$R[X]/pR[X] \xrightarrow{\sim} (R/(p))[X]$.

4.7 Irreduzibilitätskriterien

Betrachte einen faktoriellen Ring R und ein Primelement p. Der Reduktionshomomorphismus $R \twoheadrightarrow R/(p)$, $a \mapsto \overline{a} := a + (p)$ induziert einen Homomorphismus

$$R[X] \twoheadrightarrow (R/(p))[X], \quad f = \sum{}' a_i X^i \mapsto \overline{f} := \sum{}' \overline{a_i} X^i.$$

Insbesondere gilt für alle $f, g \in R[X]$ die Gleichung $\overline{(fg)} = \overline{f} \cdot \overline{g}$.

4.7.1 Proposition: Jedes primitive Element $f \in R[X] \setminus \{0\}$ mit $\deg(f) = \deg(\overline{f})$ und $\overline{f}$ irreduzibel ist selbst irreduzibel.

Beweis: Sei $f = gh$ mit $g, h \in R[X]$.

$\Rightarrow \overline{f} = \overline{g} \cdot \overline{h}$ ($\overline{f}$ irreduzibel, insbesondere $\neq 0$) $\Rightarrow \overline{g}, \overline{h} \neq 0$ und $\overline{g}$ oder $\overline{h} \in (R/(p))^\times$. $\Rightarrow g$ oder $h \in R$

g oder $h \in R^\times$ (primitiv)

höchster Koeff. von f nicht durch p teilbar

dann für g, h: $\deg(\overline{g}) = \deg(g)$ und $\deg(\overline{h}) = \deg(h)$ gelt

Bsp.: $f = X + 2X^2 \in \mathbb{Z}[X]$
$p = 2 \Rightarrow \overline{f} = X \in \mathbb{F}_2[X]$
irreduzibel, aber
$f = X(1+2X)$ reduzibel

Bsp.: $f = 5X \in \mathbb{Z}[X]$
$p = 2 \Rightarrow \overline{f} = X \in \mathbb{F}_2[X]$
irred., aber f reduzibel

4.7.2 Beispiel: Das Polynom $X^5 + 2X^2 + 1 \in \mathbb{Z}[X]$ ist irreduzibel. (Benutze $p = 3$.)

f:

$p=2$: $f \equiv X^5 + 1 = (X+1)(X^4 + X^3 + X^2 + X + 1) \bmod 2$ reduzibel.

$p=3$: linearfaktor? $\leftrightarrow$ Nullstelle in $\mathbb{F}_3$, $f(0) \equiv 1$, $f(\pm 1) \equiv \pm 1 + 2 + 1 \equiv \pm 1$

quadratische Faktoren? $X^2 + aX + b$, $a, b \in \{0, 1, 2\}$.

Ansatz: $X^2 + aX \pm 1$ ...

f ↓

4.7.3 Beispiel: Das Polynom $X^4+3X^3-X^2+1 \in \mathbb{Z}[X]$ ist irreduzibel. (Benutze $p=5$. Aliter: Untersuche die Reduktionen bei $p=2$ und $p=3$ und vergleiche Grade.)

$p=2$: $f \equiv X^4+X^3+X^2+1 \equiv (X+1)(X^3+X+1) \mod (2)$ } Zerlegung in irreduzible

$p=3$: $f \equiv X^4+2X^2+1 = (X^2+1)^2$

$p=5$: $f \bmod (5)$ irred.

4.7.4 Satz: *(Eisenstein-Kriterium)* Sei $f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$ primitiv mit $n \geqslant 1$ und $p \nmid a_n$ und $\forall i < n$: $p \mid a_i$ und $p^2 \nmid a_0$. Dann ist f irreduzibel.

Bew.: Sei $f = g \cdot h$ mit $g, h \in R[X]$ und $\deg(g) = m$, $\deg(h) = \ell$; und $m, \ell > 0$

$g = \sum_{i=0}^{m} b_i X^i$, $h = \sum_{j=0}^{\ell} c_j X^j$

$\Rightarrow \bar{f} = \bar{g} \cdot \bar{h}$ in $(R/(p))[X]$

Voraussetzung $\Rightarrow \bar{f} = \bar{a}_n \cdot X^n$ mit $\bar{a}_n \neq 0$.

Beh.: $\bar{g} = \bar{b}_m \cdot X^m$ und $\bar{h} = \bar{c}_\ell X^\ell$.

Ber.: Sei i minimal mit $\bar{b}_i \neq 0$

j " " $\bar{c}_j \neq 0$

$\Rightarrow \bar{g}\bar{h} = \bar{b}_i X^i \cdot \bar{c}_j X^j +$ höhere Terme

$= \underbrace{\bar{b}_i \bar{c}_j}_{\neq 0} \cdot X^{i+j} + \ldots$

$\bar{g}\bar{h} = \bar{a}_n X^n$

$\Rightarrow i+j = n = m+\ell$

$\Rightarrow i = m, j = \ell$.

qed

Also ist $p \mid b_i$ für alle $0 \leq i < m$ und $p \mid c_j$ " " $0 \leq j < \ell$.

Insbesondere ist $p \mid b_0$ und $p \mid c_0$.

$\Rightarrow p^2 \mid b_0 c_0 = a_0$.

$\Rightarrow$ Widerspruch!

qed.

4.7.5 Beispiel: Das Polynom $X^n - 2 \in \mathbb{Z}[X]$ ist irreduzibel für jedes $n \geqslant 1$.

$p = 2$.

4.7.6 Beispiel: Für jedes $n \geqslant 1$ ist das Polynom $X^n + Y^n + Z^n \in \mathbb{C}[X, Y, Z]$ irreduzibel.

$\in \mathbb{C}[Y,Z][X]$

$f = X^n + (Y^n + Z^n) \cdot X^0$

normiert $\Rightarrow$ prim.

Bew.: es gibt $p \in \mathbb{C}[Y,Z]$ irred. mit $p \mid Y^n + Z^n$ und $p^2 \nmid Y^n + Z^n$.

$$Y^n + Z^n = \frac{Y^{2n} - Z^{2n}}{Y^n - Z^n} = \frac{\prod_{S^{2n}=1} (Y - SZ)}{\prod_{S^n=1} (Y - SZ)}$$

$$= \prod_{S \in \mathbb{C} \atop S^n = -1} (Y - SZ) .$$

↑ paarweise insbesondere irreduzibel in $\mathbb{C}[Y,Z]$.

Falls $p = Y - SZ$ hat's.

$Y^n + Z^n = \left[\left(\frac{Y}{Z} \right)^n + 1 \right] \cdot Z^n$.

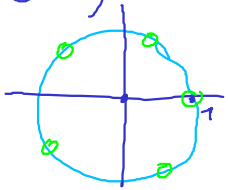
$X^n - 1$

4.7.7 Proposition: Für jede Primzahl p ist das *p-te Kreisteilungspolynom*

$$\Phi_p(X) := 1 + X + \ldots + X^{p-1} = \frac{X^p - 1}{X - 1}$$

in $\mathbb{Z}[X]$ irreduzibel.

$= \prod_{n=1}^{p-1} \left(X - e^{\frac{2\pi i n}{p}} \right)$



Bew.:

$$\Phi_p(Y+1) = \frac{(Y+1)^p - 1}{(Y+1) - 1} = \frac{1}{Y} \cdot \left(\sum_{n=0}^{p} \binom{p}{n} \cdot Y^n - 1 \right)$$

$$= \sum_{n=1}^{p} \binom{p}{n} \cdot Y^{n-1} = Y^{p-1} + pY^{p-2} + \ldots + \binom{p}{2} Y + p$$

$$\binom{p}{n} = \frac{p!}{n!(p-n)!} = \begin{cases} 1 & \text{für } n = 0, p \\ p \cdot a_p & 0 < n < p \\ & \text{für } a_p \in \mathbb{Z} \setminus p\mathbb{Z} . \end{cases}$$

Eisenstein mit $p = p$.

qed.

4.7.8 Satz: *(Kronecker)* Es existiert ein Algorithmus, der jedes Polynom in beliebig vielen Variablen über $\mathbb{Z}$ oder $\mathbb{Q}$ in irreduzible Faktoren zerlegt.

---

p prim,

$$\#\{f \in \mathbb{F}_p[X] \text{ normiert vom Grad } d, \text{ irreduzibel}\} = \frac{1}{d} \cdot \sum_{e \mid d} \mu\left(\frac{d}{e}\right) \cdot p^e$$

(Möbius)

$$\Rightarrow \text{Anteil} = \frac{1}{d \cdot p^d} \cdot \sum_{e \mid d} \mu\left(\frac{d}{e}\right) p^e = \frac{1}{d} \cdot \sum_{e \mid d} \mu\left(\frac{d}{e}\right) \cdot p^{e-d} = \frac{1}{d}\left(1 + O\left(p^{-d/2}\right)\right) \sim \frac{1}{d}.$$

$e \mid d, e < d \Rightarrow d - e \geq d/2$.