Musterlösung Serie 14

PRIMELEMENTE, IRREDUZIBLE ELEMENTE, UND DER RING DER POTENZREIHEN

---

73. Beweisen Sie, dass es unendlich viele Primzahlen $p \in \mathbb{Z}$ gibt.

Hinweis: Nehmen Sie an, es gibt nur endlich viele Primzahlen $p_1, \ldots, p_n$ und betrachten Sie die Primfaktorzerlegung von $p_1 p_2 \cdots p_n + 1$.

Lösung: Wir nehmen an, es gäbe nur endlich viele Primzahlen $2, p_1, \ldots, p_n \in \mathbb{N}$. Wir setzen $p_0 := 2$ und definieren die Zahl $N := 2p_1 p_2 \cdots p_n + 1$. Nach der Existenz der Primfaktorzerlegung existieren $e_0, \ldots, e_n \geqslant 0$ mit

$$N = p_0^{e_0} p_1^{e_1} \cdots p_n^{e_n}.$$

Wir haben $N > 1$, also existiert $k \geqslant 0$ so dass $e_k > 0$. Nun gilt

$$0 \equiv N \equiv 1 \pmod{p_k}.$$

Dies ist ein Widerspruch, also müssen unendlich viele Primzahlen existieren.

74. Wir betrachten den Ring der Potenzreihen

$$\mathbb{C}[[t]] := \left\{ \sum_{n=0}^{\infty} a_n t^n : a_n \in \mathbb{C} \right\}.$$

Die Addition wird definiert durch

$$\sum_{n=0}^{\infty} a_n t^n + \sum_{n=0}^{\infty} b_n t^n = \sum_{n=0}^{\infty} (a_n + b_n) t^n$$

und die Multiplikation durch

$$\left(\sum_{n=0}^{\infty} a_n t^n \right) \left(\sum_{n=0}^{\infty} b_n t^n \right) = \sum_{n=0}^{\infty} \sum_{m=0}^{n} a_m b_{n-m} t^n.$$

(a) Zeigen Sie, dass eine Potenzreihe $P \in \mathbb{C}[[t]]$ eine Einheit ist dann und nur dann wenn $P(0) \neq 0$.

Hinweis: Beweisen Sie die Gleichung

$$\frac{1}{1 - tP} = \sum_{n=0}^{\infty} P^n t^n$$

für alle $P \in \mathbb{C}[[t]]$.

(b) Zeigen Sie, dass für jede Potenzreihe $P \in \mathbb{C}[[t]]$ mit $P \neq 0$ eine eindeutige Einheit $u \in \mathbb{C}[[t]]$ und ein eindeutiges $k \geqslant 0$ mit $P = ut^k$ existiert. Schliessen Sie daraus, dass $\mathbb{C}[[t]]$ ein faktorieller Ring ist.

(c) Wir definieren den Ring der Laurentreihen

$$\mathbb{C}((t)) := \left\{ \sum_{n \geqslant M}^{\infty} a_n t^n : M \in \mathbb{Z}, a_n \in \mathbb{C} \right\}.$$

Beweisen Sie, dass der Quotientenkörper von $\mathbb{C}[[t]]$ isomorph zu $\mathbb{C}((t))$ ist.

Lösung:

(a) Sei $P \in \mathbb{C}[[t]]$ eine Einheit. Dann existiert $Q \in \mathbb{C}[[t]]$ mit $PQ = 1$. Wir schreiben $P = \sum a_n t^n$ und $Q = \sum b_n t^n$. Dann gilt $P(0) = a_0$ und $Q(0) = b_0$. Aus der Multiplikationsregel schliessen wir

$$1 = (PQ)(0) = a_0 b_0 = P(0)Q(0).$$

Also folgt $P(0) \neq 0$.
Sei $P \in \mathbb{C}[[t]]$ eine beliebige Potenzreihe. Die Potenzreihe

$$Q := \sum_{n=0}^{\infty} P^n t^n$$

ist wohldefiniert, denn der Summand $P^n t^n$ hat nur Koeffizienten vom Grad $\geqslant n$. Sei $m \geqslant 1$. Dann gilt

$$Q \equiv \sum_{n=0}^{m-1} P^n t^n \pmod{t^m}.$$

Nun erhalten wir

$$(1 - tP)Q \equiv \sum_{n=0}^{m-1} (1 - tP)t^n P^n \equiv 1 - t^m P^m \equiv 1 \pmod{t^m}$$

Zwei Potenzreihen $Q_1, Q_2 \in \mathbb{C}[[t]]$ erfüllen $Q_1 \equiv Q_2 \pmod{t^m}$ dann und nur dann falls die ersten m Koeffizienten in Q_1 und Q_2 übereinstimmen. Dies folgt aus der Beschreibung des Ideals

$$(t^m) = \left\{ \sum_{n=m}^{\infty} a_n t^n : a_n \in \mathbb{C} \right\}.$$

Also gilt $Q_1 \equiv Q_2 \pmod{t^k}$ für alle $k \geqslant 1$ dann und nur dann falls $Q_1 = Q_2$. Insbesondere erhalten wir

$$(1 - tP)Q = 1.$$

Sei $P \in \mathbb{C}[[t]]$ mit $P(0) \neq 0$. Da $P(0)$ eine Einheit ist, reicht es aus ein Inverses für $Q := P/P(0)$ zu konstruieren. Es gilt $Q(0) = 1$, also existiert eine eindeutige Potenzreihe $\tilde{Q} \in \mathbb{C}[[t]]$ mit

$$Q = 1 + t\tilde{Q}.$$

Die vorher bewiesene Formel definiert ein Inverses für Q. Also ist Q eine Einheit.

(b) Sei $P \in \mathbb{C}[[t]]$ mit $P \neq 0$ und $P = \sum a_n t^n$. Wir definieren die *Ordnung von* P als die minimale Zahl $\operatorname{ord} P \in \mathbb{N}$ mit $a_{\operatorname{ord} p} \neq 0$. Wir definieren

$$Q := \sum_{n=0}^{\infty} a_{n+\operatorname{ord} P} t^n.$$

Die definierende Eigenschaft der Ordnung impliziert nun $P = t^{\operatorname{ord} P} Q$ und $Q(0) \neq 0$.
Seien $P, Q \in \mathbb{C}[[t]]$ mit $P \neq 0$ und $Q \neq 0$. Dann gilt $PQ \neq 0$ und die Ordnung wird beschrieben wird durch

$$\operatorname{ord} PQ = \operatorname{ord} P + \operatorname{ord} Q.$$

Weiters folgt aus Aufgabe (a), dass P eine Einheit ist dann und nur dann falls die Ordnung $\operatorname{ord} P = 0$ erfüllt.
Wir beachten eine Potenzreihe $P \in \mathbb{C}[[t]]$ mit zwei Faktorisierungen $P = t^{k_1} u_1$ und $P = t^{k_2} u_2$. Nun gilt

$$k_1 = \operatorname{ord} t^{k_1} + \operatorname{ord} u_1 = \operatorname{ord} P = k_2.$$

Also erhalten wir $t^k u_1 = t^k u_2$. Da $\mathbb{C}[[t]]$ ein Integritätsbereich ist, folgt nun $u_1 = u_2$.
Sei $t = PQ$ für $P, Q \in \mathbb{C}[[t]]$. Dann gilt

$$1 = \operatorname{ord} P + \operatorname{ord} Q.$$

O.B.d.A. können wir $\operatorname{ord} P = 1$ und $\operatorname{ord} Q = 0$ annehmen. Also ist Q eine Einheit. Somit ist t irreduzibel.
Sei $P \in \mathbb{C}[[t]]$ irreduzibel. Dann ist P keine Einheit, also gilt $\operatorname{ord} P > 0$. Falls $\operatorname{ord} P > 1$, dann existiert eine Potenzreihe $Q \in \mathbb{C}[[t]]$ mit

$$P = t^2 Q = (tQ)t.$$

Dies ist ein Wiederspruch, weil weder tQ noch t eine Einheit ist. Also gilt $\operatorname{ord} P = 1$. Also existiert eine Einheit $u \in \mathbb{C}[[t]]$ mit

$$P = ut.$$

Also sind alle irreduziblen Elemente zu t assoziiert.
Sei $P \in \mathbb{C}[[t]]$ eine Potenzreihe mit $P = vQ_1Q_2 \cdots Q_n$ für irreduzible Elemente $Q_i \in \mathbb{C}[[t]]$ und eine Einheit $v \in \mathbb{C}[[t]]$. Dann gilt $n = \operatorname{ord} P$ wegen der Additivität der Ordnung. Also ist diese Faktorisierung eine Unnummerierung bis aus Assoziierung der Faktorisierung $P = ut^n$. Somit sind alle Zerlegungen von P Unnummerierungen bis auf Assoziierung der irreduziblen Faktoren voneinander, weil diese Relation transitiv ist.
Man könnte den Beweis alternativ auch wie folgt führen. Sei $I \subseteq \mathbb{C}[[t]]$ ein nicht-triviales Ideal. Sei

$$n := \min\{\operatorname{ord} P : P \in I, P \neq 0\}.$$

Dann existiert $P \in I$ mit $P = ut^n$ für eine Einheit $u \in \mathbb{C}[[t]]$ nach der Existenz der Faktorisierung, welche wir bereits bewisen haben. Also folgt $(t^n) = (P) \subseteq I$. Sei

nun $P \in I$ mit $P \neq 0$. Dann können wir $P = t^m u$ für ein $m \geqslant n$ und eine Einheit $u \in \mathbb{C}[[t]]$ schreiben. Also gilt $P \in (t^n)$. Somit folgt

$$I = (t^n).$$

Wir haben bereits bewiesen, dass $\mathbb{C}[[t]]$ ein Integritätsbereich ist, also ist es ein Hauptidealring. Also ist $\mathbb{C}[[t]]$ ein faktorieller Ring. Wir wissen, dass (t) das einzige maximale Ideal in $\mathbb{C}[[t]]$ ist, weil jedes nicht-triviale Ideal in $\mathbb{C}[[t]]$ von der Form (t^n) ist. Insbesondere ist t irreduzibel (weil jedes maximale Ideal ist prim) und jedes irreduzible Element zu t assoziiert. Also folgt aus der Eindeutigkeit der Zerlegung in irreduzible Faktoren, dass für jedes Element $P \in \mathbb{C}[[t]]$ eine eindeutige Einheit $u \in \mathbb{C}[[t]]$ und ein eindeutiges $k \geqslant 0$ existiert mit $P = ut^k$.

(c) Sei $P \in \mathbb{C}((t))$ eine Laurentreihe mit $P \neq 0$ und $P = \sum a_n t^n$. Dann existiert eine minimale Zahl $\operatorname{ord} P \in \mathbb{Z}$ mit $a_{\operatorname{ord} P} \neq 0$. Es existiert eine Einheit $u \in \mathbb{C}[[t]]$ mit

$$P = t^{\operatorname{ord} P} u.$$

Somit ist P invertierbar weil $P^{-1} := t^{-\operatorname{ord} P} u^{-1}$ ein Inverses von P definiert. Also ist $\mathbb{C}((t))$ ein Körper.

Sei K der Quotientenkörper von $\mathbb{C}[[t]]$. Die Inklusion definiert einen injektiven Ringhomomorphismus

$$i\colon \mathbb{C}[[t]] \to \mathbb{C}((t)),\ P \mapsto P.$$

Nach der universellen Eigenschaft des Quotientenkörpers existiert ein Ringhomomorphismus $j\colon K \to \mathbb{C}((t))$ mit $j\left(\frac{P}{1}\right) = P$. Die Abbildung j ist injektiv weil sie ein Ringhomomorphismus von Körpern ist. Sei $P \in \mathbb{C}((t))$ mit $P \neq 0$. Dann können wir $P = Qt^{-n}$ für ein $Q \in \mathbb{C}[[t]]$ und $n \geqslant 0$ schreiben. Dann gilt

$$i\left(\frac{Q}{t^n}\right) = i(Q)(i(t^n))^{-1} = Qt^{-n} = P.$$

Also ist i bijektiv. Somit folgt, dass j ein Isomorphismus ist.

75. Im Ring $R := \mathbb{Z}[i\sqrt{5}] \subset \mathbb{C}$ gilt die Gleichheit

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

Zeige:

(a) Die Funktion $N\colon R \to \mathbb{N}, z = a + bi\sqrt{5} \mapsto |z|^2 = a^2 + 5b^2$ ist multiplikativ (das heisst, $\forall \alpha, \beta \in R : N(\alpha\beta) = N(\alpha)N(\beta)$).

(b) $R^* = \{u \in R \mid N(u) = 1\} = \{\pm 1\}$.

(c) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind unzerlegbar in R.

(d) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind keine Primelemente in R.

(e) Für das Ideal $I = (2, 1 + i\sqrt{5})$ gilt $I \cdot I = (2)$.

(f) I ist kein Hauptideal von R.

(g) I ist ein maximales Ideal von R.

(h) Kein anderes Primideal enthält die Zahl 2.

(i) R ist nicht faktoriell.

Lösung: (a) F"ur alle $\alpha \in R$ gilt $N(\alpha) = |\alpha|^2$, wobei $|\cdot|$ den gewöhnlichen komplexen Absolutbetrag bezeichnet. Für alle $\alpha, \beta \in R$ folgt daraus

$$N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta),$$

wie gewünscht.

Variante: Seien $\alpha = a_1 + a_2 i\sqrt{5}$ und $\beta = b_1 + b_2 i\sqrt{5} \in R$. Dann ist

$$\begin{aligned} N(\alpha\beta) &= N(a_1b_1 - 5a_2b_2 + (a_1b_2 + a_2b_1)i\sqrt{5}) \\ &= (a_1b_1 - 5a_2b_2)^2 + 5(a_1b_2 + a_2b_1)^2 \\ &= a_1^2b_1^2 + 25a_2^2b_2^2 + 5a_1^2b_2^2 + 5a_2^2b_1^2 \\ &= (a_1^2 + 5b_1^2)(b_1^2 + 5b_2^2) \\ &= N(a_1 + a_2 i\sqrt{5})N(b_1 + b_2 i\sqrt{5}) = N(\alpha)N(\beta). \end{aligned}$$

(b) Betrachte eine Einheit $u = a + bi\sqrt{5} \in R$. Da N multiplikativ ist, gilt $N(u^{-1}) \cdot N(u) = N(u^{-1}u) = N(1) = 1$. Wegen $N(u^{-1}), N(u) \in \mathbb{N}$ muss daher $N(u) = a^2 + 5b^2 = 1$ sein. Daraus folgt sofort $b = 0$ und $a^2 = 1$, also $u = a = \pm 1$. Umgekehrt gilt für jedes Element $u = a + bi\sqrt{5} \in R$ mit $a^2 + 5b^2 = 1$ auch $(a + bi\sqrt{5})(a - bi\sqrt{5}) = 1$, also ist u eine Einheit in R.

(c) Falls $2 = \alpha\beta$ mit $\alpha, \beta \in R$ ist, folgt $4 = N(2) = N(\alpha)N(\beta)$. Wenn α und β keine Einheiten sind, ist $N(\alpha), N(\beta) > 1$ nach (b). Es gibt dann nur die Möglichkeit $N(\alpha) = N(\beta) = 2$. Diese kann aber nicht auftreten, da 2 wegen $a^2 + 5b^2 \neq 2$ für alle $a, b \in \mathbb{Z}$ nicht im Bild von N liegt. Somit ist 2 unzerlegbar in R.

Wegen $a^2 + 5b^2 \neq 3$ für alle $a, b \in \mathbb{Z}$ liegt auch 3 nicht im Bild von N. Wegen $N(3) = 9 = 3 \cdot 3$ folgt darum analog, dass 3 unzerlegbar in R ist.

Falls $1 + i\sqrt{5} = \alpha\beta$ mit $\alpha, \beta \in R$ ist, folgt $6 = N(1 + i\sqrt{5}) = N(\alpha)N(\beta)$. Wenn α und β keine Einheiten sind, dann müssen $N(\alpha), N(\beta) \in \{2, 3\}$ sein. Dies ist wiederum nicht möglich, da 2 und 3 nicht im Bild von N liegen. Daher ist $1 + i\sqrt{5}$ unzerlegbar. Mit der gleichen Argumentation folgt auch die Unzerlegbarkeit von $1 - i\sqrt{5}$.

(d) Wegen der Gleichheit $6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ sind 2 und 3 Teiler von $(1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ und $1 + i\sqrt{5}$ und $1 - i\sqrt{5}$ Teiler von $2 \cdot 3$. Keines der vier Elemente ist aber ein Teiler eines anderen, weil sie nach (c) unzerlegbar sind, sich aber nach (b) nicht um Einheiten unterscheiden, da sie vershiedene Bilder unter N haben.

(e) Durch Multiplikation der Erzeuger erhalten wir

$$I \cdot I = (2, 1 + i\sqrt{5})(2, 1 + i\sqrt{5}) = (4, 2 + 2i\sqrt{5}, -4 + 2i\sqrt{5}).$$

Da $(2) = \{2a + 2bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ist, haben wir $4, 2 + 2i\sqrt{5}, -4 + 2i\sqrt{5} \in (2)$ und daher $I \cdot I \subset (2)$. Umgekehrt ist

$$2 = (2 + 2i\sqrt{5}) - (-4 + 2i\sqrt{5}) - 4 \in I \cdot I.$$

Somit gilt $(2) = I \cdot I$.

(f) Wir nehmen an, dass I ein Hauptideal ist, d.h. $I = (2, 1 + i\sqrt{5}) = (\alpha)$ für ein $\alpha \in R$. Dann ist $2 = x\alpha$ für ein $x \in R$. Wegen der Unzerlegbarkeit von 2 ist entweder $x \in R^\times$ oder $\alpha \in R^\times$. Im ersten Fall ist 2 assoziiert zu α, also $(2) = (\alpha) = (2, 1 + i\sqrt{5})$. Dies ist ein Widerspruch, da $1 + i\sqrt{5}$ nicht in (2) liegt.

Es bleibt nur der Fall $\alpha \in R^\times$ übrig, in dem $I = (\alpha) = R$ ist. Auch dieser Fall kann nach (e) wegen des Widerspruchs

$$R = R \cdot R = I \cdot I = (2) \neq R$$

nicht auftreten. Somit ist I kein Hauptideal.

(g) Aus (f) folgt bereits, dass $I \neq (1)$, also ein echtes Ideal ist. Betrachte ein echt grösseres Ideal $I \subsetneq I' \subset R$ und wähle ein Element $a + bi\sqrt{5} \in I' \backslash I$. Die Rechnung $a + bi\sqrt{5} = (a - b) + b \cdot (1 + i\sqrt{5})$ zeigt dann, dass $a - b \notin I$ ist. Wegen $\mathbb{Z} \cap I = 2\mathbb{Z}$ bedeutet dies, dass $a - b$ ungerade ist. Also ist

$$1 \;=\; (a + bi\sqrt{5}) - \tfrac{a-b-1}{2} \cdot 2 - b \cdot (1 + i\sqrt{5}) \;\in\; (a + bi\sqrt{5}) + I \;\subset\; I'.$$

Somit ist $I' = (1)$; und deshalb ist I maximal.

(h) Sei $\mathfrak{p}$ ein Primideal, das 2 enthält. Dann ist auch $2 + 2 + 2 = 6 \in \mathfrak{p}$. Somit muss das Ideal $1 + i\sqrt{5}$ oder $1 - i\sqrt{5}$ enthalten. Wegen $1 + i\sqrt{5} = 2 - (1 - i\sqrt{5})$ enthält $\mathfrak{p}$ dann sowohl $1 + i\sqrt{5}$ als auch $1 - i\sqrt{5}$ und es folgt $I \subseteq \mathfrak{p}$. Da I maximal ist, folgt $I = \mathfrak{p}$.

(i) Mögliche Lösungen sind:

- Aus (c) und (d) folgt, dass in R unzerlegbare Elemente existieren, die nicht prim sind. Daher ist R nicht faktoriell.
- Die Gleichung $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ ergibt nach (c) zwei Zerlegungen von 6 in unzerlegbare Elemente. Bei (d) haben wir festgestellt, dass $2, 3 \nmid 1 \pm i\sqrt{5}$ und $1 \pm i\sqrt{5} \nmid 2, 3$ gilt. Daher sind $2, 3$ nicht zu $1 \pm i\sqrt{5}$ assoziiert und die beiden obigen Zerlegungen sind nicht zueinander assoziiert. Deshalb kann R nicht faktoriell sein.