Wiederholung:

Satz 7.14: Sei $d<0$. Die Einheiten von $\mathbb{Z}[\omega_d]$ sind

$$\begin{cases} \pm 1, \pm i & \text{falls } d=-1 \\ \pm 1, \pm \omega_{-3}, \pm \omega_{-3}^2 & \text{falls } d=-3 \\ \pm 1 & \text{sonst} \end{cases}$$

Beweis: Falls $d \equiv 2,3 \bmod 4$, $x,y \in \mathbb{Z}$, gilt

$$N(x+y\sqrt{d}) = \pm 1 \iff x^2 - dy^2 = \pm 1$$

$$\iff x^2 - dy^2 = 1 \qquad (d<0)$$

$$\iff x=\pm 1, y=0 \text{ oder } x=0, y=\pm 1 \quad (\text{nur im Fall } d=-1)$$

$$\iff x+y\sqrt{d} = \pm 1 \text{ oder auch } \pm i \text{ im Fall } d=-1$$

Falls $d \equiv 1 \bmod 4$, $x,y \in \mathbb{Z}$, gilt

$$N\left(\frac{x}{2} + \frac{y\sqrt{d}}{2}\right) = \pm 1 \iff x^2 - dy^2 = \pm 4$$

$$\iff x^2 - dy^2 = 4$$

$$\iff x=\pm 2, y=0 \text{ oder } x=\pm 1, y=\pm 1 \quad (\text{nur im Fall } d=-3)$$

$$\iff \frac{x}{2} + \frac{y}{2}\sqrt{d} = \pm 1 \text{ oder auch } \frac{\pm 1 \pm \sqrt{-3}}{2} \text{ im Fall } d=-3$$

$\frac{1+\sqrt{-3}}{2} = \omega_{-3}$

$\omega_{-3}(\omega_{-3}-1) = \frac{\sqrt{-3}+1}{2} \cdot \frac{\sqrt{-3}-1}{2} = \frac{-4}{4} = -1$

$\Rightarrow \omega_{-3}^2 = \omega_{-3} - 1 = \frac{-1+\sqrt{-3}}{2}$

Daraus folgt die Behauptung □

Wie sieht es aus, wenn $d > 0$?

Das Problem ist schwieriger, da es mehrere Zahlen $z \in \mathbb{Z}[\omega_d]$ geben kann, sodass $N(z) = \pm 1$

Man beachte: Die Norm hat in diesem Fall nichts mit „Distanz von Null" in $\mathbb{R}$ zu tun.

Beispiel: $N(1+\sqrt{2}) = -1$

$(1+\sqrt{2}) \cdot (-1+\sqrt{2}) = 1$

Mit dem folgenden Lemma versuchen wir, die Anzahl der Einheiten einzuschränken

Lemma 7.15: Sei $d > 0$ und $1 < M \in \mathbb{R}$ beliebig.

Dann existieren endlich viele Einheiten $e \in \mathbb{Z}[\omega_d]$ mit $1 < e < M$

Für den Beweis brauchen wir folgendes (einfaches) Lemma:

Lemma 7.16: Sei $\alpha \in K$ mit Grad 2 und $m(X)$ sein Minimalpolynom.

Dann ist $m(X) = X^2 - Sp(\alpha)X + N(\alpha)$

Beweis: Übungsaufgabe

Beweis von Lemma 7.15: Das inverse zu e ist $\pm\sigma(e)$ (wie im Beweis von L. 7.13)

und $e > 1 \Rightarrow -1 < \sigma(e) < 1$

$\Rightarrow 0 < Sp(e) = e + \sigma(e) < M + 1$

Also hat das Minimalpolynom von α die Form

$X^2 - bX + c$ mit $b = Sp(e) \in \{1, 2, \ldots, M\}$

$c = N(e) = \pm 1$

Davon gibt es nur endlich viele, also gibt es auch nur endlich viele solche Einheiten. □

Def: Eine Grundeinheit (manchmal auch Fundamentaleinheit genannt) von $\mathbb{Z}[\omega_d]$ ist eine Einheit $\alpha \neq \pm 1$ sodass jede Einheit $\beta \in \mathbb{Z}[\omega_d]$ eine eindeutige Darstellung der Form

$$\beta = \pm \alpha^m, \quad m \in \mathbb{Z}$$

hat.

Bemerkung: Ein imaginär-quadratischer Ganzheitsring hat keine Grundeinheiten, weil die gewünschte Darstellung nie eindeutig ist.

z.B. in $\mathbb{Z}[\sqrt{-1}]$ sind die Einheiten $\pm 1, \pm i$

aber es ist z.B. $-1 = i^2 = i^6 = i^{10} = \dots$

Für reell-quadratische Ganzheitsringe ist die Situation aber ganz anders.

Lemma 7.17: Sei $d > 0$. Wenn $\mathbb{Z}[\omega_d]$ eine von ± 1 verschiedene Einheit hat, dann gibt es eine Grundeinheit

Beweis: Ist ε eine Einheit, so sind auch $-\varepsilon, \varepsilon^{-1}, -\varepsilon^{-1}$ Einheiten. Wenn es also eine von ± 1 verschiedene Einheit gibt, gibt es eine Einheit >1.

Sei α die kleinste Einheit mit $\alpha > 1$.

Es genügt zu zeigen, dass jede Einheit $\beta > 1$ die Form α^n mit $n \in \mathbb{N}^+$ hat. Dann decken $\alpha^{-n}, -\alpha^n, -\alpha^{-n}$ die Fälle $0 < \beta < 1$, $\beta < -1$ und $-1 < \beta < 0$ ab.

Angenommen β hat nicht diese Form.
Dann existiert ein $n \in \mathbb{N}^+$ sodass $\alpha^n < \beta < \alpha^{n+1}$

$$\Rightarrow 1 < \beta\alpha^{-n} < \alpha$$

Aber $\beta\alpha^{-n}$ ist eine Einheit $\lightning$ (α minimal)

Die Darstellung ist eindeutig weil $-\alpha^n < -\alpha^m < 0 < \alpha^m < \alpha^n$ für $m, n \in \mathbb{Z}$, $m < n$. $\square$

Satz 7.18: Jeder reell-quadratische Ganzheitsring hat eine Grundeinheit

Beweis: (vorläufig) ausgelassen (siehe Schmidt)

Nach Lemma 7.17 müssten wir nur zeigen, dass es eine von ± 1 verschiedene Einheit gibt.

Erinnerung: Eine Menge $I \subseteq \mathbb{Z}[\omega_d]$ ist ein Ideal wenn

(i) $I + I := \{\alpha + \beta : \alpha, \beta \in I\} \subseteq I$

(ii) $zI := \{z\alpha : \alpha \in I\} \subseteq I \quad \forall z \in \mathbb{Z}[\omega_d]$

Addition: $I_1 + I_2 := \{\alpha + \beta : \alpha \in I_1, \beta \in I_2\}$

~~Multiplikation: $I_1 \cdot I_2 := \{\alpha\beta : \alpha \in I_1, \beta \in I_2\}$~~

Wir definieren Multiplikation durch

Def: $I_1 \cdot I_2 := \{\sum_{i=1}^{n} \alpha_i \beta_i : \alpha_i \in I_1, \beta_i \in I_2, n \in \mathbb{N}^+\}$

Beachten: Das ist nicht die einfache Multiplikation von Mengen $\{\alpha\beta : \alpha \in I_1, \beta \in I_2\}$

Def: Ein Hauptideal ist ein Ideal der Form $\{\alpha z : z \in \mathbb{Z}[\omega_d]\}$

für ein $\alpha \in \mathbb{Z}[\omega_d]$

Wir schreiben $\langle \alpha \rangle$ und sprechen von dem

von α erzeugten Ideal

Wir schreiben auch $\langle \alpha, \beta \rangle$ für $\langle \alpha \rangle + \langle \beta \rangle$

Def: Die Diskriminante von $\mathbb{Z}[\omega_d]$ ist definiert durch

$$\Delta_d := \begin{cases} 4d & \text{falls } d \equiv 2, 3 \bmod 4 \\ d & \text{falls } d \equiv 1 \bmod 4 \end{cases}$$

Satz 7.19: Sei $p \in \mathbb{P} \setminus \{2\}$ und $\delta = \Delta_d$

(i) $\left(\frac{\delta}{p}\right) = 1 \Rightarrow \langle p \rangle = I_1 \cdot I_2$ mit Idealen $I_1 \neq I_2$
$I_1, I_2 \neq \mathbb{Z}[\omega_d]$

(ii) $\left(\frac{\delta}{p}\right) = -1 \Rightarrow \langle p \rangle$ ist nicht das Produkt anderer Ideale

(iii) $\left(\frac{\delta}{p}\right) = 0 \Rightarrow \langle p \rangle = I \cdot I$ mit einem Ideal I.

Beweis: (i): Es gilt $\left(\frac{\delta}{p}\right) = \left(\frac{d}{p}\right)$

$\left(\frac{d}{p}\right) = 1 \Rightarrow \exists a \in \mathbb{Z}$ mit $a^2 \equiv d \bmod p$

Es ist $(d, p) = 1$ also ist $(a^2, p) = 1$

$\Rightarrow (a, p) = 1$

$\Rightarrow (2a, p) = 1$ (p ungerade)

Es ist $2a = (a + \sqrt{d}) + (a - \sqrt{d})$

$\Rightarrow 2a \in \langle p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p} \rangle =: I$

$\Rightarrow (2a, p) = 1 \in I$

$\Rightarrow I = \mathbb{Z}[\omega_d]$

Ausserdem ist $\langle p, a+\sqrt{d} \rangle \langle p, a-\sqrt{d} \rangle$

$= \langle p^2, p(a+\sqrt{d}), p(a-\sqrt{d}), a^2-d \rangle$

$= \langle p \rangle \langle p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p} \rangle$

$= \langle p \rangle \mathbb{Z}[\omega_d]$

$= \langle p \rangle$

(ii): ausgelassen

(iii): d ist quadratfrei also gilt $p \nmid \frac{d}{p}$

$$\Rightarrow (p, \tfrac{d}{p}) = 1$$

$$\Rightarrow \langle p, \tfrac{d}{p} \rangle = \mathbb{Z}[\omega_d]$$

$$\Rightarrow \langle p, \sqrt{d}, \tfrac{d}{p} \rangle = \mathbb{Z}[\omega_d]$$

und $\langle p, \sqrt{d} \rangle^2 = \langle p^2, p\sqrt{d}, d \rangle$

$$= \langle p \rangle \langle p, \sqrt{d}, \tfrac{d}{p} \rangle$$

$$= \langle p \rangle \mathbb{Z}[\omega_d]$$

$$= \langle p \rangle$$

□