

§ 5. Irreduzibilitätskriterien

(5.1) LEMMA: Sei K ein Körper und $f \in K[T]$. Dann gilt:

- a) Jedes Polynom $f \in K[T]$ vom Grade 1 ist irreduzibel.
- b) Ein Polynom $f \in K[T]$ vom Grade ≥ 2 , das eine Nullstelle in K besitzt, ist reduzibel.
- c) $\text{grad}(f) \in \{2, 3\}$: f irreduzibel über $K \iff f$ hat keine Nullstelle in K .
- d) Besitzt ein Polynom $f \in K[T]$ vom Grade ≥ 4 **keine** Nullstelle in K , so ist f nicht notwendig irreduzibel.

Bew: b) Besitzt f eine Nullstelle $a \in K$, so spaltet a den Linearfaktor $T - a$ ab (4.6a). Wegen $\text{grad}(f) \geq 2$ ist dann $T - a$ ein nichttrivialer Teiler von f , d.h. f ist nicht irreduzibel.

c) “ $\implies$ ” gilt nach b) “ $\impliedby$ ” Besitzt f keine Nullstelle in K , so hat f keinen Teiler vom Grade 1 aus $K[T]$. Wäre f reduzibel, so müßte aber f mindestens einen Teiler vom Grade 1 haben, da f den Grad 2 oder 3 hat.

d) Das Polynom $f = (T^2 - 2)(T^2 - 3) \in \mathbb{Q}[T]$ ist reduzibel, besitzt aber keine Nullstelle in $\mathbb{Q}$. •

(5.2) SATZ: Irreduzibilitätskriterium von Eisenstein

$f = \sum_{k=0}^m a_k T^k \in \mathbb{Z}[T]$ sei ein Polynom vom Grade $m \geq 1$ mit teilerfremden Koeffizienten. Es gebe eine Primzahl $p \in \mathbb{Z}$ mit

$$p \mid a_k \quad (\forall k \in \{0, 1, \dots, m-1\}) \quad , \quad p^2 \nmid a_0$$

Dann ist f irreduzibel über $\mathbb{Z}$.

Bew: Wegen $\text{ggT}(a_0, a_1, \dots, a_m) = 1$ folgt $p \nmid a_m$. Annahme: f ist reduzibel. Dann ist f das Produkt zweier echter Teiler $g = \sum_{j=0}^r b_j T^j$ und $h = \sum_{k=0}^s c_k T^k$ mit $b_r \neq 0$ und $c_s \neq 0$.

Annahme: $\text{grad}(g) = 0$, dh. $g \in \mathbb{Z} \setminus \{0\}$. Aus $f = g \cdot h$ folgt dann, daß g jeden Koeffizienten von f teilt, also $g \sim 1$. Damit ist aber g dann kein echter Teiler von f . Widerspruch! Folglich $r > 0$ und ebenso $s > 0$.

Aus $a_0 = b_0 c_0$ und $p \mid a_0$ ergibt sich wegen der Primzahleigenschaft von p : $p \mid b_0$ oder $p \mid c_0$. Es können aber beide Bedingungen nicht gleichzeitig gelten:

Aus $p \mid b_0$ **und** $p \mid c_0$ würde nämlich $p^2 \mid a_0$ im Gegensatz zur Voraussetzung folgen.

Gelte o.B.d.A. $p \mid b_0$ ($\implies p \nmid c_0$). Nun können nicht alle Koeffizienten von g durch p teilbar sein, da dies sonst auch für alle Koeffizienten von f folgen würde. Daher existiert ein $i \in \{0, 1, \dots, m\}$ mit

$$p \mid b_0, p \mid b_1, \dots, p \mid b_{i-1}, p \nmid b_i \quad (0 \leq i \leq r < m)$$

Für den Koeffizienten a_i von f ergibt sich damit

$$a_i = \underbrace{b_0 c_i + b_1 c_{i-1} + \dots + b_{i-1} c_1}_{\text{durch } p \text{ teilbar}} + b_i c_0 = px + b_i c_0$$

Nach Vor. ist a_i durch p teilbar, damit $p \mid b_i c_0$. Folglich $p \mid b_i$ oder $p \mid c_0$, was aber beides nicht möglich ist. **Widerspruch!**

Ein Polynom, das die Bedingungen aus (5.2) erfüllt, heißt ein **Eisenstein-Polynom (zur Primzahl p)**. Ist f insbesondere normiert, so sind alle Koeffizienten von f teilerfremd.

(5.3) BEISPIELE: a) $T^4 + 4T + 2 \in \mathbb{Z}[T]$ ist ein Eisenstein-Polynom für $p = 2$ und daher irreduzibel.

b) $T^n - p \in \mathbb{Z}[T]$ ist für jedes $n \in \mathbb{N}$ und für jede Primzahl $p \in \mathbb{P}$ irreduzibel.

!!! Es ist von vorneherein **nicht** klar, daß ein irreduzibles Polynom aus $\mathbb{Z}[T]$ auch irreduzibel über $\mathbb{Q}$ ist. Daß dies doch der Fall ist, zeigt das folgende Ergebnis.

(5.4) SATZ: Lemma von Gauß

R sei ein HIB und $K := \mathbb{Q}(R)$ der Quotientenkörper von R . Dann gilt für ein Polynom $f \in R[T]$ vom Grade ≥ 1 :

$$f \text{ irreduzibel in } R[T] \implies f \text{ irreduzibel in } K[T]$$

BEM: Die Umkehrung von (5.4) gilt nicht: $2T + 2$ ist irreduzibel über $\mathbb{Q}$, aber reduzibel über $\mathbb{Z}$.

(5.5) BEISPIELE: a) $2T^5 - 3T^3 + 9T - 12 \in \mathbb{Z}[T]$ ist irreduzibel über $\mathbb{Q}$ (Eisenstein-Polynom für $p = 3$).

b) $T^n - p \in \mathbb{Q}[T]$ ist irreduzibel für alle $n \in \mathbb{N}$, $p \in \mathbb{P}$. Nach (5.1b) folgt $\sqrt[n]{p} \notin \mathbb{Q}$

$$\forall n \in \mathbb{N}, n \geq 2, \forall p \in \mathbb{P}.$$

Das Polynom $f := T^2 + T + 1 \in \mathbb{Z}[T]$ ist kein Eisenstein-Polynom zu irgendeinem p . Es läßt sich jedoch durch Einsetzen von $T + 1$ zu einem solchen transformieren:

$f(T+1) = (T+1)^2 + (T+1) + 1 = T^2 + 2T + 1 + T + 1 + 1 = T^2 + 3T + 3$ ist Eisenstein-Polynom zu $p = 3$. Daß jetzt auch f irreduzibel ist, zeigt der folgende Satz, der in Aufgabe 17 bewiesen wird:

(5.6) SATZ: Es sei R ein IB. Sei $g = T - a \in R[T]$ und $E_g : R[T] \longrightarrow R[T]$ der Einsetzungshomomorphismus. Dann gilt:

a) E_g ist ein Ringisomorphismus

b) $f \in R[T] : f \text{ irreduzibel} \iff E_g(f) \text{ irreduzibel.}$

(5.7) BEISPIEL: Das Polynom $f := T^{p-1} + T^{p-2} + \dots + T^2 + T + 1 \in \mathbb{Z}[T]$ ist für jede Primzahl p irreduzibel über $\mathbb{Z}$ und $\mathbb{Q}$.

Es gilt $(T - 1)f = T^p - 1$. Sei $g = T + 1$. Dann folgt $E_g(T - 1)E_g(f) = E_g(T^p - 1)$ und daraus $TE_g(f) = (T+1)^p - 1 = \sum_{k=0}^p \binom{p}{k} T^k - 1 = \sum_{k=1}^p \binom{p}{k} T^k = T \left(\sum_{k=1}^p \binom{p}{k} T^{k-1} \right) \implies E_g(f) = \sum_{k=1}^p \binom{p}{k} T^{k-1} = T^{p-1} + \binom{p}{p-1} T^{p-2} + \dots + \binom{p}{2} T + \binom{p}{1}$ (nach dem binomischen Satz). Da alle Binomialkoeffizienten $\binom{p}{k}$ für $1 \leq k \leq p-1$ durch die Primzahl p teilbar sind (s. Aufg. 11a), ist $E_g(f)$ ein Eisenstein-Polynom für p . Daher ist $E_g(f)$ irreduzibel und damit auch f .