Satz 1 (Polynomdivision)**.** *Sei K ein Körper und $P, Q \in K[t]$ mit $Q \neq 0$. Dann existieren eindeutige Polynome $q, r \in K[t]$, sodass $P = q \cdot Q + r$ mit* $\deg(r) < \deg(Q)$.

Beweis. **Eindeutigkeit**: Seien $q, q', r, r' \in K[t]$, sodass $P = q \cdot Q + r$ mit $\deg(r) < \deg(Q)$ und $P = q' \cdot Q + r'$ mit $\deg(r') < \deg(Q)$. Dann gilt $(q - q')Q = (r' - r)$ und nach Satz I.1 der Vorlesung $\deg(r - r') \leq \max(\deg(r), \deg(r'))$, also $\deg(r - r') < \deg(Q)$. Wiederum nach Satz I.1 muss dann gelten $\deg(q - q') = -\infty$, also $q = q'$ und dann auch $r = r'$.

Existenz: Angenommen, es existiert $q \in K[t]$ mit $P = q \cdot Q$. Dann setzen wir $r = 0$; in diesem Fall gilt $\deg(r) = -\infty$ und wir sind fertig. Andernfalls existiert kein $q \in K[t]$ mit $P = q \cdot Q$. Wir wählen dann $q \in K[t]$, sodass $\deg(P - q \cdot Q)$ minimal ist (dies ist möglich, da $\deg(P - qQ) \geq 0$ für alle $q \in K[t]$ gilt). Wir setzen dann $r = P - q \cdot Q$. Zu zeigen bleibt: $\deg(r) < \deg(Q)$. Angenommen es gelte

$$d := \deg(r) \geq \deg(Q) =: d'.$$

Wir schreiben $Q = \sum_{i=0}^{d'} a_i t^i$ und $r = \sum_{i=0}^{d} b_i t^i$. Es gilt insbesondere $a_{d'} \neq 0$, also ist $a_{d'}$ invertierbar in K. Betrachte nun das Polynom $p = q + b_d a_{d'}^{-1} t^{d-d'}$ (beachte dabei, dass $d - d' \geq 0$ nach Annahme). Damit gilt

$$r - b_d a_{d'}^{-1} t^{d-d'} Q = P - (q + b_d a_{d'}^{-1} t^{d-d'})Q = P - pQ. \tag{1}$$

Andererseits gilt aber, da K ein Integritätsbereich ist,

$$\deg(b_d a_{d'}^{-1} t^{d-d'} Q) = d - d' + d' = d = \deg(r).$$

Weiterhin stimmen die Leitkoeffizienten von $b_d a_{d'}^{-1} t^{d-d'} Q$ und r überein. Damit gilt aber

$$\deg(r - b_d a_{d'}^{-1} t^{d-d'} Q) < \deg(r)$$

(da sich die beiden Leitkoeffizienten wegheben). Gleichung (1) liefert dann einen Widerspruch zur Definition von q und r. Somit gilt $\deg(r) < \deg(Q)$ und der Satz ist bewiesen. □

Bemerkungen 2.

- Der Beweis gibt kein explizites Verfahren, die Polynome q, r zu finden. Das kann man mit dem (aus der Schule bekannten) Verfahren der Polynomdivision machen. (Beachte dabei, dass jeder Schritt in dem Verfahren in der Tat über einem beliebigen Körper funktioniert.)
- Die Aussage des Satzes stimmt im Allgemeinen nicht, wenn man einen beliebigen Ring R vewendet, und sogar auch nicht notwendigerweise für Intergitätsbereiche. Denn sei beispielsweise $P = 3t \in \mathbb{Z}[t]$ und $Q = 5t \in \mathbb{Z}[t]$. Falls $P = q \cdot Q + r$ wie im Satz, muss $\deg q \cdot Q = \deg P = 1$ sein, also $\deg(q) = 0$ nach Satz I.1. der Vorlesung. Dies bedeutet $q = c$ für ein $c \in \mathbb{Z}$, aber die Gleichung $5c = 3$ hat keine Lösung im Ring der ganzen Zahlen.
- Gegeben seien $P, Q \in K[t]$. Dann gibt es ein (bis auf Einheiten in $K[t]$, also bis auf Elemente in $K \backslash \{0\}$ eindeutiges) Polynom $d \in K[t]$, welches der größte gemeinsame Teiler, $d = \mathrm{ggT}(P, Q)$, von P und Q ist. Damit meinen wir, dass $P = P' \cdot d$ und $Q = Q' \cdot d$ für geeignete

$P', Q' \in K[t]$, wobei d maximalen Grad unter allen Polynomen mit dieser Eigenschaft hat. Man erhält d durch den sogenannten erweiterten *Euklidischen Algorithmus*. Es gibt damit auch Polynome $a, b \in K[t]$ so dass $d = a \cdot P + b \cdot Q$.

Satz 3. *Sei K ein Körper und seien $P, Q \in K[t]$ und $d = \mathrm{ggT}(P, Q)$. Dann existieren $a, b \in K[t]$, sodass $d = a \cdot P + b \cdot Q$.*

Beweis. Setze $r_0 = Q$. Nach der Polynomdivision existieren q_0, r_1, sodass

$$P = q_0 \cdot r_0 + r_1 \quad \text{mit} \quad \deg(r_1) < \deg(r_0).$$

Wiederum nach der Polynomdivision existieren q_1, r_2, sodass $r_0 = q_1 \cdot r_1 + r_2$ mit $\deg(r_2) < \deg(r_1)$. Wendet man dieses Prinzip endlich oft an, erhält man schliesslich $q_0, \ldots, q_n, r_1, \ldots, r_{n+1}$ mit

$$\begin{aligned}
r_0 &= q_1 \cdot r_1 + r_2 && \text{mit } \deg(r_2) < \deg(r_1);\\
r_1 &= q_2 \cdot r_2 + r_3 && \text{mit } \deg(r_3) < \deg(r_2);\\
&\vdots && \vdots\\
r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n && \text{mit } \deg(r_n) < \deg(r_{n-1});\\
r_{n-1} &= q_n \cdot r_n + r_{n+1} && \text{mit } r_{n+1} = 0.
\end{aligned}$$

Damit folgt (indem man die Gleichungen in umgekehrter Reihenfolge betrachtet), dass r_n das Polynom r_{n-1} teilt, und dann aber auch alle $r_{n-2}, \ldots, r_0 = Q$ und schliesslich auch P. Ausserdem ergeben die Gleichungen $r_n = g \cdot P + h \cdot Q$. Da d sowohl P als auch Q teilt, teilt es auch r_n. Nach der Maximalität des ggT gilt $d = r_n$. Damit folgt die Behauptung. □

Bemerkungen 4. Völlig analog zeigt man, dass für gegebene $a, b \in \mathbb{Z}$, ganze Zahlen $c, r \in \mathbb{Z}$ mit $|r| < |b|$ existieren, sodass $a = cb + r$ gilt. Man folgert dann daraus, dass $d = \mathrm{ggT}(a, b)$ sich schreiben lässt als $d = c'a + c''b$ für gewisse $c', c'' \in \mathbb{Z}$.