Lemma. (Teilen mit Rest)
Sei A ein kommutativer Ring und sei $g \in A[X]$ mit

$$g = g_n X^n + (\text{niedrigere } X\text{-Potenzen}) \qquad \text{wobei} \quad g_n \in A^\times \ .$$

Für jedes $f \in A[X]$ gibt es eindeutige $q, r \in A[X]$ („Quotient“ und „Rest“) mit

$$f = gq + r \qquad \text{wobei} \quad \operatorname{grad}(r) < \operatorname{grad}(g) \ .$$

Beweis.

- *Existenz:*

  Sei $B(k)$ die Aussage „Für alle $f \in A[X]$ mit $\operatorname{grad}(f) \leq k$ gibt es $q, r \in A[X]$ mit $f = gq + r$ und $\operatorname{grad}(r) < \operatorname{grad}(g)$“.

  Für $k < n$ gilt $B(k)$, denn dann können wir $q = 0$ und $r = f$ wählen.

  Sei nun $k \geq n$. Angenommen, $B(k-1)$ ist wahr. Sei $f = f_k X^k + (\text{niedriger})$ gegeben. Betrachte $\tilde{f} = f - f_k g_n^{-1} X^{k-n} g$. Da f und $X^{k-n} g$ Grad $\leq k$ haben, gilt auch $\operatorname{grad}(\tilde{f}) \leq k$. Der Koeffizient von X^k in $\tilde{f}$ ist $f_k - f_k g_n^{-1} g_n = 0$. Somit gilt sogar $\operatorname{grad}(\tilde{f}) \leq k - 1$. Nach $B(k-1)$ gilt $\tilde{f} = g\tilde{q} + \tilde{r}$ mit $\operatorname{grad}(\tilde{r}) < n$. Einsetzen ergibt

  $$f = g\tilde{q} + \tilde{r} + f_k g_n^{-1} X^{k-n} g = g(\tilde{q} + f_k g_n^{-1} X^{k-n}) + \tilde{r} \ .$$

  Also ist auch $B(k)$ wahr.

- *Eindeutigkeit:*

  Sei $f = gq + r = g\tilde{q} + \tilde{r}$, wobei $r, \tilde{r}$ Grad $< n$ haben. Dann folgt $g(q - \tilde{q}) = \tilde{r} - r$. Angenommen, $q - \tilde{q} \neq 0$. Dann ist auch $g(q - \tilde{q}) \neq 0$ und es gilt $\operatorname{grad}(g(q - \tilde{q})) \geq n$. (Warum? Es ist nicht gefordert, dass A ein Integritätsbereich ist.) Dies ist ein Widerspruch, da $\operatorname{grad}(r - \tilde{r}) < n$. Somit $q = \tilde{q}$ und damit auch $r = \tilde{r}$.

□