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

# 2.Vorlesung

27. April 2017

*Beweis Fortsetzung.* Die Quadrate mod 4 sind 0 und 1, also gilt entweder

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

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:

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

## §Faktorisierung in $\mathcal{O}_K$?

$\mathbb{Z} = \mathcal{O}_\mathbb{Q}$ ist faktoriell (fundamentaler Satz der Arithmetik), aber im Allgemeinen ist $\mathcal{O}_K$ nicht faktoriell, z.B. (ÜA) ist $3 \in \mathbb{Z}[\sqrt{-5}]$ irreduzibel aber nicht prim. Andererseits haben wir gezeigt (siehe BIII), dass in einem faktoriellen Ring Primelemente=Irreduzibele. Wir werden zeigen, dass $\mathcal{O}_K$ noethersch ist (siehe ÜB) und damit gilt die Existenz der Faktorisierung in irreduzibele Elemente. Was fehlt also i.A ist die Eindeutigkeit (siehe ÜB). Betrachte wieder:

**Beispiel 2.1**
In $\mathbb{Z}[\sqrt{-5}]$ gilt

$$(\dagger) \qquad 6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

$2, 3, 1 + \sqrt{-5}$ und $1 - \sqrt{-5}$ sind alle irreduzibel und nicht assoziiert (siehe ÜB).
Die Idee von Kummer und Dedekind ist stattdessen eine Faktorisierung von Idealen zu verlangen: Faktorisierung vom Hauptideal $< 6 >$ ist:

$$(\ddagger) \qquad < 6 >=< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >< 3, 1 + \sqrt{-5} >< 3, 1 - \sqrt{-5} >$$

**Erinnerung:** $I, J$ Ideale, $IJ := \{ \underbrace{\sum_i a_i b_i}_{\text{endliche Summe}} \mid a_i \in I, b_i \in J\}$, z.B.:
$I =< a >$ und $J =< b > \Rightarrow IJ =< ab >$

Wir beweisen (‡). Wir behaupten:

**Behauptung 1:** $< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >=< 2 >$
und $< 3, 1 + \sqrt{-5} >< 3, 1 - \sqrt{-5} >=< 3 >$

(und damit erhalten wir durch (†):
$< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >< 3, 1 + \sqrt{-5} >< 3, 1 - \sqrt{-5} >=< 2 >< 3 >=< 6 >$.)

**Bemerkung 2.1**
Man könnte zeigen:

**Behauptung 2:** $< 2, 1 + \sqrt{-5} >< 3, 1 + \sqrt{-5} >=< 1 + \sqrt{-5} >$
und $< 2, 1 - \sqrt{-5} >< 3, 1 - \sqrt{-5} >=< 1 - \sqrt{-5} >$

und die andere Faktorisierung von 6 ausnutzen (siehe ÜB).

*Beweis von Behauptung 1:* Wir berechnen
$< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >=< 4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6 >$, wir sehen, dass alle Erzeuger hier gerade sind, also gilt $< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >\subseteq< 2 >$. Umgekehrt:
$2 = 6 - 4 \in< 4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6 >$ und damit ist $< 2 >\subseteq< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >$.
□

**Behauptung 3:** Alle vier Ideale sind Primideale (siehe ÜB). Z.B ist die Abbildung

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \to & \mathbb{Z}[\sqrt{-5}]/ < 3, 1 - \sqrt{-5} > \\ & z & \mapsto & z + < 3, 1 - \sqrt{-5} > \end{array}$$

ein surjektiver Homomorphismus mit $ker(\phi) =< 3 >$, also ist
$\mathbb{Z}[\sqrt{-5}]/ < 3, 1 - \sqrt{-5} >\cong \mathbb{Z}/ < 3 >$ ein Körper.