B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

1.Vorlesung

13. April 2021

Wir werden in diesem Skript die gleiche Notationen, Definitionen, Begriffe und Terminologie (von Skript B1, B2 und B3) implizit und stillschweigend beibehalten und verwenden.
In dieser Vorlesung B4; Algebra II werden wir die Einführung in die Algebra der B3 fortsetzen. Wir werden ***Moduln*** *über Hauptidealringe studieren, und die Theorie der Körpererweiterungen auf Ringerweiterungen übertragen. Insbesondere werden wir* ***Ganze Ringerweiterungen*** *sowie* ***Dedekindringe*** *genau untersuchen. Diese Themen dienen zur Vorbereitung zur algebraischen Zahlentheorie, wo diese algebraische Klassen eine wesentliche Rolle spielen. Als Motivation, Leitmotiv, und wichtiges Beispiel führen wir in Kapitel 1 quadratische Zahlkörper ein.*

Kapitel 1: Quadratische Zahlkörper

Definition 1.1 i) Ein Zahlkörper ist eine endliche Körpererweiterung Erweiterung K von $\mathbb{Q}$.

ii) $[K : \mathbb{Q}]$ heißt der Grad des Zahlkörpers.

iii) eine algebraische Zahl ist ein Element $\alpha \in K$.

iv) $\alpha \in K$ ist eine ganze (algebraische) Zahl, wenn es ein Polynom $m(x) \in \mathbb{Z}[x]$ gibt mit $m(x)$ normiert und $m(\alpha) = 0$.

Bemerkung 1.1
Wir werden gleich zeigen dass die Menge $\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ ganz } \}$ ein Ring ist. Algebraische Zahlentheorie studiert die Arithmetik vom Zahlkörper K, den Ring $\mathcal{O}_K$, seine Ideale, Einheiten und Faktorisierungseigenschaften.

Proposition 1.1
Sei K ein Zahlkörper. Es gilt: $\alpha \in \mathcal{O}_K \iff \text{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$. Insbesondere ist $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Beweis. „$\Leftarrow$“: klar.

„$\Rightarrow$“: Sei $\alpha \in \mathcal{O}_K$ und $f(x)$ normiert von minimalem Grad in $\mathbb{Z}[x]$, so dass α eine Nullstelle von $f(x)$ ist. Wenn $f(x)$ reduzibel in $\mathbb{Q}[x]$ ist, liefert dann das Lemma von Gauss, dass $f(x)$ reduzibel in $\mathbb{Z}[x]$ ist, also $f(x) = g(x)h(x)$ mit $g, h \in \mathbb{Z}[x]$ normiert, $\deg(g), \deg(h) < \deg(f)$ und $g(\alpha) = 0$ oder $h(\alpha) = 0$: Widerspruch. Also ist $f(x)$ irreduzibel in $\mathbb{Q}[x]$. Die Eindeutigkeit von $\text{MinPol}_{\mathbb{Q}}(\alpha)$ ergibt nun $f(x) = \text{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$.

Sei $\alpha = \frac{r}{s} \in \mathbb{Q}$, dann ist $\text{MinPol}_{\mathbb{Q}}(\alpha) = x - \frac{r}{s}$, $r, s \in \mathbb{Z}$, $ggT(r, s) = 1$. Nun ist
$x - \frac{r}{s} \in \mathbb{Z}[x] \Leftrightarrow s = 1 \Leftrightarrow \alpha \in \mathbb{Z}$. □

Wir sehen also: $K = \mathbb{Q} \Rightarrow \mathcal{O}_K = \mathbb{Z}$. Wie berechnet man $\mathcal{O}_K$ im Allgemeinen? Wir werden diese Frage für quadratische Zahlkörper (Zahlkörper vom Grad 2) untersuchen. Wir werden die folgende Definition benötigen.

Definition 1.2
$D \in \mathbb{Z}$ ist quadratfrei, falls D ein Produkt von verschiedenen Primzahlen ist.

Beispiel 1.1 (Quadratische Körpererweiterungen)
Sei F ein Körper mit $\mathrm{Char}(F) \neq 2$, und K/F eine Körpererweiterung mit $[K : F] = 2$.
Sei $\alpha \in K \backslash F$. Dann gibt es $b, c \in F$ so dass $\mathrm{MinPol}_F(\alpha) = x^2 + bx + c$. Also ist $K = F(\alpha)$ weil $[K : F] = 2$. Die Nullstellen sind $\frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$ ($\mathrm{Char}(F) \neq 2$). Setze $D := b^2 - 4c \in F$.
Also gilt $K = F(\sqrt{D})$ und $D \in F$ ist kein Quadrat.

Zusatz: wenn $F = \mathbb{Q}$ gilt, kann man o.E. $D \in \mathbb{Z}$ sogar quadratfrei wählen.

Beweis. Sei $D = \frac{\prod p_i^{\nu_i}}{\prod p_i^{\mu_i}} = \prod p_i^{\epsilon_i} \in \mathbb{Q}$, $\epsilon_i \in \mathbb{Z}$, $p_i \in \mathbb{Z}$ Primzahlen, $p_i \neq p_j$ wenn $i \neq j$.

Behauptung: O.E. gilt $\epsilon_i = 1$.

Diese Behauptung gilt weil $\epsilon_i = 2\rho_i$ oder $\epsilon_i = 2\rho_i + 1$, $p_i \in \mathbb{Z}$, also

$$D = \prod_{i \in I} p_i^{2\rho_i} \prod_{j \in J} p_j^{2\rho_j + 1} \Rightarrow D = \prod_{i \in I} p_i^{2\rho_i} \prod_{j \in J} p_j^{2\rho_j} \underbrace{\prod_{j \in J} p_j}_{:= D' \text{ ist quadratfrei}}$$

Damit ist aber $\sqrt{D} = \underbrace{\prod p_i^{\rho_i} \prod p_j^{\rho_j}}_{\in \mathbb{Q}} \sqrt{D'}$ und $K = \mathbb{Q}(\sqrt{D'})$. □

Proposition 1.2
Sei K ein quadratische Zahlkörper und setze also $K := \mathbb{Q}(\sqrt{D})$ mit D quadratfrei. Die Menge $\mathcal{O}_K$ der ganzen (algebraischen) Zahlen ist ein Ring und zwar

$$\mathcal{O}_K = \mathbb{Z}[\omega] := \{r + s\omega \mid, r, s \in \mathbb{Z}\}$$
$$\text{wobei } \omega := \begin{cases} \sqrt{D} \text{ wenn } D \equiv 2, 3 \bmod 4 \\ \frac{1+\sqrt{D}}{2} \text{ wenn } D \equiv 1 \bmod 4 \end{cases}$$

Beweis. Bemerke dass $D \equiv 0 \bmod 4$ nicht möglich ist.
• Wir prüfen zunächst dass $\mathbb{Z}[\omega]$ ein Ring ist: $\mathbb{Z}[\omega]$ abgeschlossen unter Addition ist klar. Wenn $\omega = \sqrt{D}$ ist es auch klar, dass $\mathbb{Z}[\omega]$ abgeschlossen unter Multiplikation ist.
Wenn $\omega = \frac{1+\sqrt{D}}{2}$ berechne
$(r + s\frac{1+\sqrt{D}}{2})(t + u\frac{1+\sqrt{D}}{2}) = \underbrace{(rt + su\frac{D-1}{4})}_{\in \mathbb{Z} \text{ weil } D \equiv 1 \bmod 4} + \underbrace{(ru + st + su)}_{\in \mathbb{Z}} \frac{1+\sqrt{D}}{2} \in \mathbb{Z}[\omega]$.
• Nun zeigen wir $\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$. Bemerke dass wenn $\alpha \in K$, $\alpha \notin \mathbb{Q}$, dann ist $\alpha = a + b\sqrt{D}$ (mit $a, b \in \mathbb{Q}$), und $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = x^2 - 2ax + (a^2 - b^2 D)$.
Sei nun $\alpha = r + s\omega \in \mathbb{Z}[\omega]$, $r, s \in \mathbb{Z}$, o.E. $s \neq 0$. Es genügt zu zeigen, dass $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$ (s. Proposition 1.1).

Fall 1: $D \equiv 2, 3 \bmod 4$
$\alpha = r + s\sqrt{D}$, $r, s \in \mathbb{Z}$, also $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = \underbrace{x^2 - 2rx + (r^2 - s^2 D)}_{\in \mathbb{Z}[x]}$.

Fall 2: $D \equiv 1 \bmod 4$
$\alpha = r + s\frac{1+\sqrt{D}}{2} = \underbrace{(r + \frac{s}{2})}_{:=a} + \underbrace{(\frac{s}{2})}_{:=b}\sqrt{D}$, $a, b \in \mathbb{Q}$.

Also ist $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = x^2 - 2(r+\frac{s}{2})x + ((r+\frac{s}{2})^2 - (\frac{s}{2})^2 D) = x^2 - 2\underbrace{(r + \frac{s}{2})}_{\in\mathbb{Z}}x + \underbrace{(r^2 + rs + s^2\frac{1-D}{4})}_{\in\mathbb{Z}}$.

• Nun zeigen wir $\mathcal{O}_K \subseteq \mathbb{Z}[\omega]$. Sei $\alpha = a + b\sqrt{D} \in \mathcal{O}_K$, $a, b \in \mathbb{Q}$. Falls $b = 0$, dann ist $\alpha \in \mathbb{Q}$ und Proposition 1.1 impliziert $\alpha \in \mathbb{Z}$, also $\alpha \in \mathbb{Z}[\omega]$. Also gilt o.E. $b \neq 0$ ($\alpha \notin \mathbb{Q}$). Betrachte $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = x^2 - 2ax + (a^2 - b^2 D)$. Proposition 1.1 impliziert $2a \in \mathbb{Z}$ und $a^2 - b^2 D \in \mathbb{Z}$. Dann ist $4b^2 D \in \mathbb{Z}$, weil $\underbrace{4(a^2 - b^2 D)}_{\in\mathbb{Z}} = \underbrace{(2a)^2}_{\in\mathbb{Z}} - (2b)^2 D$. Nun ist aber D quadratfrei, also $2b \in \mathbb{Z}$.
Setze also $a := \frac{x}{2}$ und $b = \frac{y}{2}$, $x, y \in \mathbb{Z}$, also $x^2 - y^2 D = 4(a^2 - b^2)D$ und damit erhalten wir $x^2 - y^2 D \equiv 0 \bmod 4$, also

$$(*) \qquad y^2 D \equiv x^2 \bmod 4$$

D.h.: $y^2 D$ ist ein Quadrat mod 4.
Die Quadrate mod 4 sind 0 und 1, also gilt entweder

$$\begin{aligned} (1) \quad & y^2 D \equiv 0 \bmod 4 \\ \text{oder } (2) \quad & y^2 D \equiv 1 \bmod 4 \end{aligned}$$

Fall (1): $y^2 D \equiv 0 \bmod 4$ impliziert:

- entweder $y^2 \equiv 0 \bmod 4$; dann ist $x^2 \equiv 0 \bmod 4$ wegen $(*)$, also $x, y \equiv 0 \bmod 2$
- oder $y^2 \equiv D \equiv 2 \bmod 4$: unmöglich, weil 2 kein Quadrat mod 4 ist.

Fall (2): $y^2 D \equiv 1 \bmod 4$ $(**)$:

y^2, D sind in $\mathbb{Z}_4^\times$, also entweder 1 oder 3, also gilt:

- entweder $y^2 \equiv D \equiv 1 \bmod 4$ also $y \equiv 1 \bmod 2$, also mit $(*) + (**)$: $x \equiv 1 \bmod 2$
- oder $y^2 \equiv D \equiv 3 \bmod 4$: unmöglich, weil 3 kein Quadrat mod 4 ist.

Wir haben also gezeigt, die folgenden Fälle sind möglich:

(1) $D \equiv 1, 2, 3 \bmod 4$ und x, y beide gerade

oder

(2) $D \equiv 1 \bmod 4$ und x, y beide ungerade.

Das heißt:

(i) $D \equiv 2, 3 \bmod 4$ und x, y beide gerade

oder

(ii) $D \equiv 1 \bmod 4$ und x, y beide ungerade oder beide gerade.

Im Fall (i): $\omega = \sqrt{D}$, $a = \frac{x}{2}, b = \frac{y}{2} \in \mathbb{Z}$ und damit $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\omega]$.
Im Fall (ii): $\omega = \frac{1+\sqrt{D}}{2}$, $\alpha = a + b\sqrt{D} = r + s\omega$ mit $r := \frac{x-y}{2} \in \mathbb{Z}$ und $s := y \in \mathbb{Z}$. □