ALG Ü10

353) Eisensteinsches Kriterium

R... faktorieller Ring $\quad f = \sum_{i=0}^{n} a_i x^i \in R[x]$ mit Grad ≥ 1 ... primitives Polynom
$p \in R$... irreduzibel mit $p \nmid a_n$, $p \mid a_i$ für $i \in \{0, ..., n-1\}$ und $p^2 \nmid a_0$
$\Rightarrow f$ ist irreduzibel in $R[x]$

Indirekt angenommen f ist reduzibel in $R[x]$.

$\Rightarrow \exists\, q, r \in R[x]$ mit $0 < \text{grad}(q), \text{grad}(r) < n$ und $f = q \cdot r$

$$q = \sum_{i=0}^{m} b_i x^i \qquad r = \sum_{i=0}^{\ell} c_i x^i$$

*

$$h: R[x] \longrightarrow R[x]/pR[x] \qquad \text{"mod } p\text{"}$$
$$\sum_{i=0}^{k} d_i x^i \longmapsto \sum_{i=0}^{k} (d_i x^i) + pR[x] \cong \sum_{i=0}^{k} (d_i + pR) x^i$$

$h(q) \cdot h(r) = h(q \cdot r) = h(f) = a_n x^n + pR[x]$, da alle anderen Koeffizienten von p geteilt werden.

△ $\Rightarrow \exists\, j, k: 0 < j, k < n \;\wedge\; h(q) = \tilde{b}_j x^j + pR[x] \;\wedge\; h(r) = \tilde{c}_k x^k + pR[x]$

Also sind alle anderen Koeffizienten von p geteilt, insbesondere $p \mid b_0 \wedge p \mid c_0$

$\Rightarrow a_0 = b_0 \cdot c_0$ ergibt $p^2 \mid a_0$ ↯

---

* Da $pR[x] = \langle p \rangle_{\text{Ideal}}$ ein Primideal ist (p... irreduzibel und weil in faktoriellem Ring damit prim) folgt $R[x]/pR[x]$... Integritätsbereich.

△ $h(q) \cdot h(r) = (q + pR[x])(r + pR[x]) = qr + pR[x] = a_n x^n + pR[x]$

Angenommen $h(q)$ oder $h(r)$ ist kein "Monom" $z x^\alpha + pR[x]$.

o.B.d.A. $\exists\, \alpha, \beta \in \{1, ..., m\}: p \nmid b_\alpha \wedge p \nmid b_\beta \qquad \exists\, \gamma \in \{1, ..., \ell\}: p \nmid c_\gamma$

$$\Rightarrow q \cdot r = \Big(b_\alpha x^\alpha + b_\beta x^\beta + \sum_{\substack{i=0 \\ i \neq \alpha \\ i \neq \beta}}^{m} b_i x^i\Big)\Big(c_\gamma x^\gamma + \sum_{\substack{i=0 \\ i \neq \gamma}}^{\ell} c_i x^i\Big) = b_\alpha c_\gamma x^{\alpha+\gamma} + b_\beta c_\gamma x^{\beta+\gamma} + \ldots$$
$$\neq a_n x^n$$

□

ALG Ü10

353) Eisensteinsches Kriterium

R ... faktorieller Ring $f=\sum_{i=0}^{n} a_i x^i \in R[x]$ $grad(f) \geq 1$ f ... primitives Polynom

$p \in R$ ... irreduzibel $p \nmid a_n$ $p \mid a_i$ für $i \in \{0,\dots,n-1\}$ $p^2 \nmid a_0$

$\Rightarrow f$ ist irreduzibel in $R[x]$

Indirekt Angenommen f ist reduzibel in $R[x]$

$\Rightarrow \exists q, r \in R[x]$ mit $f = q \cdot r$ und $0 < grad(q), grad(r)$, da f primitives Polynom ist sowie $grad(q), grad(r) < n$, damit $grad(f) = n$

$q(x) = \sum_{i=0}^{m} b_i x^i$ $r(x) = \sum_{j=0}^{l} c_j x^j$

$\Rightarrow a_0 = b_0 \cdot c_0$

1. Fall $p \mid b_0 \wedge p \mid c_0 \Rightarrow p^2 \mid a_0$ ↯

2. Fall $p \mid b_0 \wedge p \nmid c_0 \Rightarrow \exists k \in \{1,\dots,m\}: p \nmid b_k$, da sonst $\forall k \in \{0,\dots,m\}: p \mid b_k$

$\Rightarrow p \mid q \Rightarrow p \mid f$ ↯ zu $p \nmid a_n$

Sei k mit dieser Eigenschaft minimal also $\forall i \in \{0,\dots,k-1\}: p \mid b_i \wedge$ $p \nmid b_k$

$\Rightarrow a_k = \sum_{i=0}^{k} b_i c_{k-i} = \sum_{i=0}^{k-1} b_i c_{k-i} + b_k c_0$

$p \mid \sum_{i=0}^{k-1} b_i c_{k-i}$, da $\forall i \in \{0,\dots,k-1\}: p \mid b_i$ $p \mid a_k$ da $\forall i \in \{0,\dots,n-1\}: p \mid a_i$ und $k \in \{1,\dots,m\}$; $m = grad(q) < n$

$\Rightarrow p \mid b_k c_0$ ↯ da $p \nmid b_k$ und $p \nmid c_0$

3. Fall $p \nmid b_0 \wedge p \mid c_0$ analog

4. Fall $p \nmid b_0 \wedge p \nmid c_0 \Rightarrow p \nmid a_0$ $(a_0 = b_0 \cdot c_0)$ ↯

$\Rightarrow f$ ist irreduzibel in $R[x]$

□