§5 Summen von zwei Quadraten in $\mathbb{Z}$ und der Gaußsche Zahlring $\mathbb{Z}[i]$.

Ausgangspunkt ist §3, F8:

$p \equiv 1 \bmod 4 \implies \exists\, c \in \mathbb{Z}$ [z.B. $c = \left(\frac{p-1}{2}\right)!$] mit

(1) $c^2 \equiv -1 \bmod p$, d.h. $c^2 + 1 = kp$ mit einem $k \in \mathbb{Z}$

Satz 1 (Fermat, Euler): Sei p eine Primzahl.

Ist $p \equiv 1 \bmod 4$, so gibt es $x, y \in \mathbb{Z}$ mit

(*) $$p = x^2 + y^2.$$

(Ist umgekehrt p in der Gestalt (*) darstellbar, so ist $p \equiv 1 \bmod 4$ oder $p = 2$.)

Bew. *Vorbehaltung:* Gelte (*) mit $x, y \in \mathbb{Z}$. Dann $(x, y) = 1$. Insb. $p \nmid x$, $p \nmid y$. Aus (*) folgt trivialerweise

$$x^2 + y^2 \equiv 0 \bmod p, \quad \text{also (wegen } p \nmid x\text{)}$$

$$1 + \left(\frac{y}{x}\right)^2 \equiv 0 \bmod p \quad [\xrightarrow{\text{§3 F8}} p \equiv 1 \bmod 4 \text{ oder } p = 2]$$

Vergleich mit (1) liefert

$$\frac{y}{x} \equiv \pm c \bmod p$$

$$y \equiv \pm cx \bmod p$$

Sei nun $p \equiv 1 \bmod 4$. $\exists\, c \in \mathbb{Z}$, so daß (1) gilt. Wähle $d \in \mathbb{N}$ minimal mit $d^2 > p$. Dann $1 < d \leq p$.

$p^2 > p$

Nach Aufgabe 25b) [mit $e = d$ und $m = p$] gibt es $x, y \in \mathbb{Z}$ mit beachte $(c, p) = 1$

(2) $y \equiv \pm cx \bmod p$ und $0 < x, y < d$

$x^2, y^2 \leq (d-1)^2 \leq p$ (nach Wahl von d), $\Longrightarrow$ p kein Quadrat

(3) $x^2, y^2 < p$

$x^2+y^2 \overset{(2)}{\equiv} x^2 + c^2x^2 = x^2(1+c^2) \equiv 0 \bmod p$, $\Longrightarrow$

$x^2+y^2 = mp$, $m \in \mathbb{N}$. Nach (3)

$mp < 2p$, $\Longrightarrow m = 1$. Also $p = x^2+y^2$. □

Ein weiterer, sehr natürlicher Beweis von Satz 1 ergibt sich aus der Betrachtung des Ringes

"Ring der ganzen ganzzahligen Zahlen"
"Ganzzahliger Zahlbereich"

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

mit der Einheitengruppe $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$. Es ist

$$(a+bi)(a-bi) = a^2+b^2$$

Satz 2: $\mathbb{Z}[i]$ ist ein <u>euklidischer Ring</u> mit euklid. Normfunktion ν, def. durch

$$\nu(z) = z\bar{z} =: N(z) \qquad (z \in \mathbb{Z}[i])$$

Bew. $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha \neq 0$

(*) $\gamma := \frac{\beta}{\alpha}$ liegt in $\mathbb{Q}[i] = \{ x+yi \mid x, y \in \mathbb{Q} \}$ ist Körper! (klar?!)

<u>Bem.</u> $\mathbb{Q}(i) = \mathbb{Q}[i]$

<u>Beh.</u> Zu jedem $\eta \in \mathbb{Q}(i)$ gibt es ein $\gamma \in \mathbb{Z}[i]$ mit

$$N(\eta - \gamma) < 1$$

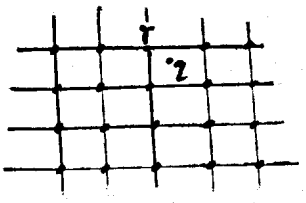
Beh. $\Rightarrow$ Satz: η wie in (*), γ wie in Beh. $\rho := \beta - \gamma\alpha \overset{!}{\in} \mathbb{Z}[i]$.

$N(\rho) = N(\beta - \gamma\alpha) = N(\eta\alpha - \gamma\alpha) = N((\eta-\gamma)\alpha) = N(\eta-\gamma)N(\alpha) < N(\alpha)$

Also $\beta = \gamma\alpha + \rho$ mit $\gamma, \rho \in \mathbb{Z}[i]$ und $N(\rho) < N(\alpha)$.

Beweis des Satz.

$q = x + yi \; ; x, y \in \mathbb{Q}$



$\exists a \in \mathbb{Z}$ mit $|x-a| \le \frac{1}{2}$ $\quad \exists b \in \mathbb{Z}$ mit $|y-b| \le \frac{1}{2}$. Dann $\gamma := a+bi \in \mathbb{Z}[i]$

$q - \gamma = r_1 + r_2 i$ mit $|r_1|, |r_2| \le \frac{1}{2}$, also

$N(q-\gamma) = N(r_1 + r_2 i) = r_1^2 + r_2^2 \le \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$

F1: Sei π ein Primelement $\neq 0$ von $\mathbb{Z}[i]$. Dann gibt es genau eine Primzahl p mit

$$\pi \mid p \qquad \text{[in } \mathbb{Z}[i]\text{]}$$

Es gilt entweder $N(\pi) = p$ oder $N(\pi) = p^2$. (Im ersten Fall nennen wir π vom Grade 1, im zweiten Fall vom Grade 2).

Beweis. $N\pi = \pi\bar{\pi} \Rightarrow \pi \mid N\pi$, $N\pi \in \mathbb{N}$ keine Einheit in $\mathbb{Z}$

$\Rightarrow N\pi = p_1 \cdots p_r$ mit Primzahlen p_j, $r \ge 1$.

π Primelement, $\Rightarrow \pi$ teilt ein $p_j =: p$.

$\pi \mid p$, $\Rightarrow N\pi \mid Np$, $\Rightarrow N\pi = p$ oder $N\pi = p^2$.
$\qquad\qquad\qquad\qquad\qquad\quad\; \| \; p^2$

p eindeutig: $\pi \mid q$, $\Rightarrow N\pi \mid Nq = q^2 \Rightarrow p \mid q^2 \Rightarrow$
$p = q$. □

Um alle Primelemente π von $\mathbb{Z}[i]$ zu finden, haben wir also die PFZ aller p in $\mathbb{Z}[i]$ zu untersuchen.

[die p heißen rationale Primzahlen, die π ganzzahlige Primzahlen]

Satz 3: p Primzahl. Sei dann π ein Primfaktor von p in $\mathbb{Z}[i]$. Dann gibt es drei Fälle:

(i) $p \hat{=} \pi^2$ (p 'verzweigt' in $\mathbb{Z}[i]$)

(ii) $p \hat{=} \pi$ (d.h. p bleibt Primelt. in $\mathbb{Z}[i]$: p 'träge' in $\mathbb{Z}[i]$)

(iii) $p = \pi\bar{\pi}$ mit $\pi \not\hat{=} \bar{\pi}$ (p 'zerfällt' in $\mathbb{Z}[i]$),

und zwar gilt:

(i) $\Leftrightarrow$ $p = 2$

(ii) $\Leftrightarrow$ $N(\pi) = p^2$ $\Leftrightarrow$ $p \equiv 3 \bmod 4$

(iii) $\Leftrightarrow$ $N(\pi) = p$ $\Leftrightarrow$ $p \equiv 1 \bmod 4$

also z.B. 7 Primelt. auch in $\mathbb{Z}[i]$, 5 dagegen nicht
[$5 = (2+i)(2-i)$]

Bew. $p = \gamma\pi$, $\Rightarrow$ $p^2 = N(\gamma)N(\pi)$

1. Fall: $N(\pi) = p^2$, $\Leftrightarrow$ $N\gamma = 1$ $\Leftrightarrow$ γ Einheit $\Leftrightarrow$ $p \hat{=} \pi$

2. Fall: $N(\pi) = p$, $\Leftrightarrow$ $\pi\bar{\pi} = p$, $\bar{\pi}$ auch Primelt. (denn $\alpha \mapsto \bar{\alpha}$ ist Automorphismus)

im 2. Fall: $\pi \hat{=} \bar{\pi}$ $\Leftrightarrow$ $p \hat{=} \pi^2$

*) $\pi \mid c$, $c \in \mathbb{Z}$ $\Rightarrow N\pi \mid Nc \Rightarrow p \mid c^2 \Rightarrow p \mid c$.

$\pi = a+bi$, $\Rightarrow (a,b) = 1$. Gelte $\pi \hat{=} \bar{\pi}$, $\overset{*)}{\Rightarrow}$

$\pi \mid \pi+\bar{\pi}$, $\pi \mid \pi-\bar{\pi}$, $\Rightarrow \pi \mid 2a$, $\pi \mid 2b$ $\Rightarrow$ $p \mid 2a$, $p \mid 2b$

$\overset{(a,b)=1}{\Rightarrow}$ $p \mid 2$, $\Rightarrow p = 2$.

$2 = (1+i)(1-i)$ $\quad 1-i = -i(1+i) \hat{=} 1+i$.

$1+i$ Primelt. (klar?!)

b.z.z. Für $p \neq 2$ gilt

(*) $N\pi = p \iff p \equiv 1 \bmod 4$

$N\pi = p, \Rightarrow a^2+b^2 = p, \overset{*)}{\Rightarrow} p \equiv 1 \bmod 4$

*) vgl. Satz 1. Direkter Bew. als ÜA, beachte: Für jedes ungerade $c \in \mathbb{Z}$ ist $c^2 \equiv 1 \bmod 4$.

Sei $p \equiv 1 \bmod 4$. Gelte nicht $N\pi = p$. Dann (nach F1)

$N\pi = p^2, \overset{\text{s.o.}}{\Rightarrow}$ p Primelt. in $\mathbb{Z}[i]$.

Wegen $p \equiv 1 \bmod 4$ gibt es (nach §3, F8) ein $a \in \mathbb{Z}$ mit

$a^2 \equiv -1 \bmod p, \Rightarrow p \mid a^2+1 = (a+i)(a-i)$,

$\overset{p \text{ prim in } \mathbb{Z}[i]}{\Rightarrow}$ $p \mid a+i$ oder $p \mid a-i$ W!

$\lceil a \pm i = p(x+yi) \Rightarrow py = \pm 1 \Rightarrow p \mid \pm 1 \rfloor$

Korollar: Ist p eine Primzahl mit $p \equiv 1 \bmod 4$, so ist p in der Gestalt

$$p = a^2 + b^2 \quad \text{mit } a, b \in \mathbb{N}$$

darstellbar. Bis auf Vertauschung von a, b ist diese Darstellung eindeutig. (Ferner ist notwendig $(a,b) = 1$).

Bew. 1) $p = N(\pi)$ nach Satz 3. $\pi = x+yi \quad x, y \in \mathbb{Z}$.

$p = x^2+y^2 = (\pm x)^2 + (\pm y)^2 \quad x \neq 0, y \neq 0$

2) $p = \underset{c,d \in \mathbb{N}}{c^2+d^2} = N(\underbrace{c+di}_{=:\pi'})$; π' unzerlegbar (klar?!)

$p = \pi' \overline{\pi'} = \pi \overline{\pi}$, $\overset{\mathbb{Z}[i] \text{ faktoriell}}{\Rightarrow}$ $\pi' \sim \pi$ oder $\pi' \sim \overline{\pi}$

$\Rightarrow \quad \exists\, \varepsilon \in \{1,-1,i,-i\}$

$$c+di = \varepsilon(a \pm bi) = \begin{cases} \pm a \pm bi \\ \mp b \pm ai \end{cases}, \quad \overset{a,b,c,d>0}{\Longrightarrow}$$

$$\begin{cases} c=a\,,\ d=b \\ c=b\,,\ d=a \end{cases}$$

q.e.d.

Satz 4: Sei $n \in \mathbb{N}$.

(i) Genau dann ist n eine Summe von 2 Quadraten in $\mathbb{Z}$, wenn für jede Primzahl $p \equiv 3 \bmod 4$ der Exponent $w_p(n)$ gerade ist.

(ii) Besitzt n eine primitive Darstellung als Summe von 2 Quadraten, d.h.

(1) $n = a^2+b^2$ mit teilerfremden $a, b \in \mathbb{Z}$,

so folgt:

(2) n hat keine Primteiler $p \equiv 3 \bmod 4$, und es ist $4 \nmid n$.

(iii) Umgekehrt: Gelte (2), und bezeichne s die Anzahl der ungeraden Primteiler von n. Für $n>2$ hat dann n genau 2^{s-1} primitive Darstellungen als Summe von 2 Quadraten (wenn nur wesentlich verschiedene Darstellungen gezählt werden). $\triangle$ n kann außerdem noch nicht-primitive Darst. haben, z.B. $50 = 7^2+1^2 = 5^2+5^2$.

Bew. (ii): Gelte (1). Sei $p \mid n$. Annahme: $p \equiv 3 \bmod 4$

Dann p prim in $\mathbb{Z}[i]$. $p \mid n = \alpha\bar{\alpha}$ mit $\alpha = a+bi$ $[\in \mathbb{Z}[i]]$,

$\Rightarrow p \mid \alpha$ oder $p \mid \bar{\alpha} \Rightarrow p \mid a \pm bi$, $\Longrightarrow p \mid a$ und $p \mid b$

Widerspruch zu $(a,b) = 1$.

Annahme: $4 \mid n$. $\overset{(a,b)=1}{\Longrightarrow}$ a, b beide ungerade, $\Rightarrow a^2+b^2 \equiv 2 \bmod 4$

$\| \; a^2+b^2$ [also $a^2 \equiv b^2 \equiv 1 \bmod 4$] W!