Algebraische Zahlentheorie - Woche 1

Montag, 8. März 2021 15:06

$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$

$(a+bi)+(c+di) = (a+c)+(b+d)i$

$(a+bi)+(c+di) = (ac-bd)+(ad+bc)i$

$\overline{(a+bi)} = a-bi$

$\mathbb{Z}[\sqrt{-3}] = \{a+b\sqrt{-3} \mid a,b \in \mathbb{Z}\}$

$(a+b\sqrt{-3})+(c+d\sqrt{-3}) = (a+c)+(b+d)\sqrt{-3}$

$(a+b\sqrt{-3})(c+d\sqrt{-3}) = (ac+3bd) + (ad+bc)\sqrt{-3}$

$\overline{(a+b\sqrt{-3})} = a-b\sqrt{-3}$

Integritätsring:

$ab=0 \Rightarrow a=0$ oder $b=0$

faktoriell:

$a \neq 0$ und a keine Einheit

$\Longrightarrow a = p_1 \cdots p_k$

wobei p_i irr und das Produkt ist eindeutig bis auf Reihenfolge und Einheiten.

Prop. Für jeden eukl. Ring R existiert eine Norm N mit

$$N(a) \leq N(ab)$$

$\forall\, a,b \in R$ ungleich 0.

Bem: $a \mid b$ dann folgt $N(a) \leq N(b)$.

Prop. In einem eukl. Ring R mit Normfunktion, die $N(a) \leq N(ab)$ $\forall\, a,b \neq 0$ erfüllt, gilt, dass $e \in R$ eine Einheit ist gdw. $N(e) = N(1)$.

assoziiert:

$a \mid b$ und $b \mid a$

irreduzibel:

$a \neq 0$, keine Einheit und

$a = bc \Rightarrow b$ oder c ist eine Einheit.

Prim:

$a \neq 0$, a keine Einheit

$a \mid bc \Rightarrow a \mid b$ oder $a \mid c$

euklidischer Ring:

Ein Integritätsring R heisst euklidisch, wenn eine Abb.

$N: R\setminus\{0\} \longrightarrow \mathbb{N}$

existiert, s.d. für alle $a,b \in R$, wobei $b \neq 0$, gilt, dass $q,r \in R$ existieren mit $a = qb+r$ und $r = 0$ oder $N(r) < N(b)$.

Prop. Ein eukl. Ring ist faktoriell.

Lemma In faktoriellen Ringen ist jedes irr. Element prim.

Bew:

Sei $e \in R$ eine Einheit, dann gibt es ein $a \in R$, s.d. $ea = 1$, also gilt

$N(e) \leq N(ea) = N(1)$

Es gilt $1 \mid e \Rightarrow N(1) \leq N(e)$

$\Longrightarrow N(e) = N(1)$

Sei $e \in R$ mit $N(e) = N(1)$.

$\mathbb{Z}[i]$:

Sei $N: \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ gegeben durch

$$(a+bi) \longmapsto a^2+b^2$$

Bem: $N(\cdot) = |\cdot|^2$, $N(a) = a\bar{a}$

Lemma 17

$$N(ab) = N(a)N(b)$$

Lemma Die Einheiten in $\mathbb{Z}[i]$ sind $\{\pm 1, \pm i\}$

Bew:

$$N(a) \leq N(ab)$$

$e \in \mathbb{Z}[i]$ ist eine Einheit

$\Longleftrightarrow N(e) = N(1)$

Da aber $N(1) = 1$

$\Rightarrow$ e Einheit wenn

$$N(e) = N(a+bi) = a^2+b^2 = 1$$

$\square$

$a+b\sqrt{3} \longmapsto |a^2-3b^2|$:

Wenn $q, p \in \mathbb{Q}$ s.d. $|q|, |p| \leq \frac{1}{2}$

dann gilt [illegible]

Sei $e \in R$ mit $N(e) = N(1)$.

Es existieren $q, r \in R$ s.d. $qe + r = 1$. Dabei erfüllt r, dass $r = 0$ oder $N(r) < N(e)$.

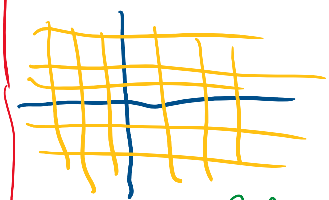
$N(e)$ ist allerdings minimal.

Deshalb gilt $r = 0$

$\Rightarrow qe = 1 \quad \Rightarrow e \in R^\times$

Bew: Seien $a, b \in \mathbb{Z}[i]$, wobei $b \neq 0$. Wir suchen $q, r \in \mathbb{Z}[i]$ s.d. $a = qb + r$ mit $N(r) < N(b)$ oder $r = 0$.

Beachten wir, dass $\mathbb{Z}[i] \subseteq \mathbb{C}$



D.h. $\frac{a}{b} \in \mathbb{C}$ und liegt in einer Masche.

Deshalb folgt, dass der Abstand zum nächsten Gitterpunkt kleiner gleich $\frac{\sqrt{2}}{2}$. Wir können ein $q \in \mathbb{Z}[i]$ wählen, so dass $|\frac{a}{b} - q| < 1$. Definiere nun $r = a - qb$. Dann folgt

$$\begin{aligned} N(r) &= N(a-qb) \\ &= |b(\tfrac{a}{b}-q)|^2 \\ &= |b|^2 |\tfrac{a}{b}-q|^2 < |b|^2 = N(b) \end{aligned}$$

$\square$

Prop. Die Abb. $N_{\sqrt{-3}}: \mathbb{Q}[\sqrt{-3}] \setminus \{0\} \to \mathbb{N}$ gegeben durch

$$(a+b\sqrt{-3}) \longmapsto |a^2-3b^2|$$

eingeschränkt auf $\mathbb{Z}[\sqrt{-3}]$ ist eine eukl. Norm für $\mathbb{Z}[\sqrt{-3}]$.

Lemma Die Abb $N_{\sqrt{-3}}$ ist multiplikativ, also $N(ab) = N(a)N(b)$

$x, y \in \mathbb{Z}[\sqrt{-3}]$, also

$x = a + b\sqrt{-3}$, $y = a' + b'\sqrt{-3}$

Wenn $q, p \in \mathbb{Q}$ s.d. $|q|, |p| \leq \frac{1}{2}$

dann gilt $|p^2 - 3q^2| \leq \frac{3}{4} < 1$.

Wir wählen $a, b \in \mathbb{Z}[\sqrt{3}]$ und beobachten, dass $\frac{a}{b} \in \mathbb{Q}[\sqrt{3}]$.

Seien $\frac{a}{b} = u + v\sqrt{3}$ wobei $u, v \in \mathbb{Q}$.

Wir finden $m, n \in \mathbb{Z}$ s.d. $|u - m| \leq \frac{1}{2}$ und $|v - n| \leq \frac{1}{2}$.

Definiere $q = m + n\sqrt{3}$.

Dann gilt

$$N_{\sqrt{3}}\left(\frac{a}{b} - q\right) = |(u-m)^2 - 3(v-n)^2| < 1$$

Sei dann $r = a - bq \in \mathbb{Z}[\sqrt{3}]$

und

$$\begin{aligned} N_{\sqrt{3}}(r) &= N_{\sqrt{3}}(a - bq) \\ &= N_{\sqrt{3}}\left(b\left(\frac{a}{b} - q\right)\right) \\ &= N_{\sqrt{3}}(b)\, N_{\sqrt{3}}\left(\frac{a}{b} - q\right) \\ &< N_{\sqrt{3}}(b) \end{aligned}$$

Bem: $N_{\sqrt{3}}(a) = |a\bar{a}|$

Lemma Die Einheiten in $\mathbb{Z}[\sqrt{3}]$ sind alle Elemente $a + b\sqrt{3}$ für die gilt

$$a^2 - 3b^2 = \pm 1$$

Bew:

$$N_{\sqrt{3}}(1) = 1$$

Also folgt $e \in \mathbb{Z}[\sqrt{3}]$ ist eine Einheit gdw.

$$N_{\sqrt{3}}(e) = 1.$$

Mit $e = a + b\sqrt{3}$ gilt

$$N_{\sqrt{3}}(e) = |a^2 - 3b^2| = 1$$

$$\iff a^2 - 3b^2 = \pm 1 \quad \square$$

Lemma Ist $\pi \in \mathbb{Z}[i]$ ein

$x = a + b\sqrt{3}$, $y = a' + b'\sqrt{3}$

$$\frac{(a + b\sqrt{3})}{(a' + b'\sqrt{3})} = \frac{(a + b\sqrt{3})(a' - b'\sqrt{3})}{(a' + b'\sqrt{3})(a' - b'\sqrt{3})} = \frac{aa' - bb'3}{a'^2 - 3b'^2} + \frac{a'b - ab'}{a'^2 - 3b'^2}\sqrt{3}$$

Bsp.

$2 \in \mathbb{Z}$

$2 = (1+i)(1-i)$

$\implies$ 2 ist nicht prim in $\mathbb{Z}[i]$

$13 \in \mathbb{Z}$ in $\mathbb{Z}[\sqrt{3}]$

$13 = (4 + \sqrt{3})(4 - \sqrt{3})$

$\implies$ 13 nicht prim

$N_{\sqrt{3}}(e) = 1.$

Mit $e = a + b\sqrt{3}$ gilt

$$N_{\sqrt{3}}(e) = |a^2 - 3b^2| = 1$$

$\Longleftrightarrow$ $a^2 - 3b^2 = \pm 1$ $\square$

Lemma Ist $\pi \in \mathbb{Z}[i]$ ein Element mit $N(\pi) = p$ für p prim, so folgt π prim in $\mathbb{Z}[i]$.

Bew:

Ang. $\pi = ab$ für $a, b \in \mathbb{Z}[i]$ dann gilt

$$p = N(\pi) = N(ab) = N(a)N(b)$$

$N(a) = 1$ oder $N(b) = 1$, also a oder b eine Einheit

$\Longrightarrow$ π irr.

$\Longrightarrow$ π prim

$\Longrightarrow$ 2 ist nicht prim in $\mathbb{Z}[i]$

$13 \in \mathbb{Z}$ in $\mathbb{Z}[\sqrt{3}]$

$$13 = (4 + \sqrt{3})(4 - \sqrt{3})$$

$\Longrightarrow$ 13 nicht prim

Bem: Das Selbe gilt auch für $\mathbb{Z}[\sqrt{3}]$.

Lemma Für ein Primelement $\pi \in \mathbb{Z}[i]$ gilt, dass $N(\pi) \in \{p, p^2\}$ wo p prim.

Bew:

Für π prim, schreiben

$$N(\pi) = \pi\overline{\pi} \Longrightarrow \pi \mid N(\pi)$$

$$\pi \mid N(\pi) = p_1 \dots p_k$$

und es folgt, dass $\pi \mid p_i$.

Es folgt $\pi b = p_i$ für $b \in \mathbb{Z}[i]$. Deshalb gilt

$$p^2 = N(p) = N(\pi b) = N(\pi)N(b)$$

$\Longrightarrow$ $N(\pi) \in \{p, p^2\}$.

Bem: Das Selbe gilt für $\mathbb{Z}[\sqrt{3}]$. Außerdem sind in Int.ringen Elemente die sich durch Mult. mit Einheiten unterscheiden assoziiert. Deshalb gilt für π wie oben mit $N(\pi) = p^2$, dass $\pi \sim p$

$\underline{\mathbb{Z}[i]}$

Prop. Für Primzahlen $p \neq 2$

$$p = a^2 + b^2 \ (a, b \in \mathbb{Z})$$

$\Longleftrightarrow$ $p \equiv 1 \mod 4$

Bew:

$\Longleftarrow$ Wir zeigen, dass solches p kein Primelement in $\mathbb{Z}[i]$ ist. Denn dann können wir $p = ab$

$\Leftrightarrow \quad p \equiv 1 \mod 4$

Bew:

"$\Longrightarrow$"

Wenn $p = a^2 + b^2$ dann folgt Beh. weil a^2 und b^2 erfüllen dann

$$a^2 \equiv 1 \text{ oder } 0 \mod 4$$

Thm. Die Primelemente in $\mathbb{Z}[i]$, bis auf Assoz., sind

- $1+i$
- $a+bi$ wobei $a^2+b^2 = p \in \mathbb{Z}\setminus\{2\}$ mit p prim und $p \equiv 1 \mod 4$
- p, mit p prim und $p \equiv 3 \mod 4$

Sei $\pi \in \mathbb{Z}[i]$ prim.
Wir wissen $N(\pi) \in \{p, p^2\}$.
Wenn $N(\pi) = 2$, dann müssen $|a| = |b| = 1$
sind alle assoziiert

Primelement in $\mathbb{Z}[i]$ ist.
Denn dann können wir $p = ab$ für $a, b \notin \mathbb{Z}[i]^\times$ schreiben.
Dann folgt

$$p^2 = N(p) = N(a)N(b)$$

$\Longrightarrow N(a) = N(b) = p$

$\Longrightarrow$ für $a = a_1 + a_2 i$ folgt

$$a_1^2 + a_2^2 = p$$

Nach dem Satz von Wilson ist

$$(p-1)! \equiv -1 \mod p$$

$p \equiv 1 \mod 4$, dann gilt $p = 4k+1$ und es folgt

$$-1 \equiv_p (p-1)! = (1 \dots 2k)(p-1 \dots p-2k)$$

$$\equiv_p (2k)!\,((-1)^{2k}(2k)!)$$

$$= ((2k)!)^2$$

$$p \mid ((2k)!)^2 + 1 = ((2k)! + i)((2k)! - i)$$

$\Longrightarrow p$ nicht prim in $\mathbb{Z}[i]$.

Bew:

$1+i$, $a+bi$ wie oben haben primnorm, also sind sie prim.
Nehmen wir an $p \equiv 3 \mod 4$, aber nicht prim. $p = ab$ für $a, b \in \mathbb{Z}[i]^\times$ schreiben. Es gilt

$p^2 = N(p) = N(a)N(b)$, da beide keine Einheiten

$\Longrightarrow \quad N(a) = N(b) = p$

mit $a = a_1 + a_2 i$ folgt

$$a_1^2 + a_2^2 = p$$

$\Longrightarrow \quad p \equiv 1 \mod 4 \quad ⚡$

$\Longrightarrow \quad p$ Primelement in $\mathbb{Z}[i]$

Wenn $N(\pi) = 2$, dann müssen $|a| = |b| = 1$
$\Rightarrow$ sind alle assoziiert zu $1+i$

Wenn $N(\pi) = p \in \mathbb{Z} \setminus \{2\}$.
Dann gilt für $\pi = a+bi$, dass $a^2 + b^2 = p$.

Ang $N(\pi) = p^2$. Es folgt $\pi \sim p$. Also z.z.
$p \equiv 3 \mod 4$ ist

Wenn nicht, dann
$p = 2$ oder $p \equiv 1 \mod 4$
wenn $p = 2$ schreiben wir
$2 = (1+i)(1-i)$
wenn $p \equiv 1 \mod 4$
$p = (a+bi)(a-bi) = a^2+b^2$

In beiden Fällen ist p nicht prim, deshalb wäre π nicht prim. $\square$

Thm. Primelemente von $\mathbb{Z}[\sqrt{-3}]$ bis auf Assoz. sind

- $-1+\sqrt{-3}$
- $\sqrt{-3}$
- $a+b\sqrt{-3}$, wobei $a^2-3b^2 = \pm p \in \mathbb{Z} \setminus \{2,3\}$ prim ist und 3 ist ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$
- p, p ist prim s.d. 3 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$

Lemma Für eine Primzahl $p \in \mathbb{Z}$ gilt $\pm p = a^2 - 3b^2$
$\Rightarrow$ 3 ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$

Bew:
Die ersten drei Elemente haben Prim norm $\Rightarrow$ prim.
Ang. 3 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ aber p nicht prim in $\mathbb{Z}[\sqrt{-3}]$.
In dem Fall gilt $p = ab$ für $a, b \in \mathbb{Z}[\sqrt{-3}]^\times$.
$p^2 = N(p) = N(a)N(b)$, also $N(a) = p$, deshalb ist mit $a = a_1 + a_2\sqrt{-3}$
$\pm p = a^2 - 3b^2$
$\Rightarrow$ 3 ist Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ↯
$\Rightarrow p$ prim in $\mathbb{Z}[\sqrt{-3}]$.

Sei $\pi \in \mathbb{Z}[\sqrt{-3}]$ prim. Dann gilt $N(\pi) \in \{p, p^2\}$.
$N(\pi) = 2$: Dann gilt
$2 = (2+\sqrt{-3})(-1+\sqrt{-3})^2$
und $\pi | 2$, also $\pi \cdot \beta = 2$
deshalb

folgt $\pi \sim (-1+\sqrt{-3})$.
$N(\pi) = 3$: identisch mit $3 = \sqrt{-3}^2$
$N(\pi) = p \in \mathbb{Z} \setminus \{2,3\}$:
$a^2 - 3b^2 = \pm p$
Lem $\Rightarrow$ 3 Quadrat in $\mathbb{Z}/$

und $\pi \mid 2$, also $\pi\beta = 2$

deshalb

$$\pi\beta = 2 = (2+\sqrt{3})(-1+\sqrt{3})^2$$

$\Longrightarrow$ wegen Eindeutigkeit der Primfaktorzerlegung

$N(\pi) = p^2$:

Wieder $\pi \sim p$.

Z.z. 3 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$

Ang. $3 \equiv c^2 \mod p$.

$N(c+\sqrt{3}) = \pm(c^2-3) \equiv 0 \mod p$

O.B.d.A wähle $c \in \{-\frac{p-1}{2}, \frac{p-1}{2}\}$

$(p^2 > \pm c^2 - 3)$, also

$$p^2 \nmid c^2 - 3$$

$a^2 - 3b^2 = \pm p$

$\overset{\text{Lem}}{\Longrightarrow}$ 3 Quadrat in $\mathbb{Z}/p\mathbb{Z}$

$\Longrightarrow$ Element unserer Liste

Gleichzeitig

$$p \mid (c+\sqrt{3})(c-\sqrt{3}) = c^2 - 3$$

p ist prim, also folgt

$$p \nmid (c+\sqrt{3}),\ p \nmid (c-\sqrt{3})$$

$\Longrightarrow$ $\operatorname{ggT}(p, c+\sqrt{3}) \neq \pm 1$

oder

$\operatorname{ggT}(p, c-\sqrt{3}) \neq \pm 1$

Sei β ein solcher ggT ungleich ± 1.

Dann ist wegen Multi. der Norm

$$N(\beta) \mid N(p) = p^2$$

und $N(\beta) \mid c^2 - 3 = (c+\sqrt{3})(c-\sqrt{3})$

$N(\beta) \in \{p, p^2\}$ und da

$$p^2 \nmid c^2 - 3 \Longrightarrow N(\beta) = p$$

$\overset{p \text{ prim}}{\Longrightarrow}$ β prim

$$\pi\bar{\pi} = \pm p^2 = \beta\bar{\beta}\beta\bar{\beta}$$

$\lightning$ zur Eindeutigkeit Primzerlegung

$\Longrightarrow$ 3 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$

$\Longrightarrow$ Beh folgt

$\square$