Wiederholung:

Lemma 7.9: $\forall z \in K$ gilt

(i) $N(z), Sp(z) \in \mathbb{Q}$

(ii) $z \in \mathcal{O}_K \Leftrightarrow N(z), Sp(z) \in \mathbb{Z}$

Beweis: (i) Es gilt $\sigma(N(z)) = \sigma(z\sigma(z))$

$= \sigma(z)\sigma(\sigma(z))$

$= \sigma(z)\, z$

$= N(z)$

$\Rightarrow N(z) \in \mathbb{Q}$ (L. 7.8 (iv))

und $\sigma(Sp(z)) = \sigma(z + \sigma(z))$

$= \sigma(z) + \sigma(\sigma(z))$

$= \sigma(z) + z$

$= Sp(z)$

$\Rightarrow Sp(z) \in \mathbb{Q}$.

(ii) Sei $z \in \mathcal{O}_K$ und $f(x) \in \mathbb{Z}[X]$ sein Minimalpolynom

Dann gilt $f(\sigma(z)) = \sigma(f(z))$

$= \sigma(0)$

$= 0$.

: also ist $\sigma(z) \in \mathcal{O}_K$

$\Rightarrow N(z),\ Sp(z) \in \mathcal{O}_K$ da $\mathcal{O}_K$ ein Ring ist

$\Rightarrow N(z),\ Sp(z) \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$

Andererseits, sind $N(z),\ Sp(z) \in \mathbb{Z}$, so ist das Polynom

$$f(X) = (X - z)(X - \sigma(z)) = X^2 - Sp(z)X + N(z) \in \mathbb{Z}[X]$$

und normiert mit Nullstelle z, also ist $z \in \mathcal{O}_K$ □

Bemerkung: Ist $z = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$,

dann ist $Sp(z) = 2a$

$N(z) = a^2 - db^2$

Ist $d < 0$, dann entspricht die Norm dem Quadrat der euklidischen Distanz von 0 in der komplexen Ebene.

Lemma 7.10: $\forall z_1, z_2 \in K$ gilt

(i) $N(z_1 z_2) = N(z_1) N(z_2)$

(ii) $Sp(z_1 + z_2) = Sp(z_1) + Sp(z_2)$

Beweis: (i): $N(z_1 z_2) = z_1 z_2 \sigma(z_1 z_2)$

$= z_1 z_2 \sigma(z_1) \sigma(z_2)$

$= N(z_1) N(z_2)$

(ii): ~~add~~ ähnlich □

Satz 7.11:

$$\mathcal{O}_K = \begin{cases} \{a+b\sqrt{d} : a,b \in \mathbb{Z}\} & \text{wenn } d \not\equiv 1 \bmod 4 \\ \{\frac{a+b\sqrt{d}}{2} : a,b \in \mathbb{Z},\ a \equiv b \bmod 2\} & \text{wenn } d \equiv 1 \bmod 4 \end{cases}$$

Korollar: $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] \iff d \not\equiv 1 \bmod 4$

Beweis: Sei $z = A + B\sqrt{d} \in K$, $A, B \in \mathbb{Q}$

Es gilt

$$z \in \mathcal{O}_K \iff N(z), Sp(z) \in \mathbb{Z}$$
$$\iff A^2 - dB^2,\ 2A \in \mathbb{Z}$$

Für $A, B \in \mathbb{Z}$ ist die Bedingung offensichtlich erfüllt, also ist $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K \ \forall d$.

Sei $d \equiv 1 \bmod 4$ und $A = \frac{a}{2}$, $B = \frac{b}{2}$ mit $a, b \in \mathbb{Z}$, $a \equiv b \bmod 2$.

Dann ist $2A \in \mathbb{Z}$ und $A^2 - dB^2 = \frac{1}{4}(a^2 - db^2) \in \mathbb{Z}$
(da $a^2 \equiv b^2 \equiv db^2 \bmod 4$)

also ist $\{\frac{a+b\sqrt{d}}{2} : a,b \in \mathbb{Z},\ a \equiv b \bmod 2\} \subseteq \mathcal{O}_K$

Wir müssen noch zeigen, dass es keine weiteren Zahlen in $\mathcal{O}_K$ gibt.

Sei $z \in \mathcal{O}_K \Rightarrow 2A,\ A^2 - dB^2 \in \mathbb{Z}$

$\Rightarrow 4dB^2 = (2A)^2 - 4(A^2 - dB^2) \in \mathbb{Z}$

$\Rightarrow 2B \in \mathbb{Z}$ (d quadratfrei)

also gibt es $a, b \in \mathbb{Z}$ sodass $A = \frac{a}{2}$, $B = \frac{b}{2}$

$A^2 - dB^2 \in \mathbb{Z} \Rightarrow 4 \mid (2A)^2 - d(2B)^2 = a^2 - db^2$

Für $d \not\equiv 1 \bmod 4$:

Wäre a ungerade, dann ist $a^2 \equiv 1 \bmod 4$

$\Rightarrow db^2 \equiv 1 \bmod 4$

$\Rightarrow$ b ungerade

$\Rightarrow b^2 \equiv 1 \bmod 4$

$\Rightarrow d \equiv 1 \bmod 4$ ↯

Wäre b ungerade, dann ist $b^2 \equiv 1 \bmod 4$

$\Rightarrow db^2 \equiv d \equiv 2, 3 \bmod 4$ $d \not\equiv 1 \bmod 4$ und $d \not\equiv 0 \bmod 4$ da $d \neq 0$ quadratfrei

aber $a^2 \equiv 0, 1 \bmod 4$ ↯

also sind a, b gerade $\Rightarrow A, B \in \mathbb{Z}$

Für $d \equiv 1 \bmod 4$ gilt $a^2 - db^2 \equiv 0 \bmod 4 \Leftrightarrow a^2 \equiv b^2 \bmod 4$

$\Leftrightarrow a \equiv b \bmod 2$

□

Def: Wir bezeichnen

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

Korollar 7.12: $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\omega_d]$

Beweis: Im Fall $d \equiv 2, 3 \bmod 4$ ist das nach Satz 7.11 offensichtlich.

Im Fall $d \equiv 1 \bmod 4$

$$\mathbb{Z}[\omega_d] = \{a' + b'\omega_d : a', b' \in \mathbb{Z}\} \quad \text{(S. 7.6, da } \omega_d \text{ Grad 2 hat)}$$

$$= \left\{ \frac{2a'+b'}{2} + \frac{b'}{2}\sqrt{d} : a', b' \in \mathbb{Z} \right\}$$

$$= \left\{ \frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z},\ a \equiv b \bmod 2 \right\} \quad \begin{matrix} a = 2a'+b' \\ b = b' \end{matrix}$$

$$= \mathcal{O}_{\mathbb{Q}[\sqrt{d}]} \quad \text{(S. 7.11)} \qquad \square$$

Bemerkung: Wir haben für $\mathcal{O}_K$ eine $\mathbb{Z}$-Basis gefunden, $\{1, \omega_d\}$

Für allgemeine (d.h. nicht unbedingt quadratische) Zahlkörper $\mathbb{Q}[\alpha]$ ist es ein schwieriges Problem, eine $\mathbb{Z}$-Basis für $\mathcal{O}_{\mathbb{Q}[\alpha]}$ zu bestimmen.

In der Regel gibt es kein $\omega \in \mathbb{Q}[\alpha]$, sodass $\mathcal{O}_K = \mathbb{Z}[\omega]$

Einheiten in $\mathbb{Z}[\omega_d]$

Lemma 7.13: Ein Element $\alpha \in \mathbb{Z}[\omega_d]$ ist eine Einheit genau dann, wenn $N(\alpha) = \pm 1$

äquivalent: Für $r, s \in \mathbb{Z}$ ist

im Fall $d \equiv 2, 3 \bmod 4$, $r + s\sqrt{d}$ eine Einheit von $\mathbb{Z}[\omega_d]$
$\Leftrightarrow r^2 - ds^2 = \pm 1$

im Fall $d \equiv 1 \bmod 4$, $\frac{r}{2} + \frac{s}{2}\sqrt{d}$ eine Einheit von $\mathbb{Z}[\omega_d]$
$\Leftrightarrow r^2 - ds^2 = \pm 4$.

Beweis: $\Rightarrow$: $\alpha\beta = 1 \Rightarrow N(\alpha\beta) = 1$
$\Rightarrow N(\alpha) N(\beta) = 1$

~~Falls $d \not\equiv 1 \bmod 4$ ist $N(z) \in \mathbb{Z}$ $\forall z \in \mathbb{Z}[\omega_d]$~~

$\forall z \in \mathbb{Z}[\omega_d] = \mathcal{O}_K$ ist $N(z) \in \mathbb{Z}$

$\Rightarrow N(\alpha) = N(\beta) = \pm 1$

$\Leftarrow$: Wenn $N(\alpha)=1$, dann ist $\alpha \cdot \sigma(\alpha) = N(\alpha) = 1$

Wenn $N(\alpha)=-1$, dann ist $\alpha \cdot (-\sigma(\alpha)) = -N(\alpha) = 1$

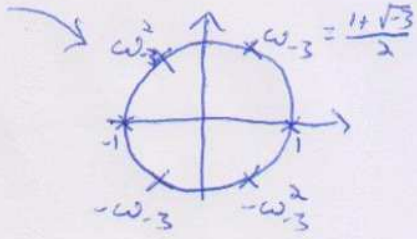
also ist $\pm\sigma(\alpha)$ das Inverse von α

also ist α eine Einheit.

Def: Ein quadratischer Zahlkörper $\mathbb{Q}[\sqrt{d}]$ (bzw. sein Ganzheitsring $\mathbb{Z}[\omega_d]$) heisst <u>reell-quadratisch</u> falls $d>0$ und <u>imaginär-quadratisch</u> falls $d<0$.

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

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



d.h. die vierten, sechsten oder zweiten