Wiederholung:

Satz 7.3: Sei $\alpha \in \bar{\mathbb{Q}}$ mit Grad n.

Dann hat der $\mathbb{Q}$-Vektorraum $\mathbb{Q}[\alpha]$ die Dimension n und $\mathbb{Q}[\alpha]$ ist ein Körper.

Beweis: Die Vektoren $1, \alpha, \dots, \alpha^{n-1}$ erzeugen $\mathbb{Q}[\alpha]$
(wie in Beweis von S. 7.2)

Wäre $b_0 \cdot 1 + b_1 \alpha + \dots + b_{n-1} \cdot \alpha^{n-1} = 0$ mit $b_i \in \mathbb{Q}$ nicht alle gleich 0

dann ist $\alpha^k + \frac{b_{k-1}}{b_k} \alpha^{k-1} + \frac{b_{k-2}}{b_k} \alpha^{k-2} + \dots + \frac{b_0}{b_k} = 0$

(k Maximal sodass $b_k \neq 0$)

Aber $k < n$, in Widerspruch zur Minimalität vom Minimalpolynom.

Also bilden $1, \dots, \alpha^{n-1}$ eine Basis der Größe n.

$\mathbb{Q}[\alpha]$ ist offensichtlich ein Ring

Sei $0 \neq \beta \in \mathbb{Q}[\alpha]$

Es ist $\beta \mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\alpha]$, also ist β algebraisch (S. 7.2, (iii)⇒(i))

: also existieren $b_i \in \mathbb{Q}$ mit $b_m \beta^m + \dots + b_0 = 0$ (Minimalpolynom)

$$\Rightarrow \frac{(b_m \beta^{m-1} + \dots + b_1)\beta}{-b_0} = 1$$ ($b_0 \neq 0$ da $\beta \neq 0$ und wegen Minimalität)

und $\frac{b_m}{-b_0}\beta^{m-1} + \dots + \frac{b_1}{-b_0} \in \mathbb{Q}[\alpha]$ (da $\beta \in \mathbb{Q}[\alpha]$ und $\mathbb{Q}[\alpha]$ ein Ring)

also ist β in $\mathbb{Q}[\alpha]$ invertierbar, also ist $\mathbb{Q}[\alpha]$ ein Körper ($\beta \neq 0$ war beliebig) □

Satz 7.4: Die quadratischen Zahlkörper sind die Körper $\mathbb{Q}[\sqrt{d}]$ wobei $0, 1 \neq d \in \mathbb{Z}$ und d quadratfrei ist. Alle diese Körper sind verschieden.

Beispiele: $\mathbb{Q}[\sqrt{-1}] = \{a+bi : a, b \in \mathbb{Q}, i^2 = -1\}$

$$\mathbb{Q}[3+\sqrt{\tfrac{1}{2}}] = \mathbb{Q}[\sqrt{\tfrac{1}{2}}]$$
$$= \mathbb{Q}[\tfrac{1}{2}\sqrt{2}]$$
$$= \mathbb{Q}[\sqrt{2}]$$

Beweis: dass $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{q}]$ mit $q \in \mathbb{Q}$:

Sei $\alpha \in \overline{\mathbb{Q}}$ mit Grad 2

und $m(X) = X^2 + bX + c$ das Minimalpolynom von α.

: Dann ist $\alpha = \frac{-b \pm \sqrt{b^2-4c}}{2}$

$= \frac{-b}{2} \pm \sqrt{\frac{b^2}{4}-c}$

Es ist $\frac{-b}{2} \in \mathbb{Q}$ und $-1 \in \mathbb{Q}$, also ist

$\mathbb{Q}[\alpha] = \mathbb{Q}\left[\frac{-b}{2} \pm \sqrt{\frac{b^2}{4}-c}\right] = \mathbb{Q}\left[\sqrt{\frac{b^2}{4}-c}\right]$

und $\frac{b^2}{4}-c \in \mathbb{Q}$.

dass $\mathbb{Q}[\sqrt{q}] = \mathbb{Q}[\sqrt{z}]$ mit $z \in \mathbb{Z}$:

Sei $\frac{b^2}{4}-c = \frac{s}{t}$ mit $s, t \in \mathbb{Z}$

$t > 0$

$(s,t) = 1$.

Es ist $\sqrt{\frac{s}{t}} = \frac{1}{t}\sqrt{st}$, also ist $\mathbb{Q}[\sqrt{\frac{s}{t}}] = \mathbb{Q}[\sqrt{st}]$.

dass $\mathbb{Q}[\sqrt{z}] = \mathbb{Q}[\sqrt{d}]$ mit $d \in \mathbb{Z}$ quadratfrei:

Sei $st = de^2$ mit $d, e \in \mathbb{Z}$, d quadratfrei

Dann ist $\mathbb{Q}[\sqrt{st}] = \mathbb{Q}[e\sqrt{d}]$

$= \mathbb{Q}[\sqrt{d}]$

Ist $d = 0, 1$, dann ist $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{d}] = \mathbb{Q}$,

also $\alpha \in \mathbb{Q}$, aber dann hat α Grad 1 $\lightning$ (Nullstelle von $X-\alpha$)

Also ist $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{d}]$ mit $0, 1 \neq d \in \mathbb{Z}$ quadratfrei.

dass alle verschieden sind:

Angenommen $d \neq d'$ für $0, 1 \neq d, d' \in \mathbb{Z}$ quadratfrei

aber $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{d'}]$

Dann ist $\sqrt{d'} = a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$

$$\Rightarrow d' = (a^2 + b^2 d) + 2ab\sqrt{d}$$

Da $d \neq 0, 1$ quadratfrei ist, ist $ab = 0$

(sonst wäre $2ab\sqrt{d} \notin \mathbb{Z}$)

Wäre $a = 0$, dann wäre $d' = b^2 d$

$$\Rightarrow b = \pm 1 \quad (d' \text{ quadratfrei}, d' \neq 0)$$

$$\Rightarrow d' = d \quad \lightning$$

Wäre $b = 0$, dann wäre $d' = a^2$

$$\Rightarrow a = \pm 1$$

$$\Rightarrow d' = 1 \quad \lightning$$

□

Def: Ein $\mathbb{Z}$-Modul M ist eine abelsche Gruppe mit einer Multiplikation $\mathbb{Z} \times M \to M$ sodass $\forall z_1, z_2 \in \mathbb{Z}$ $\forall m_1, m_2 \in M$ gilt:

(i) $z_1(m_1 + m_2) = z_1 m_1 + z_1 m_2$

(ii) $(z_1 + z_2) m_1 = z_1 m_1 + z_2 m_1$

(iii) $(z_1 z_2) m_1 = z_1 (z_2 m_1)$

Intuition: Ein Modul ist ein „Vektorraum über einen Ring" (anstatt über einen Körper).

Ein $\mathbb{Z}$-Modul ist endlich erzeugt falls es endlich viele Elemente $m_1, \dots, m_n \in M$ gibt, sodass $\forall m \in M$ eine Darstellung $m = a_1 m_1 + \dots + a_n m_n$ mit $a_i \in \mathbb{Z}$ existiert.

Die folgenden zwei Sätze sind analog zu den Sätzen 7.2 und 7.3, aber für ganz-algebraische Zahlen.

Die Beweise sind ausgelassen, aber analog zu den ursprünglichen.

Satz 7.5: Für eine Zahl $\alpha \in \mathbb{C}$ sind die folgenden Aussagen äquivalent:

(i) $\alpha \in \mathcal{O}$

(ii) Der $\mathbb{Z}$-Modul $\mathbb{Z}[\alpha]$ ist endlich erzeugt

(iii) Es existiert ein endlich erzeugter $\mathbb{Z}$-Modul $\{0\} \neq M \subseteq \mathbb{C}$ mit $\alpha M \subseteq M$.

Satz 7.6: Sei $\alpha \in \mathcal{O}$ mit Grad n.

Dann ist der $\mathbb{Z}$-Modul $\mathbb{Z}[\alpha]$ von $1, \alpha, \dots, \alpha^{n-1}$ erzeugt.

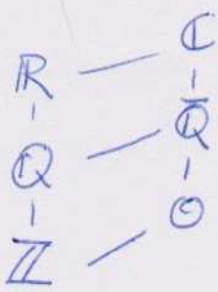
Korollar 7.7: (Korollar zu den Sätzen 7.2 und 7.5)

Die Summe und das Produkt zweier algebraischer (bzw. ganz-algebraischer) Zahlen ist algebraisch (bzw. ganz-algebraisch).

$\overline{\mathbb{Q}}$ ist ein Körper

$\mathcal{O}$ ist ein Ring

Beweis: Aufgabe.



Def: Für ein algebraischer Zahlkörper K:

$\mathcal{O}_K := K \cap \mathcal{O}$ heißt der <u>Ring der ganzen Zahlen von K</u>

(oder <u>Ganzheitsring von K</u>)

z.B. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$

Ein wichtiges Ziel ist, $\mathcal{O}_K$ zu bestimmen.

Wegen Korollar 7.7 ist $\mathcal{O}_K$ ein Ring.

Es ist $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$, aber die andere Richtung gilt nicht unbedingt.

z.B. sei $z = \frac{-1+\sqrt{-3}}{2}$.

Es ist $z(z+1) = -1$ also $z \in \mathcal{O}_{\mathbb{Q}[\sqrt{-3}]}$

Aber $z \notin \mathbb{Z}[\sqrt{-3}]$

Von nun an sei $d \in \mathbb{Z} \setminus \{0,1\}$, d quadratfrei fixiert

und $K = \mathbb{Q}[\sqrt{d}]$

Def: Für $z = x + y\sqrt{d} \in K$ $(x, y \in \mathbb{Q})$ definieren wir das

<u>konjugierte Element</u> $\sigma(z)$ zu z durch

$$\sigma(z) := x - y\sqrt{d}$$

Bemerkung: Falls $d < 0$ entspricht σ der komplexen Konjugation.

Lemma 7.8: $\forall z, z' \in K$ gilt

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

(ii) $\sigma(zz') = \sigma(z)\sigma(z')$

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

(iv) $z \in \mathbb{Q} \Leftrightarrow \sigma(z) = z$

Beweis: Einfaches Verifizieren

Def: Für $z \in K$ ist die <u>Norm</u> $N(z)$ von z definiert durch

$$N(z) := z\sigma(z)$$

und die <u>Spur</u> $Sp(z)$ von z durch

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

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: Nächstes Mal.