Beispiel: Primelemente in den Gaußschen Zahlen

Satz Primelemente in $\mathbb{Z}[i]$

Für die Primelemente $\pi \in \mathbb{Z}[i]$ gilt bis auf Assoziiertheit

1. $N(\pi) = p$ für ein $p \in \mathbb{P}$ oder
2. $\pi = p$ für ein $p \in \mathbb{P}$ mit $p \neq x^2 + y^2$ für $(x, y) \in \mathbb{Z}^2$.

Beweis:

- Sei $\pi \in \mathbb{Z}[i]$ prim. Wegen $\pi\bar{\pi} = N(\pi)$ gilt $\pi \mid N(\pi)$.
- Sei $N(\pi) = p_1 \cdot \ldots \cdot p_n$ die Primzerlegung von $N(\pi)$.
- Da π prim ist, folgt $\pi | p$ für ein $p = p_i$. Sei also $\pi c = p$.
- Wegen $N(\pi) \cdot N(c) = p^2$ und $N(\pi) > 1$, muss gelten
$$N(\pi) = p \text{ oder } N(\pi) = p^2.$$
- Dies ist eine notwendige Bedingung für die Primheit von π.

Beweis:

- **Fall 1** $N(\pi) = p$: Aus $\pi = ab$ folgt $N(\pi) = p = N(a) \cdot N(b)$.
- Damit ist entweder $N(a)$ oder $N(b)$ eine Einheit, π also irreduzibel.
- Da $\mathbb{Z}[i]$ faktoriell ist, muss π damit prim sein.
- **Fall 2** $N(\pi) = p^2$: Aus $\pi = ab$ folgt $N(\pi) = p^2 = N(a) \cdot N(b)$.
- Dies ist eine nicht-triviale Zerlegung für $a = x + iy$ mit
$$N(a) = p = x^2 + y^2.$$
- D.h. π ist reduzibel gdw $p = x^2 + y^2$ für $(x, y) \in \mathbb{Z}^2$.
- Für irreduzibles π mit $N(\pi) = p^2$ gilt $\pi = p$ bis auf Assoziiertheit.

Übung: Faktorisieren Sie 30 in $\mathbb{Z}[i]$ in Primelemente.

Satz Polynomring

Sei R ein faktorieller Ring. Dann ist auch der Polynomring $R[X]$ faktoriell.

(ohne Beweis)

Größte gemeinsame Teiler

Definition ggT

Sei R ein faktorieller Ring und $a, b \in R$, nicht beide 0. Ein Element c heißt $\mathrm{ggT}(a, b)$ – *größter gemeinsamer Teiler von a und b*– falls

$$c|a,\ c|b \text{ und für jeden Teiler } d \text{ von } a \text{ und } b \text{ gilt } d|c.$$

Falls $\mathrm{ggT}(a, b) = 1$, so heißen a, b *teilerfremd*. Wir definieren

$$\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(a_1, \mathrm{ggT}(a_2, \ldots, \mathrm{ggT}(a_{n-1}, a_n))).$$

Eindeutigkeit:

- Der ggT ist eindeutig bis auf Assoziiertheit, z.B. $\mathrm{ggT}(4, 6) = \pm 2$.
- Seien $c = \mathrm{ggT}(a, b)$ und $c' = \mathrm{ggT}(a, b)$.
- Nach der Eigenschaft des ggT muss $c|c'$ und $c'|c$ gelten.
- D.h. $cd = c'$ und $c'd' = c$, woraus $cdd' = c$ folgt.
- Wir erhalten $dd' = 1$ bzw. $d, d' \in R^*$.
- Damit sind c und c' in R assoziiert.

Einfache Eigenschaften

Einfache Eigenschaften des ggT:

- Symmetrie: $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,a)$
- Spezielle Elemente: $\mathrm{ggT}(a,0) = a$ und $\mathrm{ggT}(a,1) = 1$
- Multiplikativität: $\mathrm{ggT}(ca,cb) = c \cdot \mathrm{ggT}(a,b)$
- Teiler: $a|b \Leftrightarrow \mathrm{ggT}(a,b) = a$
- Teilbarkeit: $\mathrm{ggT}(a,b)|\mathrm{ggT}(a,bc)$
- Additivität: $\mathrm{ggT}(a,b) = \mathrm{ggT}(a,b+ca)$

Mehr Eigenschaften

Lemma ggT-Eigenschaften

Sei R ein faktorieller Ring und $a, b, c \in R$. Dann gilt

1. $\mathrm{ggT}(a,b) = 1 \Rightarrow \mathrm{ggT}(a^i, b^j) = 1$ für $i, j \in \mathbb{N}$
2. $a|bc$ und $\mathrm{ggT}(a,b) = 1 \Rightarrow a|c$
3. $\mathrm{ggT}(a,b) = 1 \Rightarrow \mathrm{ggT}(a,bc) = \mathrm{ggT}(a,c)$

Beweis:

(1) Annahme: $p|\mathrm{ggT}(a^i, b^j)$ für ein primes p.
- Da p prim ist, folgt $p|a$, $p|b$ und damit $p|\mathrm{ggT}(a,b)$. (Widerspruch)

(2) Betrachte die Primfaktorzerlegungen von a, b und c.
- Da $\mathrm{ggT}(a,b) = 1$, besitzen a und b keine gemeinsamen Faktoren.
- Wegen $a|bc$ müssen damit alle Faktoren von a in c enthalten sein.

(3) Nach Teilbarkeit gilt $\mathrm{ggT}(a,c)|\mathrm{ggT}(a,bc)$.
- Wir zeigen $\mathrm{ggT}(a,bc)|\mathrm{ggT}(a,c)$. Sei $d = \mathrm{ggT}(a,bc)$.
- Dann gilt $d|a$ und $d|bc$. Wegen $\mathrm{ggT}(a,b) = 1$ folgt $\mathrm{ggT}(d,b) = 1$.
- Mit (2) folgt $d|c$ und damit $d|\mathrm{ggT}(a,c)$.

Existenz und Eindeutigkeit des ggT

Satz Existenz und Eindeutigkeit des ggT

In einem faktoriellen Ring R mit $a, b \in R$, nicht beide 0, existiert $\mathrm{ggT}(a, b)$ und ist eindeutig bis auf Assoziiertheit.

Beweis: Die Eindeutigkeit wurde schon gezeigt.

- Falls $a = 0$ oder $b = 0$ ist die Existenz trivial. Seien also $a, b \neq 0$.
- Sei $P = \{p \in R \mid p \text{ taucht als Primfaktor von } a \text{ oder von } b \text{ auf}\}$.
- Wir schreiben die Primfaktorzerlegung von a und b in der Form
$$a = u \prod_{p \in P} p^{n_p},\ b = v \prod_{p \in P} p^{m_p} \text{ für } u, v \in R^*.$$
- Wir definieren $c = \prod_{p \in P} p^{\min\{n_p, m_p\}}$.
- Offenbar gilt $c|a$ und $c|b$, d.h. c ist gemeinsamer Teiler von a, b.
- Ferner ist jeder gemeinsamer Teiler von der Form
$$d = \prod_{p \in P} p^{k_p} \text{ mit } k_p \leq \min\{n_p, m_p\}.$$
- Damit folgt $d|c$ und c ist der größte gemeinsame Teiler von a, b.

Bsp: In $\mathbb{Z}$ gilt $93 = 3 \cdot 31$ und $42 = 2 \cdot 3 \cdot 7$, d.h. $\mathrm{ggT}(93, 42) = 3$.

ggT als Linearkombination

Lemma von Bézout

Sei R ein Hauptidealring und $a, b \in R$. Dann existieren $x, y \in R$ mit

$$xa + yb = \mathrm{ggT}(a, b).$$

Wir bezeichnen x, y als *Bézout-Koeffizienten* von a, b.

Beweis:

- Wir betrachten das Ideal $I = \langle a, b \rangle = \{xa + yb \mid x, y \in R\}$.
- Da R ein Hauptidealring ist, gilt $I = \langle c \rangle$.
- Behauptung: $c = \mathrm{ggT}(a, b)$.
- Wegen $a, b \in I$ gilt $a = ec$ und $b = e'c$. D.h. $c|a$ und $c|b$.
- Ist ferner d ein gemeinsamer Teiler von a und b, so teilt d jedes Element der Form $xa + yb$, d.h. jedes Element in I.
- Insbesondere gilt $d|c$, d.h. c muss der ggT sein.
- Da $c \in I = \{xa + yb \mid x, y \in R\}$ existieren $x, y \in R$ mit

$$xa + yb = c = \mathrm{ggT}(a, b).$$

Anmerkung:

(x, y) ist nicht eindeutig, auch $(x - kb, y + ka)$ erfüllt obige Gleichung.

Euklidischer Algorithmus (um 300 v.Chr.)

Ziel: Berechne $\mathrm{ggT}(a, b)$ effizient, ohne Primfaktorzerlegung.

Szenario: Sei R ein euklidischer Ring mit Bewertungsfunktion $N(\cdot)$.

Algorithmus EUKLID

EINGABE: $a_0, a_1 \in R$ mit $N(a_0) \geq N(a_1)$

1. Setze $i := 1$.
2. While $(a_i \neq 0)$
   1. Berechne mittels euklidischer Division q_i, a_{i+1} mit
      $$a_{i-1} = q_i a_i + a_{i+1} \text{ und } N(a_{i+1}) < N(a_i) \text{ oder } a_{i+1} = 0.$$
   2. Setze $i := i + 1$.

AUSGABE: $a_{i-1} = \mathrm{ggT}(a_0, a_1)$

Korrektheit des Euklidischen Algorithmus

Satz Euklid

Bei Eingabe $a_0, a_1 \in R$ berechnet Algorithmus EUKLID $\mathrm{ggT}(a_0, a_1)$.

Beweis:

- Da die Bewertungsfunktion nur positive Werte annimmt und $N(a_1) > N(a_2) > \ldots$, muss EUKLID mit einem $a_k = 0$ terminieren.
- Für alle $0 < i < k$ gilt

$$\begin{aligned}\mathrm{ggT}(a_{i-1}, a_i) &= \mathrm{ggT}(q_i a_i + a_{i+1}, a_i) = \mathrm{ggT}(a_{i+1}, a_i) \\ &= \mathrm{ggT}(a_i, a_{i+1}).\end{aligned}$$

- Es folgt

$$\mathrm{ggT}(a_0, a_1) = \ldots = \mathrm{ggT}(a_{k-1}, a_k) = \mathrm{ggT}(a_{k-1}, 0) = a_{k-1}.$$

Übung: In $\mathbb{Z}$ kann $\mathrm{ggT}(a_0, a_1)$ in Zeit $\mathcal{O}(\log^3 a_0)$ berechnet werden.