei Elementen. Diese wird vom Element $x \neq 1$ erzeugt (wegen $x^1 = x$ und $x^2 = 1$). Daher ist $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3)^\times$ zyklisch.

"$n = 2$" Wegen $\pi_3^2 \sim (1-\omega)^2 = 1-2\omega+\omega^2 = -3\omega+(\omega^2+\omega+1) = -3\omega$ ist zu zeigen dass $(\mathbb{Z}[\omega]/3\omega\mathbb{Z}[\omega])^\times$ zyklisch ist.
Es gilt dass $\left|(\mathbb{Z}[\omega]/\mathbb{Z}[\omega](1-\omega)^2)^\times\right| = N(1-\omega)^{2-1}(N(1-\omega)-1) = 3(3-1) = 6$. Somit ist ein Element $x \in (\mathbb{Z}[\omega]/3\omega\mathbb{Z}[\omega])^\times$ zu finden für das gilt $ord(x) = 6$.
Es gilt $1 = (\omega)(3\omega) + (1+\omega)(3-\omega)$. Daher gilt nach 2.2 $GGT(3\omega, 3-\omega) = \mathbb{Z}[\omega]^\times$. Mit 3.5 folgt nun dass $\Pi_{\pi_3^n}(3-\omega) \in (\mathbb{Z}[\omega]/3\omega\mathbb{Z}[\omega])^\times$ gilt. Für $3-\omega$ folgt nun

$ord(\Pi_{\pi_3^n}(3-\omega)) > 2$. Denn wegen

$$\frac{(3-\omega)^2-1}{3\omega} = \frac{7-7\omega}{3\omega} = \frac{7}{3}(-2-\omega)$$

gilt $(3-\omega)^2 - 1 \notin 3\omega\mathbb{Z}[\omega] = ker(\Pi_{\pi_3^n})$. Daher gilt $\Pi_{\pi_3^n}((3-\omega)^2) \neq \Pi_{\pi_3^n}(1) = 1$. Somit ist $ord(\Pi_{\pi_3^n}(3-\omega)) > 2$.

$ord(\Pi_{\pi_3^n}(3-\omega)) > 3$. Denn wegen

$$\frac{(3-\omega)^3-1}{3\omega} = \frac{16-36\omega}{3\omega} = \frac{4}{3}(-13-4\omega)$$

gilt $(3-\omega)^3 - 1 \notin 3\omega\mathbb{Z}[\omega] = ker(\Pi_{\pi_3^n})$. Daher gilt $\Pi_{\pi_3^n}((3-\omega)^3) \neq \Pi_{\pi_3^n}(1) = 1$, womit $ord(\Pi_{\pi_3^n}(3-\omega)) > 3$ folgt.

Da jedoch $ord(\Pi_{\pi_3^n}(3-\omega))$ ein Teiler von $\left|(\mathbb{Z}[\omega]/\mathbb{Z}[\omega](1-\omega)^2)^\times\right| = 6$ sein muss, bleibt nur noch $ord(\Pi_{\pi_3^n}(3-\omega)) = 6$ übrig.

"$n \geq 3$" Nach 3.8 ist $\left|(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^{n-2})^\times\right| = \phi_{\mathbb{Z}[\omega]}(\pi_3^{n-2}) = N(\pi_3)^{n-3}(N(\pi_3)-1) = 3^{n-3}2$. Weiters sei $\Pi_{\pi_3^{n-2}} : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/\pi_3^{n-2}\mathbb{Z}[\omega]$ der kanonische Homomorphismus.
Somit folgt für alle $x \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^{n-2})^\times$ dass $x^{3^{n-3}2} = 1$ gilt, denn die Ordnung eines jeden Gruppenelements teilt die Gruppenordnung von $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^{n-2})^\times$.
Sei nun $a \in \mathbb{Z}[\omega]$ beliebig mit $GGT(\pi_3, a) = \mathbb{Z}[\omega]^\times$. Dann gilt $GGT(\pi_3^{n-2}, a) = \mathbb{Z}[\omega]^\times$. Daher folgt mit 3.5, dass $\Pi_{\pi_3^{n-2}}(a) \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^{n-2})^\times$ gilt. Damit erhält man

$$\Pi_{\pi_3^{n-2}}(a^{3^{n-3}2}) = \Pi_{\pi_3^{n-2}}(a)^{3^{n-3}2} = 1_{\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^{n-2}}$$

Was gleichbedeutend mit

$$a^{3^{n-3}2} \equiv 1_{\mathbb{Z}[\omega]} \ (mod(\pi_3^{n-2}))$$

ist. Somit gibt es ein $b \in \mathbb{Z}[\omega]$ sodass

$$a^{3^{n-3}2} = 1 + b\pi_3^{n-2}$$

gilt. Damit folgt

$$a^{3^{n-2}2} = (1 + b\pi_3^{n-2})^3.$$

Wegen $\pi_3 \in \mathcal{C}$ gilt $3 = \pi_3\overline{\pi}_3$ und $\pi_3 \sim \overline{\pi}_3$. Daher gibt es ein $\epsilon \in \mathbb{Z}[\omega]^\times$ sodass $3 = \epsilon\pi_3^2$ gilt. Somit erhalten wir

$$a^{3^{n-2}2} = (1 + b\pi_3^{n-2})^3 = \sum_{k=0}^{3} \binom{3}{k} b^k \pi_3^{k(n-2)} = 1 + 3b\pi_3^{n-2} + 3b^2\pi_3^{2(n-2)} + b^3\pi_3^{3(n-2)}$$

$$= 1 + \epsilon b\pi_3^n + \epsilon\pi_3^{2(n-1)}b^2 + b^3\pi_3^{3(n-2)}$$

Wegen $n \geq 3$ folgt

$$a^{3^{n-2}2} \equiv 1 \mod (\pi_3^n).$$

Womit für alle $a \in \mathbb{Z}[\omega]$ mit $GGT(\pi_3, a) = \mathbb{Z}[\omega]^\times$ gilt $a^{3^{n-2}2} \equiv 1_{\mathbb{Z}[\omega]} \mod (\pi_3^n)$ folgt.
Sei nun $x \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^n)^\times$ und $a \in \mathbb{Z}[\omega]$ mit $x = \Pi_{\pi_3^n}(a)$. Dann ist mit 3.5 $GGT(\pi_3^n, a) = \mathbb{Z}[\omega]^\times$ und daher auch $GGT(\pi_3, a) = \mathbb{Z}[\omega]^\times$. Nun folgt mit dem Vorangegangenen, dass

$$x^{3^{n-2}2} = \Pi_{\pi_3^n}(a)^{3^{n-2}2} = \Pi_{\pi_3^n}(a^{3^{n-2}2}) = 1$$

gilt. Somit erhält mann dass

$$ord(x) \leq 3^{n-2}2 < 3^{n-1}2 = N(\pi_3)^{n-1}(N(\pi_3)-1) = \left|(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^n)^\times\right|.$$

(Wegen $x \in (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^n)^\times$ beliebig, folgt nun dass $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^n)^\times$ kein erzeugendes Element besitzen kann.) Daher ist $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_3^n)^\times$ nicht zyklisch.

□

Satz 4.3. *Seien $\eta \in \mathcal{B}$ und $p \in \mathfrak{B}$ sodass $p = \eta\overline{\eta}$, $\eta \nsim \overline{\eta}$ gelten, sowie $n \in \mathbb{N}^+$.*
Dann folgt $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n)^\times$ ist zyklisch.

Beweis. Seien $j : \mathbb{Z} \hookrightarrow \mathbb{Z}[\omega]$ die Inklusion und $\pi_{\eta^n} : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n$ der kanonische Homomorphismus.
Setzte

$$f : \begin{cases} \mathbb{Z} \to \mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n \\ a \mapsto \pi_{\eta^n}(j(a)) \end{cases}$$

dann ist f ein Ringhomomorphimus (da j und π_{η^n} Ringhomomorphismen sind). Dann folgt

$$\ker(f) = \{a \in \mathbb{Z} | \pi_{\eta^n}(j(a)) = 0\} = \{a \in \mathbb{Z} | j(a) \in \ker(\pi_{\eta^n}) = \mathbb{Z}[\omega]\eta^n\} = \{a \in \mathbb{Z} | a \in \mathbb{Z}[\omega]\eta^n\}$$

$$= \mathbb{Z} \cap \mathbb{Z}[\omega]\eta^n.$$

Zeige nun dass $p^n\mathbb{Z} = \mathbb{Z} \cap \mathbb{Z}[\omega]\eta^n$ gilt.

$\subseteq$**:** Es gilt $p^n\mathbb{Z} \subset \mathbb{Z}$ und $p^n\mathbb{Z} = \eta^n\overline{\eta^n}\mathbb{Z} \subset \mathbb{Z}[\omega]\eta^n$. Somit folgt $p^n\mathbb{Z}[\omega] \subset \mathbb{Z} \cap \mathbb{Z}[\omega]\eta^n$.

$\supseteq$**:** Sei $a \in \mathbb{Z} \cap \mathbb{Z}[\omega]\eta^n$. Dann besitzt a eine Darstellung der Form

$$a = \epsilon \cdot p^k \cdot q_1 \cdot ... \cdot q_m \quad \text{mit } \epsilon \in \{-1, 1\};\ k, m \in \mathbb{N};\ q_1, ...q_m \in \mathbb{P} \setminus \{p\}.$$

Damit gilt $a = \epsilon \cdot \eta^k\overline{\eta}^k \cdot q_1 \cdot ... \cdot q_m$. Wegen $\eta | p$ in $\mathbb{Z}[\omega]$ folgt mit 2.4 dass $\eta \nmid q_i$ in $\mathbb{Z}[\omega]$ für alle $i \in \{1, ..., m\}$. Wegen $\eta \nsim \overline{\eta}$ gilt $\eta \nmid \overline{\eta}$ in $\mathbb{Z}[\omega]$ und damit $\eta \nmid \overline{\eta}^k$. Da $\eta \in \mathcal{B}$ ist, ist η insbesondere prim in $\mathbb{Z}[\omega]$ und daher gilt $\eta \nmid \epsilon$.
Nach Vorraussetzung ist $a \in \mathbb{Z}[\omega]\eta^n$ und daher folgt $\eta^n | a$ in $\mathbb{Z}[\omega]$. Wegen der Eindeutigkeit von Satz 1.10 gilt $k \geq n$.
Also erhält man $p^n | p^k | a$ in $\mathbb{Z}$ und daher $a \in p^n\mathbb{Z}$.

Aus dem ***Homomorphiesatz der Ringtheorie*** folgt nun die Existenz eines injektiven Ringomomorphismus $\overline{f} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n$. (Denn $p^n\mathbb{Z} = ker(f)$.)
Mit $|\mathbb{Z}/p^n\mathbb{Z}| = p^n = N(\eta)^n = N(\eta^n) = |\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n|$ folgt wegen der Injektivität von $\overline{f}$ sofort die Surjektivität von $\overline{f}$. Daher ist $\overline{f}$ ein Ringisomorphismus, womit

$$\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n \cong \mathbb{Z}/p^n\mathbb{Z}$$

folgt. Somit wird durch $\overline{f}$ ein Gruppenisomorphismus $\underline{f} : (\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\eta^n)^\times$ induziert. Daher folgt

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

Wegen $p \in \mathfrak{C}$ folgt mit 1.2 und 2.10 dass $p > 2$ gilt. Daher folgt mit dem ***Satz von Gauß*** [1, Kapitel 5.5] dass $(\mathbb{Z}/p^n\mathbb{Z})^\times$ zyklisch ist. Womit die Behauptung folgt. □

Lemma 4.4. *Seien $n \in \mathbb{N}^+$ und $G_1, ..., G_n$ endliche Gruppen. Dann sind äquivalent*

1. *$G_1 \times ... \times G_n$ ist zyklisch.*
2. *$\forall i \in \{1, ..., n\}$ G_i ist zyklisch, und $\forall i, j \in \{1, ..., n\}, i \neq j$ gilt $ggT(|G_i|, |G_j|) = 1$.*

Beweis. $1 \Longrightarrow 2$ Angenommen 2 gilt nich, z.z.: 1 kann nicht gelten.

1.Fall: Sei $i \in \{1,..,n\}$ sodass G_i nicht zyklisch ist. Dann gilt für alle $g \in G_i$ existiert ein $h \in G_i$ sodass für alle $k \in \mathbb{N}^+$ $h \neq g^k$ gilt. Sei nun $\tilde{g} = (g_1, ..., g_n) \in G_1 \times ... \times G_n$ beliebig. Dann existiert ein $h_i \in G_i$ sodass für alle $k \in \mathbb{N}^+$ gilt $h_i \neq g_i^k$. Daher folgt fr alle $k \in \mathbb{N}^+$ dass $(1_{G_1}, ..., h_i, ..., 1_{G_n}) \neq \tilde{g}^k$ gilt (mit komponentenweiser Verknüpfung). Womit $\tilde{g}$ kein erzeugendes Element sein kann, und daher $G_1 \times ... \times G_n$ kein erzeigendes Element besitzt. Somit ist $G_1 \times ... \times G_n$ nicht zyklisch.

2.Fall: Seien jetzt $n \geq 2$ und $i, j \in \{1, ..., n\}, i \neq j$ mit $ggT(|G_i|, |G_j|) > 1$.
Sei nun $g = (g_i, g_j) \in G_i \times G_j$ beliebig, dann ist $g_i^{|G_i|} = 1_{G_i}$ und $g_j^{|G_j|} = 1_{G_j}$. Somit gilt dass $g^{kgV(|G_i|,|G_j|)} = (g_i^{kgV(|G_i|,|G_j|)}, g_j^{kgV(|G_i|,|G_j|)}) = (1_{G_i}, 1_{G_j}) = 1_{G_i \times G_j}$.
Wegen $ggT(|G_i|, |G_j|) > 1$ folgt

$$ord(g) \leq kgV(|G_i|, |G_j|) = \frac{|G_i|\,|G_j|}{ggT(|G_i|, |G_j|)} < |G_i|\,|G_j| = |G_i \times G_j|.$$

Daher kann g kein erzeugendes Element sein. Somit ist $G_i \times G_j$ nicht zyklisch.
Daher gilt, mit Fall 1, (wobei o.E. $j = i + 1$ gelte) dass $G_1 \times ... \times (G_i \times G_j) \times ... \times G_n$ nicht zyklisch ist. Womit folgt dass $G_1 \times ... \times G_n$ nicht zyklisch ist.

(2) $\Longrightarrow$ (1) Induktion nach n:

$n = 1$ gilt trivialerweise.

$n = 2$ Seien $m_1, m_2 \in \mathbb{N}^+$ mit $m_1 = |G_1|$ und $m_2 = |G_2|$. Aus dem ***Strukturssatz für zyklische Gruppen*** erhält man $G_1 \cong \mathbb{Z}/m_1\mathbb{Z}$ und $G_2 \cong \mathbb{Z}/m_2\mathbb{Z}$. Nach Vorraussetzung gilt $ggT(m_1, m_2) = 1$ und daher folgt mit dem ***Chinesischen Restsatz*** dass

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

gilt. Womit $G_1 \times G_2$ zyklisch ist (denn $\mathbb{Z}/m_1m_2\mathbb{Z}$ ist zyklisch).

$n \geq 3$ Sei die Behauptung für $n-1$ gezeigt. Nach Vorraussetzung ist für alle$i, j \in \{1, ..., n-1\}$ G_i zyklisch, und falls $i \neq j$ ist gilt $ggT(|G_i|, |G_j|) = 1$. Weiters ist $G_1 \times ... \times G_{n-1}$ zyklisch.
Wegen $G_1 \times ... \times G_n \cong (G_1 \times ... \times G_{n-1}) \times G_n$ und $ggT(|G_i|, |G_n|) = 1\ \forall i \in \{1, ..., n-1\}$ gilt $ggT(|G_1 \times ... \times G_{n-1}|, |G_n|) = ggT(|G_1| \cdot ... \cdot |G_{n-1}|, |G_n|) = 1$. Daher folgt mit der Induktionsvorraussetzung dass $(G_1 \times ... \times G_{n-1}) \times G_n$ zyklisch ist, und somit ist $G_1 \times ... \times G_n$ zyklisch.

□

Satz 4.5. *Sei $a \in \mathbb{Z}[\omega]$, dann ist $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a)^\times$ genau in folgenden Fällen zyklisch:*

1. $a \in \mathbb{Z}[\omega]^\times \cup \{0\}$.
2. $a \sim (1-\omega)^n$ *mit* $n \in \mathbb{N}^+$ *und* $n \leq 2$.
3. $a \sim \eta$ *mit* $\eta \in \mathcal{A}$.
4. $a \sim \eta^n$ *mit* $\eta \in \mathcal{B}$ *und* $n \in \mathbb{N}^+$.
5. $a \sim 2(1-\omega)$.

Beweis. **(1):** Sei $a \in \mathbb{Z}[\omega]^\times$. Wegen $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a = \mathbb{Z}[\omega]/\mathbb{Z}[\omega] \cong \{0\}$ folgt dass $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a)^\times \cong \{0\}^\times = \{0\} = \langle 0 \rangle$, womit $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a)^\times$ zyklisch ist.
Und falls $a = 0$ gilt so folgt $\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a \cong \mathbb{Z}[\omega]$. Daher folgt mit 1.3 $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a)^\times \cong \mathbb{Z}[\omega]^\times = \langle -\omega \rangle$.

(2,3,4): Nach 1.10 besitzt a die Darstellung

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

mit $\epsilon \in \mathbb{Z}[\omega]^\times, \alpha_\pi \in \mathbb{N}$ und $\alpha_\pi = 0$ für fast alle $\pi \in \mathcal{P}$.
Seien nun $\pi_1, \pi_2 \in \mathcal{P}$ mit $\pi_1 \neq \pi_2$. Wegen π_1, π_2 prim in $\mathbb{Z}[\omega]$ und $\pi_1 \nsim \pi_2$ gilt $GGT(\pi_1, \pi_2) = \mathbb{Z}[\omega]^\times$.

Daher folgt $GGT(\pi_1^k, \pi_2^l) = \mathbb{Z}[\omega]^\times$ für alle $k, l \in \mathbb{N}^+$. Mit 2.2 folgt $1 \in (\mathbb{Z}[\omega]\pi_1^k + \mathbb{Z}[\omega]\pi_2^l)$, womit $\mathbb{Z}[\omega] = \mathbb{Z}[\omega]\pi_1^k + \mathbb{Z}[\omega]\pi_2^l$ gilt. Daher sind die Ideale $\mathbb{Z}[\omega]\pi_1^k$ und $\mathbb{Z}[\omega]\pi_2^l$ teilerfremd. Somit folgt mit dem *Chinesischen Restsatz*

$$\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a = \mathbb{Z}[\omega]/\mathbb{Z}[\omega]\epsilon \prod_{\pi\in\mathcal{P}} \pi^{\alpha_\pi} = \mathbb{Z}[\omega]/ \prod_{\pi\in\mathcal{P}} \mathbb{Z}[\omega]\pi^{\alpha_\pi} \cong \prod_{\pi\in\mathcal{P}} \mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi^{\alpha_\pi}.$$

Daher gilt

$$(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a)^\times \cong (\prod_{\pi\in\mathcal{P}} \mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi^{\alpha_\pi})^\times = \prod_{\pi\in\mathcal{P}} (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi^{\alpha_\pi})^\times.$$

Ist $a = \epsilon\pi^\alpha$ dann treffen die Behauptungen 2,3,4 nach 4.2,4.3 und 4.4 zu.

(5): Sei nun $a = \epsilon\pi_1^{\alpha_1} \cdot ... \cdot \pi_m^{\alpha_m}$ mit $m \geq 2$. Es gilt

$$(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a)^\times \cong \prod_{i=1}^{m} (\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_i^{\alpha_i})^\times.$$

Daher muss als Vorraussetzung für $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a)^\times$ zyklisch gelten, dass für jedes $i \in \{1, ..., m\}$ $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_i^{\alpha_i})^\times$ zyklisch ist.
Somit verbleibt für $i \in \{1, ..., m\}$ nur mehr die Möglichkeiten

- $\pi_i \in \mathcal{A}$ und $\alpha_i = 1$
- $\pi_i \in \mathcal{B}$ und $\alpha_i \in \mathbb{N}$
- $\pi_i \in \mathcal{C}$ und $\alpha_i \leq 2$

Weiters müssen für die Zyklizität von $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]a)^\times$ auch die Gruppenordnungen $\phi_{\mathbb{Z}[\omega]}(\pi_i^{\alpha_i})$ aller Gruppen $(\mathbb{Z}[\omega]/\mathbb{Z}[\omega]\pi_i^{\alpha_i})^\times$ paarweise teilerfremd sein.
Für $\pi_p \in \mathcal{A}$ gilt mit 2.15 dass $p \equiv 2 \mod (3)$. Damit folgt $p^2 \equiv 4 \equiv 1 \mod (3)$, und somit gilt: $p^2 - 1 \in 3\mathbb{N}$. Für $i \in \{1, ..., m\}$ gilt:

- $\pi_i \in \mathcal{A}$ so folgt $\phi_{\mathbb{Z}[\omega]}(\pi_i^{\alpha_i}) = N(\pi_i)^{\alpha_i - 1}(N(\pi_i) - 1) = (p^2 - 1) \in 3\mathbb{N}^+$, nach dem eben gezeigten.
- $\pi_i \in \mathcal{B}$ so folgt $\phi_{\mathbb{Z}[\omega]}(\pi_i^{\alpha_i}) = N(\pi_i)^{\alpha_i - 1}(N(\pi_i) - 1) = p^{\alpha_i - 1}(p - 1) \in 3\mathbb{N}^+$, denn nach 2.15 folgt unmittelbar dass $p - 1 \in 3\mathbb{N}^+$ gilt.
- $\pi_i \in \mathcal{C}$ so folgt $\phi_{\mathbb{Z}[\omega]}(\pi_i^{\alpha_i}) = N(\pi_i)^{\alpha_i - 1}(N(\pi_i) - 1) = p^{\alpha_i - 1}(p - 1) = 2 \cdot 3^{\alpha_i - 1}$.

Daraus folgt dass in der Primfaktorzerlegung von a höchstens ein träges oder unverzweigtes Primelement auftreten kann. Als zweites Primelement ist dazu nur $1 - \omega$ möglich. Da $\phi_{\mathbb{Z}[\omega]}((1 - \omega)^2) = 6$ gilt bleibt nur noch $1 - \omega$ zu betrachten. Falls nun $\eta \in \mathcal{A}$ und $a \sim (1 - \omega)\eta$ gilt, dann folgt $\eta = \pi_p$ und $p \equiv 2 \mod (3)$. Wegen $\phi_{\mathbb{Z}[\omega]}(1 - \omega) = 2$ und $\phi_{\mathbb{Z}[\omega]}(\pi_p) = p^2 - 1$ muss $ggT(2, p^2 - 1) = 1$ gelten. Dann gelten folgende Äquivalenzen:

$$ggT(2, p^2 - 1) = 1 \Leftrightarrow p^2 - 1 \text{ ist ungerade } \Leftrightarrow p \text{ ist gerade } \Leftrightarrow p = 2$$

Womit der Punkt (5) folgt. Falls nun $\eta \in \mathcal{B}$ und $a \sim (1 - \omega)\eta^n$, mit $n \in \mathbb{N}$ gilt. Dann gilt $\eta = \pi_p$ und mit 1.2 ist $N(\pi_p) \neq 2$. Daher gilt $\phi_{\mathbb{Z}[\omega]}(\pi_p^n) = p^{n-1}(p - 1)$ ist immer gerade, womit die Ordnungen der beiden auftretenden Gruppen nicht mehr teilerfemd wären. Daher kann dies nicht auftreten.

□

Literatur

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

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