Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

1.Vorlesung

24. April 2017

Kapitel 1: Quadratische Zahlkörper

1. Der Ring der ganzen algebraischen Zahlen $\mathbb{Z}[\omega]$
2. Die Einheitsgruppe $\mathbb{Z}[\omega]^\times$

Definition 1.1 i) Ein Zahlkörper ist eine endliche 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 $m(\alpha) = 0$.

Algebraische Zahlentheorie studiert die Arithmetik von Zahlkörpern, den Ring $\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ ganz }\}$, seine Ideale, Einheiten und Faktorisierung.

Sei K ein Zahlkörper.

Proposition 1.1
$\alpha \in K$ ist ganz $\iff$ $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$.
Insbesondere: $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$

Beweis. „$\Leftarrow$“: klar
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 $\mathrm{MinPol}_{\mathbb{Q}}(\alpha)$ ergibt nun $f(x) = \mathrm{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$.
Sei $\alpha = \frac{r}{s} \in \mathbb{Q}$, dann ist $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = x - \frac{r}{s}$, $r, s \in \mathbb{Z}$, $ggT(r, s) = 1$. 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?

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

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

Zusatz: wenn $F = \mathbb{Q}$ gilt, kann man o.E. $D \in \mathbb{Z}$ mit D 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 $\epsilon_i = 1$:

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 $K = \mathbb{Q}(\sqrt{D'})$. □

Setze also $K := \mathbb{Q}(\sqrt{D})$ mit D quadratfrei.

Proposition 1.2
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. NB: $D \equiv 0 \bmod 4$ ist nicht möglich.
Beobachte: $\mathbb{Z}[\omega]$ ist ein Ring; abgeschlossen unter Addition ist klar, und unter Multiplikation wenn $\omega = \sqrt{D}$ ist auch klar! Für $\omega = \frac{1+\sqrt{D}}{2}$ 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 $\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$. Beobachte, dass:
Für $\alpha \in K, \alpha \notin \mathbb{Q}$, $\alpha = a + b\sqrt{D}$, $a, b \in \mathbb{Q}$, ist $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = x^2 - 2ax + (a^2 - b^2 D)$.
Nun sei $\alpha = r + s\omega \in \mathbb{Z}[\omega]$, $r, s \in \mathbb{Z}$, o.E. $s \neq 0$. Proposition 1.1 impliziert: Es genügt zu zeigen, dass $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$.

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.
Fortsetzung des Beweises in der 2.Vorlesung. □