

- Algebraische Zahlentheorie -

Algebra BIV
SS 2013
~ Kuhlmann. ~

Inhaltsverzeichnis und voraussichtliche Terminplanung:

- Kapitel 1 Quadratische Zahlkörper
 15.04 - 22.04
- Kapitel 2 Moduln
 22.04 - 02.05
- Kapitel 3 Der Ganzheitsring $\mathcal{O}_K$
 06.05 - 23.05
- Kapitel 4 Dedekindringe
 27.05 - 17.06
- Kapitel 5 Klassenzahl
 20.06 - 01.07
- Kapitel 6 Die Einheitsgruppe $\mathcal{O}_K^\times$
 04.07
- Kapitel 7 Kreisteilungs Zahlkörper
 08.07 - 18.07
(falls die Zeit reicht).

- Algebraische Zahlentheorie -

- Algebra B4 -

- Kuhlmann -

01. Vorlesung am 15.04.2013

Kapitel 1: Quadratische Zahlkörper

§ 1. Der Ring der ganzen
algebraischen Zahlen
 $\mathbb{Z}[\omega]$.

§ 2. Die Einheitsgruppe $\mathbb{Z}[\omega]^\times$.

Definition 1.

- (i) ein Zahlkörper ist eine endliche Erweiterung K von $\mathbb{Q}$.
- (ii) $n := [K : \mathbb{Q}]$ heißt 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,
 $m(x)$ 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. $d \in K$ ist ganz $\Leftrightarrow \text{Min Pol}_Q d \in \mathbb{Z}[x]$

Insbesondere $\mathcal{O}_Q = \mathbb{Z}$.

Beweis " $\Leftarrow$ " klar!

Sei $d \in \mathcal{O}_K$; $f(x)$ normiert von minimalen Grad in $\mathbb{Z}[x]$ so dass d eine N.S von $f(x)$ ist.

Wenn $f(x)$ reduzibel in $\mathbb{Q}[x]$ ist, dann liefert das Lemma von Gauß

dass $f(x)$ reduzibel in $\mathbb{Z}[x]$ ist, also

$$f(x) = g(x) h(x)$$

$g, h \in \mathbb{Z}[x]$ normiert

$\deg g < \deg f$ und

$\deg h < \deg f$

also $g(d) = 0$ oder $h(d) = 0$ $\Downarrow$

Also $f(x)$ irreduzibel in $\mathbb{Q}[x]$. Die Eindeutigkeit

des $\text{Min Pol}_Q d$ ergibt nun $f(x) = \text{Min Pol}_Q d \in \mathbb{Z}[x]$.

Sei $d = \frac{r}{s} \in \mathbb{Q}$, dann ist Min Pol $d = x - \frac{r}{s}$.
 $r, s \in \mathbb{Z}$
 $\text{ggT}(r, s) = 1$

Nun ist $x - \frac{r}{s} \in \mathbb{Z}[x] \Leftrightarrow s = 1 \Leftrightarrow d \in \mathbb{Z}$. $\square$

Wir sehen also: $K = \mathbb{Q} \Rightarrow \mathcal{O}_K = \mathbb{Z}$.

Wie berechnet man $\mathcal{O}_K$ i. a.?

Beispiel. Quadratische Zahlkörper.
Zahlkörper von Grad 2: Betrachte i. a.:
Sei F ein Körper, $\text{Char}(F) \neq 2$
 K / F Körpererweiterung,
 $[K : F] = 2$.

Sei $d \in K$ dann ist Min Pol $d = x^2 + bx + c$
 $d \notin F$ F $b, c \in F$

Also $K = F(d)$ weil $[F(d) : F] = 2$ bereits.

Die NS sind

$$\frac{1}{2} \left(-b \pm \sqrt{b^2 - 4c} \right) \quad (\text{Char } F \neq 2).$$

Setze $D := (b^2 - 4c) \in F$

Also gilt $K = F(\sqrt{D})$ und $D \in F$ ist kein Quadrat. $\square$

Definition 2. $D \in \mathbb{Z}$ ist quadratfrei

falls D ein Produkt von verschiedenen
Primzahlen ist.

Zusatz: $F = \mathbb{Q}$ so kann man $\exists$

$D \in \mathbb{Z}$ und D quadratfrei wählen.

Beweis. Sei $D = \frac{\prod p_i^{\nu_i}}{\prod p_i^{\mu_i}} = \prod p_i^{\varepsilon_i}$

$D \in \mathbb{Q}$.

Also $D = \prod p_i^{\varepsilon_i} \quad \varepsilon_i \in \mathbb{Z};$

$p_i \in \mathbb{Z}$ Primzahlen; $p_i \neq p_j$ wenn

$i \neq j$.

→ Beh:

$\exists \varepsilon_i = 1$ weil $\varepsilon_i = 2p_i$ oder $\varepsilon_i = 2p_i + 1$

$p_i \in \mathbb{Z}$. Also $D = \prod_{i \in I} p_i^{2p_i} \prod_{j \in J} p_j^{2p_j+1}$

$$\Rightarrow D = \left[\prod_{i \in I} p_i^{2p_i} \prod_{j \in J} p_j^{2p_j} \right] \prod_{j \in J} p_j \quad \leftarrow \quad \text{=: } D' \text{ quadratfrei.}$$

Damit ist aber $\sqrt{D} = \underbrace{\left[\prod_{i \in I} p_i^{p_i} \prod_{j \in J} p_j^{p_j} \right]}_{\in \mathbb{Q}} \sqrt{D'}$ und
 $K = \mathbb{Q}(\sqrt{D})$.

Setze also $K = \mathbb{Q}(\sqrt{D})$; $D \in \mathbb{Z}$; quadratfrei.

Proposition 2. Die Menge $\mathcal{O}_K$ der ganzen

(alg.) Zahlen ist ein Ring und zwar

$$\mathcal{O}_K = \mathbb{Z}[\omega] := \{r + s\omega \mid r, s \in \mathbb{Z}\}$$

wobei

$$\omega := \begin{cases} \sqrt{D} & \text{wenn } D \equiv 2, 3 \pmod{4} \\ \frac{1 + \sqrt{D}}{2} & \text{wenn } D \equiv 1 \pmod{4} \end{cases} \quad \begin{matrix} \text{NB:} \\ D \equiv 0 \pmod{4} \end{matrix}$$

Beweis: NB: $D \equiv 0 \pmod{4}$ 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

$$\left[r + s \left(\frac{1 + \sqrt{D}}{2} \right) \right] \left[t + u \left(\frac{1 + \sqrt{D}}{2} \right) \right] =$$

$$\underbrace{\left[rt + su \left(\frac{D-1}{4} \right) \right]}_{\in \mathbb{Z} \text{ weil } D \equiv 1 \pmod{4}} + \underbrace{(ru + st + su)}_{\in \mathbb{Z}} \frac{1 + \sqrt{D}}{2} \in \mathbb{Z}[\omega].$$

Nun zeigen wir $\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$.

Beobachte daß:

$$\begin{array}{lcl} \text{Für } d \in K; & d = a + b\sqrt{D} \\ d \in \mathbb{Q}; & a, b \in \mathbb{Q} \end{array}$$

$$\text{ist Min Pol}_{\mathbb{Q}} d = x^2 - 2ax + (a^2 - b^2D).$$

$$\begin{array}{l} \text{Nun sei } d = r + s\omega \in \mathbb{Z}[\omega], \\ r, s \in \mathbb{Z} \\ \text{OE } s \neq 0 \end{array}$$

Prop 1 $\Rightarrow$ es genügt zu zeigen $\text{Min Pol}_{\mathbb{Q}} d \in \mathbb{Z}[x]$.

Fall 1. $D \equiv 2, 3 \pmod{4}$.

$$\begin{array}{l} d = r + s\sqrt{D} \Rightarrow \text{Min Pol}_{\mathbb{Q}} d = x^2 - 2rx + (r^2 - s^2D) \\ r, s \in \mathbb{Z} \end{array} \quad \underbrace{\qquad\qquad\qquad}_{\in \mathbb{Z}[x]}$$

Fall 2. $D \equiv 1 \pmod{4}$.

$$d = r + s \left(\frac{1 + \sqrt{D}}{2} \right) =$$

$$\underbrace{\left(r + \frac{s}{2} \right)}_{=: a} + \underbrace{\left(\frac{s}{2} \right)}_{=: b} \sqrt{D}$$

$$=: a$$

$$=: b$$

$$a, b \in \mathbb{Q}$$

Also ist

Min Pol_Q d =

$$x^2 - 2(r + s/2)x + [(r + s/2)^2 - (s/2)^2 D]$$

$$= x^2 - \underbrace{2(r + s/2)}_{\in \mathbb{Z}} x + \underbrace{\left[r^2 + rs + s^2 \left(\frac{1-D}{4} \right) \right]}_{\in \mathbb{Z}}$$

Nun zeigen wir $\mathcal{O}_K \subseteq \mathbb{Z}[\omega]$.

Sei $d = a + b\sqrt{D}$, $d \in \mathcal{O}_K$.

$$a, b \in \mathbb{Q}$$

$$d \in K$$

Falls $b = 0$ dann ist $d \in \mathbb{Q}$ und Prop 1 impliziert $d \in \mathbb{Z}$; also $d \in \mathbb{Z}[\omega]$.

Also ist $b \neq 0$ ($d \notin \mathbb{Q}$).

Betrachte Min Pol_Q d = $x^2 - 2ax + (a^2 - b^2 D)$

Prop 1 $\Rightarrow$ $\boxed{2a \in \mathbb{Z}}$ 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

$$\boxed{2b \in \mathbb{Z}}$$

Setze also $a := x/2$ $b := y/2$

$$x, y \in \mathbb{Z}$$

$$\text{Also } x^2 - y^2 D = 4(a^2 - b^2 D)$$

und damit erhalten wir

$$x^2 - y^2 D \equiv 0 \pmod{4}$$

$$\text{oder } y^2 D \equiv x^2 \pmod{4} \quad (*)$$

D.h. $y^2 D$ ist ein Quadrat mod 4.

Fortsetzung des Beweises in der

2. Vor am 18. 04. 2013 ...