Algebraische Zahlentheorie

B4 SS 2013

2. Vorlesung am 18.04.2013

Kuhlmann.

Beweis Fortsetzung:

Die Quadrate mod 4 sind 0 oder 1. Also entweder

① $y^2 D \equiv 0 \bmod 4$ oder ② $y^2 D \equiv 1 \bmod 4$

Fall ① $y^2 D \equiv 0 \bmod 4$ (und $D \not\equiv 0 \bmod 4$)

$\Rightarrow$ entweder $y^2 \equiv 0 \bmod 4$; dann ist $x^2 \equiv 0 \bmod 4$
wegen (*), i.e
$x, y \equiv 0 \bmod 2$

oder

~~$y^2 \equiv 2 \bmod 4$ und $D \equiv 2 \bmod 4$~~ unmöglich weil 2 kein Quadrat mod 4 ist

Fall ② $y^2 D \equiv 1 \bmod 4$ (**)

[y^2, D sind in $\mathbb{Z}_4^\times$ i.e
1 oder 3

also

entweder $y^2 \equiv 1 \bmod 4$ und $D \equiv 1 \bmod 4$

also $y \equiv 1 \bmod 2$

also $x \equiv 1 \bmod 2$

mit (*) + (**)

oder ~~$y^2 \equiv 3 \bmod 4$~~ und $D \equiv 3 \bmod 4$

~~und~~ möglich weil 3 kein Quadrat mod 4 ist.

Wir haben also gezeigt: die folgende

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 sind beide gerade oder beide ungerade

Im Fall (i) $a = x/2 \quad b = y/2 \quad \in \mathbb{Z}$

und damit $\alpha \in \mathbb{Z}[\omega]$

Im Fall (ii) $\alpha = a + b\sqrt{D} = r + s\omega$

mit $r := \frac{(x-y)}{2}$ und $s := y$ und $\omega = \frac{1+\sqrt{D}}{2}$

$\in \mathbb{Z}$ $\in \mathbb{Z}$

§ Faktorisierung in $\mathcal{O}_K$?

$\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$ ist Faktoriell (Fundamentaler Satz der Arithmetik).

Aber i.a ist $\mathcal{O}_K$ nicht Faktoriell, z.B ü A 4.2 B III zeigt:

$3 \in \mathbb{Z}[\sqrt{-5}]$ ist irreduzible aber nicht prim. Anderseits haben wir gezeigt (6. Vorlesung B III Proposition 3 am 12.11.2012) daß Irreduzible = Primelemente in einem Faktoriellen Ring!

wir benötigen Moduln!

Wir werden zeigen $\mathcal{O}_K$ ist noethersch (siehe ü B 1) und damit gelt die Existenz der Faktorisierung in irreduzible Elemente. Was fehlt

also i.a ist die Eindeutigkeit (siehe üB 1).

In der Tat betrachte wieder das

Beispiel: in $\mathbb{Z}[\sqrt{-5}]$ gelt

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}) \quad (\dagger)$$

$2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$

sind alle irreduzible und nicht assoziert (siehe üB 1).

Die Idee von Kummer und Dedekind ist stattdessen eine Faktorisierung von Idealen zu erlangen: ← Kapitel über Dedekind Ringe!

Beispiel (Fortsetzung):
Faktorisierung vom Hauptideal $\langle 6 \rangle$ ist:

$$\left.\begin{aligned}\langle 6 \rangle = &\langle 2, 1+\sqrt{-5} \rangle \langle 2, 1-\sqrt{-5} \rangle \\ &\langle 3, 1+\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle\end{aligned}\right\} (\ddagger)$$

Erinnerung: I, J Ideale

$$IJ := \{ \underbrace{\sum a_i b_i}_{\text{endliche Summe}} \mid a_i \in I;\ b_i \in J \}.$$

e.g. $I = \langle a_1, \ldots, a_m \rangle \qquad J = \langle b_1, \ldots, b_n \rangle$

$$\Rightarrow IJ = \langle a_1 b_1, \ldots, a_m b_n \rangle .$$

Insbesondere $I = \langle a \rangle \qquad J = \langle b \rangle$

$$\Rightarrow IJ = \langle ab \rangle .$$

$\rightsquigarrow$ Wir beweisen $(\neq)$:

Wir behaupten daß

Beh 1 $\langle 2, 1+\sqrt{-5} \rangle \langle 2, 1-\sqrt{-5} \rangle = \langle 2 \rangle$

und

$\langle 3, 1+\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle = \langle 3 \rangle$

[und damit durch $(\neq)$ erhalten wir

$\langle 2, 1+\sqrt{-5} \rangle \langle 2, 1-\sqrt{-5} \rangle \langle 3, 1+\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle =$

$\langle 2 \rangle \langle 3 \rangle = \langle 6 \rangle$].

Bemerkung: man könnte stattdessen zeigen:

Bh 2 $\langle 2, 1+\sqrt{-5} \rangle \langle 3, 1+\sqrt{-5} \rangle = \langle 1+\sqrt{-5} \rangle$

und

$\langle 2, 1-\sqrt{-5} \rangle \langle 3, 1-\sqrt{-5} \rangle = \langle 1-\sqrt{-5} \rangle$

und die zweite Faktorisierung (+) von 6 ausnutzen! Siehe ÜB 1.

Beweis Beh 1. Wir berechnen

$\langle 2, 1+\sqrt{-5}\rangle\langle 2, 1-\sqrt{-5}\rangle =$

$\langle 4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6\rangle$, wir sehen alle Erzeuger hier sind gerade, also

$$\langle 2, 1+\sqrt{-5}\rangle\langle 2, 1-\sqrt{-5}\rangle \subseteq \langle 2\rangle$$

Umgekehrt $2 = 6-4 \in \langle 4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6\rangle$

und damit ist $\langle 2\rangle \subseteq \langle 2, 1+\sqrt{-5}\rangle\langle 2, 1-\sqrt{-5}\rangle$ ☐

Beh 3 Alle 4 Ideale sind Primideale (siehe ÜB 1). Z. B die Abbildung

$$\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}[\sqrt{-5}]/\langle 3, 1-\sqrt{-5}\rangle$$
$$z \longmapsto z + \langle 3, 1-\sqrt{-5}\rangle$$

ist surjektiver Homomorphismus mit

$\ker\varphi = \langle 3\rangle$.

Also ist $\mathbb{Z}[\sqrt{-5}]/\langle 3, 1-\sqrt{-5}\rangle \cong \mathbb{Z}/\langle 3\rangle$ (= Körper $\mathbb{F}_3$) ☐