Übungsblatt 4: Teilbarkeitslehre

Lassen Sie sich nicht durch die Menge der Aufgaben einschüchtern. Es gibt nur wenig schriftliche Aufgaben und wir halten die Menge der Votieraufgaben überschaubar. Alle weiteren Aufgaben sind ein gutgemeinter Vorschlag: Wir möchten Sie ermutigen, sich über das Notwendigste hinaus mit Algebra zu beschäftigen.

1. Hauptidealringe und faktorielle Ringe

V 1.1. Welches sind die irreduziblen Elemente in $\mathbb{C}[X]$. Und in $\mathbb{R}[X]$?

S 1.2. (3 Punkte) $\mathbb{Z}[X]$ ist kein Hauptidealring, denn z.B. $(2,X)$ ist kein Hauptideal.

1.3. Der Polynomring $K[X]$ ist genau dann ein Hauptidealring, wenn K ein Körper ist.

2. Nicht-eindeutige Zerlegung in irreduzible Elemente

2.1. Für jedes $k \in \mathbb{N}$ ist $M_k = 1+k\mathbb{N}$ ein Untermonoid von $(\mathbb{N},\cdot)$. In $M_1 = \{1,2,3,4,\dots\}$ lässt sich jedes Element eindeutig in irreduzible Faktoren zerlegen. Gilt dies auch in $M_2 = \{1,3,5,7,\dots\}$? und in $M_3 = \{1,4,7,10,\dots\}$?

2.2. Selbst ein Polynomring kann nicht-faktorielle Unterringe haben:

(a) Man zeige, dass $K := \{\, P \in \mathbb{Q}[X] \mid P'(0) = 0 \,\}$ ein Unterring von $\mathbb{Q}[X]$ ist. Es ist $K = \mathbb{Q}[X^2, X^3]$ der von $\{X^2, X^3\}$ über $\mathbb{Q}$ erzeugte Unterring.

(b) Man bestimme die Gruppe $K^\times$ der in K invertierbaren Elemente.

(c) Lässt sich jedes Element in K als Produkt irreduzibler Faktoren schreiben?

(d) Sind die Polynome X^2 und X^3 im Ring K irreduzibel? Sind sie prim?

(e) In K bestimme man alle Zerlegungen von X^6 und X^7 in irreduzible Faktoren.

(f) Man gebe $P, Q \in K$ an, die in K keinen größten gemeinsamen Teiler haben.

3. Keine Zerlegung in irreduzible Elemente

Es ist nicht einfach, einen Ring zu finden, in dem sich manche Elemente nicht als Produkt von irreduziblen Elementen schreiben lassen. Hier eines der einfachsten Beispiele:

Wir schreiben das Monoid $(\mathbb{Q}_{\geq 0},+)$ multiplikativ als $M = \{X^a \mid a \in \mathbb{Q}_{\geq 0}\}$ mit $X^a \cdot X^b = X^{a+b}$. Sei $R = \mathbb{C}M$ der Monoidring über dem Körper $\mathbb{C}$ der komplexen Zahlen: Jedes Element schreibt sich eindeutig als eine Summe $a_1 X^{e_1} + \cdots + a_n X^{e_n}$ der Länge $n \in \mathbb{N}$ mit Koeffizienten $a_1, \dots, a_n \in \mathbb{C}^*$ und Exponenten $0 \leq e_1 < \cdots < e_n$ in $\mathbb{Q}$.

3.1. (a) Für jedes $n \in \mathbb{N}$, $n \geq 1$, ist $\mathbb{C}[X^{1/n}] \subset R$ ein Polynomring in $X^{1/n}$ über $\mathbb{C}$.

(b) Jede endliche Familie $P_1, \dots, P_k \in R$ liegt in einem Polynomring $\mathbb{C}[X^{1/n}] \subset R$.

(c) Man bestimme die Gruppe $R^\times$ der in R invertierbaren Elemente.

(d) Man bestimme alle irreduziblen Elemente in R. Ist R faktoriell?

4. Der Ring $\mathbb{Z}[i]$ der Gauss'schen Zahlen

S 4.1. (6 Punkte)

(a) Die Menge $\mathbb{Z}[i] = \{\, a+bi \mid a,b \in \mathbb{Z} \,\}$ ist ein Unterring von $\mathbb{C}$.

(b) Die Norm $N(z) = z\bar{z}$ ist ein Monoidhomomorphismus $N\colon (\mathbb{Z}[i],\cdot) \to (\mathbb{N},\cdot)$ mit $N(z) = 0 \Leftrightarrow z = 0$ und $N(z) = 1 \Leftrightarrow z \in \mathbb{Z}[i]^\times$. Man bestimme $\mathbb{Z}[i]^\times$.

(c) Wenn $N(z)$ irreduzibel in $\mathbb{N}$ ist, dann ist z irreduzibel in $\mathbb{Z}[i]$.

(d) Der Ring $\mathbb{Z}[i]$ ist euklidisch bezüglich der Norm N. *Hinweis:* Zu $a,b \in \mathbb{Z}[i], b \neq 0$, approximiere man $\frac{a}{b} \in \mathbb{C}$ durch ein $q \in \mathbb{Z}[i]$ mit $|\frac{a}{b} - q|^2 \leq \frac{1}{2}$.

Dass der Ring $\mathbb{Z}[i]$ euklidisch ist, hat erstaunliche Konsequenzen für Primzahlen in $\mathbb{Z}$:

S 4.2. (2 Punkte) Jede Primzahl $p \in \mathbb{Z}$ lässt sich auf höchstens eine Art als Summe von zwei Quadraten schreiben, das heißt, aus $p = a^2 + b^2 = c^2 + d^2$ folgt $\{a^2, b^2\} = \{c^2, d^2\}$. *Hinweis:* Man betrachte $p = (a+ib)(a-ib) = (c+id)(c-id)$ in $\mathbb{Z}[i]$.

Für die Primzahl 2 gilt $2 = 1^2 + 1^2$. Für die Primzahlen $3, 7, 11, \ldots$ gibt es keine solche Zerlegung. Andererseits gilt $5 = 1^2 + 2^2$ und $13 = 2^2 + 3^2$ und $17 = 1^2 + 4^2$, ...

Satz (Zwei-Quadrate-Satz von Fermat) *Die Primzahlen $p \in \mathbb{N}$ mit $p \equiv 3 \pmod 4$ lassen sich nicht als Summe von zwei Quadraten schreiben. Zu jeder Primzahl $p \in \mathbb{N}$ mit $p \equiv 1 \pmod 4$ existiert genau ein Paar $a < b$ in $\mathbb{N}$ sodass $p = a^2 + b^2$.*

V 4.3. Für $p \equiv 3 \pmod 4$ ist $p = a^2 + b^2$ schon modulo 4 unmöglich.

Im Folgenden sei $p \in Z$ eine Primzahl mit $p \equiv 1 \pmod 4$.

V 4.4. (a) Es gibt $\xi \in \mathbb{Z}/_p$ mit $\xi^2 = -1$. *Hinweis:* In $\mathbb{Z}/_p$ vergleiche man $1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$ und $\frac{p+1}{2} \cdots (p-2) \cdot (p-1)$ und berechne ihr Produkt.
(b) Aus $p \mid q^2 + 1$ in $\mathbb{Z}$ folgt $p \mid (q+i)(q-i)$ in $\mathbb{Z}[i]$. Ist p prim?
(c) In $\mathbb{Z}[i]$ zerfällt p in zwei irreduzible Faktoren, $p = (a+ib)(a-ib)$.

5. Die Ringe $\mathbb{Z}[i\sqrt{2}]$ und $\mathbb{Z}[i\sqrt{3}]$

5.1. (a) Für $\xi = i\sqrt{2}$ ist $\mathbb{Z}[\xi] = \{\, a + b\xi \mid a, b \in \mathbb{Z} \,\}$ ein Unterring von $\mathbb{C}$.
Man zeichne das Gitter $\mathbb{Z}[\xi]$ in der komplexen Ebene und bestimme $\mathbb{Z}[\xi]^\times$.
(b) Jede komplexe Zahl $q \in \mathbb{C}$ erlaubt eine Näherung $z \in \mathbb{Z}[\xi]$ mit $|q - z|^2 \leq \frac{3}{4}$.
Man folgere daraus, dass $\mathbb{Z}[\xi]$ ein euklidischer Ring ist bezüglich $N(z) = z\bar{z}$.

5.2. (a) Für $\xi = i\sqrt{3}$ ist $\mathbb{Z}[\xi] = \{\, a + b\xi \mid a, b \in \mathbb{Z} \,\}$ ein Unterring von $\mathbb{C}$.
Man zeichne das Gitter $\mathbb{Z}[\xi]$ in der komplexen Ebene und bestimme $\mathbb{Z}[\xi]^\times$.
(b) Jede komplexe Zahl $q \in \mathbb{C}$ erlaubt eine Näherung $z \in \mathbb{Z}[\xi]$ mit $|q - z|^2 \leq 1$.
Warum bricht die Konstruktion einer euklidischen Division hier zusammen?
(c) Man zähle die kleinsten Werte der Norm $N\colon \mathbb{Z}[\xi] \to \mathbb{N}$, $N(z) = z\bar{z}$, auf und folgere daraus, dass jedes Element $z \in \mathbb{Z}[\xi]$ mit $N(z) = 4$ irreduzibel ist.
(d) Man betrachte $2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$. Ist $\mathbb{Z}[i\sqrt{3}]$ faktoriell?

6. Euklidischer Algorithmus

6.1. Die Ringe $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[X]$ sind euklidisch. Man berechne:

(a) $\operatorname{ggT}(24087, 33411)$ in $\mathbb{Z}$, (b) $\operatorname{ggT}(5+3i, 13+8i)$ in $\mathbb{Z}[i]$,

(c) $\operatorname{ggT}(X^5 + X^4 + X^3 + X^2 + X + 1, X^4 - X^3 - X + 1)$ in $\mathbb{Q}[X]$.

6.2. Prüfen Sie, ob die folgenden Gleichungen in $\mathbb{Z}^2$ lösbar sind und bestimmen Sie gegebenenfalls alle Lösungen.

(a) $320x - 18y = 2$, (b) $102x - 15y = 5$, (c) $101x - 15y = 5$.

6.3. Sei $n = 582$ und $a = 115$. Man bestimme a^{-1} in $\mathbb{Z}/_n$.

6.4. Man wende den (erweiterten) euklidischen Algorithmus auf das folgende Problem an.
(a) Zu den Polynomen $P = X^2 + 1$ und $Q = X^3 - 2$ in $\mathbb{Q}[X]$ bestimme man $T = \operatorname{ggT}(P, Q)$ in $\mathbb{Q}[X]$ sowie $U, V \in \mathbb{Q}[X]$ sodass $T = UP + VQ$.
(b) Man vereinfache $\frac{X^3+1}{(X^2+1)(X^3-2)}$ zu $A + \frac{B}{X^2+1} + \frac{C}{X^3-2}$ und bestimme hierzu $A, B, C \in \mathbb{Q}[X]$ so, dass $\deg B < 2$ und $\deg C < 3$.