4.6 Polynomringe

4.6.1 Proposition: Für jeden Integritätsbereich R gilt $R[X]^\times = R^\times$.

Beweis, Für $f,g \in R[X] \setminus \{0\}$ ist $\deg(fg) = \deg(f) + \deg(g) \in \mathbb{Z}^{\geq 0}$
Gilt zusätzlich $fg = 1$, so muss $\deg(f) = 0$ sein, also $f \in R$ und $g \in R \Rightarrow f \in R^\times$. ged.

Sei nun R ein faktorieller Ring mit Quotientenkörper K. Für zwei Elemente $a, b \in K^\times$ schreiben wir $a \sim b$ genau dann, wenn $\frac{b}{a} \in R^\times$ ist. Für Elemente von $R \setminus \{0\}$ stimmt dies mit der Definition aus §4.1 überein.
Äquivalenzrelation.

4.6.2 Definition: (a) Der *Inhalt* eines Polynoms $f(X) = \sum_{i=0}^n a_i X^i \in R[X] \setminus \{0\}$ ist

$$I(f) \;:=\; \mathrm{ggT}(a_0, \ldots, a_n) \;\in\; R \setminus \{0\}.$$

Bsp.: $2X + 18 \in \mathbb{Z}[X]$
Inhalt ~ 2.

(b) Ein Polynom $f \in R[X] \setminus \{0\}$ mit $I(f) \sim 1$ heisst *primitiv*.

4.6.3 Lemma: Für alle $f \in R[X] \setminus \{0\}$ und $a \in R \setminus \{0\}$ gilt:

(a) $\frac{f}{I(f)}$ ist ein primitives Element von $R[X] \setminus \{0\}$.

(b) $I(af) \sim a \cdot I(f)$.

Beweis: (a) $f(X) = \sum a_i X^i$ mit $a_i \in R$
$b_i = I(f) = \mathrm{ggT}(a_0, \ldots, a_n)$
Schreibe $a_i = b c_i$ mit $c_i \in R$
$\Rightarrow b = \mathrm{ggT}(bc_0, \ldots, bc_n) \sim b \cdot \mathrm{ggT}(c_0, \ldots, c_n)$
$\Rightarrow 1 \sim \mathrm{ggT}(c_0, \ldots, c_n)$

$\Rightarrow \frac{f}{I(f)} = \sum c_i X^i \in R[X] \setminus \{0\}$
$I\left(\frac{f}{I(f)}\right) \sim 1$.

(b) $I(af) \sim \mathrm{ggT}(ab_0, \ldots, ab_n)$
$\sim a \cdot \mathrm{ggT}(b_0, \ldots, b_n) \sim a \cdot I(f)$

ged.

in 4.6.3.

4.6.4 Lemma: Der Inhalt setzt sich fort zu einer Abbildung $K[X] \setminus \{0\} \to K^\times$, $f \mapsto I(f)$ mit denselben Eigenschaften für alle $f \in K[X] \setminus \{0\}$ und $a \in K^\times$.

Bew.: Für $f \in K[K] \setminus \{0\}$ wähle $b_f \in R \setminus \{0\}$ mit $b_f f \in R[K] \setminus \{0\}$ Setze $I(f) := \frac{I(b_f f)}{b_f}$.
Nimm $b_f = 1$ falls $f \in R[K]$.

(a) $\frac{f}{I(f)} = \frac{b_f f}{I(b_f f)} \in R[K]$ primitiv nach 4.6.3(a).

(b) $I(af) \sim \frac{I(b_{af} \cdot af)}{b_{af}}$

$I(f) \sim \frac{I(b_{af} f)}{b_{af}}$

$I(f) \sim \frac{I(b_f f)}{b_f}$

Schreibe $a = \frac{c}{d}$ mit $c, d \in R \setminus \{0\}$.

$\Rightarrow I(af) \sim \frac{I(b_{af} \frac{c}{d} f)}{b_{af}} \sim \frac{I(b_{af} c f \frac{b_f}{d})}{b_{af} \cdot d b_f}$

$\sim I(f) \sim \frac{c\, I(b_f f)}{d\, b_f} \sim \frac{I(c b_f f)}{d b_f}$ q.e.d.

4.6.5 Lemma: Für jedes $f \in K[X] \setminus \{0\}$ gilt $f \in R[X] \Leftrightarrow I(f) \in R$.

Bew.: "$\Rightarrow$" ✓

"$\Leftarrow$" $\frac{f}{I(f)} \in R[K]$ $\rightsquigarrow f = \underbrace{I(f)}_{\in R} \cdot \frac{f}{I(f)} \in R[K]$ q.e.d.

4.6.6 Gauss-Lemma: Für alle $f, g \in K[X] \setminus \{0\}$ gilt $I(fg) \sim I(f) \cdot I(g)$.

Bsp.: $I\left(\frac{1}{5} + \frac{7}{2}X\right) = I\left(\frac{2+35X}{10}\right) \sim \frac{1}{10}$.

$I\left(\frac{1}{6} + 7X\right) = I\left(\frac{1+42X}{6}\right) \sim \frac{1}{6}$

$I\left(\frac{5}{7} - \frac{75}{8}X^2\right) = I\left(\frac{5 \cdot (8 - 105X^2)}{7 \cdot 8}\right) \sim \frac{5}{7 \cdot 8}$.

Beweis 4.66.: Zu zeigen: $\frac{I(fg)}{I(f)\cdot I(g)} \sim 1$

Äquivalent zu $I\left(\frac{f}{I(f)}\cdot\frac{g}{I(g)}\right) \sim 1$.

Dabei ist $\frac{f}{I(f)}, \frac{g}{I(g)} \in R[X]$ primitiv.

Gauß: $f, g \in R[X]$ primitiv $\Rightarrow fg$ primitiv.

$\sigma \subset R$

$(R/\sigma)[X] \cong R[X]/\sigma\cdot R[X]$.

Wegen $fg \in R[X]$ ist dann $I(fg) \in R$.

Wenn $I(fg) \notin R^\times$ ist, so $\exists$ primelement $p \in R$ mit $p \mid I(fg)$.

Dann ist $R/(p)$ ein Integritätsbereich.

und $R/(p)[X] \cong R[X]/p\cdot R[X]$. = Integritätsbereich.

f, g primitiv $\Rightarrow p \nmid f, g$

$\Rightarrow [f], [g] \neq 0$ in $R/(p)[X]$.

$\Rightarrow [fg] = [f]\cdot[g] \neq 0$ in $R/(p)[X]$.

$\Rightarrow p \nmid fg$ in $R[X]$

$\Rightarrow p \nmid I(fg)$ $\rightarrow$ Widerspruch! qed.

4.6.7 Satz: (a) Jedes Primelement von R ist ein Primelement von $R[X]$. Grad 0

(b) Jedes primitive Polynom in $R[X] \setminus \{0\}$, das in $K[X]$ prim ist, ist prim in $R[X]$. Grad > 0.

(c) Jedes Primelement von $R[X]$ ist eines der obigen.

(d) Der Ring $R[X]$ ist faktoriell.

Beweis: (a) $p \in R$ prim. $\Rightarrow p \neq 0$ und R/pR Integritätsbereich
$\Rightarrow R[X]/pR[X] \cong (R/pR)[X]$ Integritätsbereich $\Rightarrow p$ prim in $R[X]$.

(b) Sei $q \in R[X]$ primitiv und in $K[X]$ irred. $\Rightarrow q \neq 0$, $q \notin K[X]^\times \Rightarrow q \notin R[X]^\times$.
Seien $f, g \in R[X]$ mit $q \mid f \cdot g$ in $R[X]$. Ist $f = 0$, dann gilt $q \mid f$ in $R[X]$ ✓
$\ldots$ $g = 0$ $\ldots$ $q \mid g$ $\ldots$ ✓
Sei also $f, g \neq 0$. d.h. $\exists h \in R[X]: qh = fg \Rightarrow q \mid fg$ in $K[X]$.
q in $K[X]$ irred. $\Rightarrow q \mid f$ oder $q \mid g$ in $K[X]$. Sei o.B.d.A. $q \mid f$, und $f = k \cdot q$ für $k \in K[X]$.
$f \neq 0 \Rightarrow k \neq 0$, und $I(f) = I(kq) \sim I(k) \cdot I(q) \Rightarrow R \ni I(f) \sim I(k) \Rightarrow k \in R[X]$.
($I(q) \sim 1$ da q primitiv.)
$\Rightarrow q \mid f$ in $R[X]$. Also ist q prim in $R[X]$.

$q_i' := \frac{q_i}{I(q_i)}$

(d) Sei $f \in R[X] \setminus \{0\}$. $K[X]$ Hauptidealring $\Rightarrow$ faktoriell.
Schreibe $f = a \cdot q_1 \cdots q_n$ für $q_i \in K[X]$ prim und $a \in K^\times$.
$\Rightarrow f = \left(a \cdot \prod_{i=1}^{n} I(q_i)\right) \cdot \frac{q_1}{I(q_1)} \cdots \frac{q_n}{I(q_n)}$
$b \in K^\times$ — erfüllt (b)

$R \ni I(f) \sim b \cdot I\left(\frac{q_1}{I(q_1)}\right) \cdots \sim b$.
$\Rightarrow b \in R \setminus \{0\}$.
Schreibe $b = u \cdot p_1 \cdots p_m$ für $u \in R^\times$, $p_i \in R$ prim.
(a)
$\Rightarrow f = u p_1 \cdots p_m \cdot q_1' \cdots q_n'$ in $R[X]$.

(c) $f \in R[X]$ prim $\overset{(d)}{\Rightarrow}$ $f = u p_1 \cdots u q_l'$ ged.

4.6.8 Folge: Ein primitives Polynom in $R[X]$ ist irreduzibel in $R[X]$ genau dann, wenn es irreduzibel in $K[X]$ ist. (vom Grad >0)

4.6.9 Folge: Für jedes normierte Polynom in $R[X]$ liegt jede Nullstelle in K schon in R.

Beweis: $f \in R[X]$ normiert $\Rightarrow I(f) \sim 1$.
$a, b \in R^\times$, $f(\frac{a}{b}) = 0 \Rightarrow bX - a$ Teiler von f in $K[X]$. } $\Rightarrow bX - a$ Teiler in f in $R[X]$.
$\gcd(a,b) \sim 1$ ($\Rightarrow$ primitiv $\Rightarrow$ prim.) f normiert $\Rightarrow b \mid 1 \Rightarrow b \sim 1$.
$\Rightarrow \frac{a}{b} \in R$.

4.6.10 Satz: Für jeden faktoriellen Ring R und jedes $n \geqslant 0$ ist $R[X_1, \ldots, X_n]$ faktoriell. Insbesondere ist für jeden Körper K der Ring $K[X_1, \ldots, X_n]$ faktoriell.

Beweis: Induktion über n: $R[X_1, \ldots, X_n] \cong R[X_1, \ldots, X_{n-1}][X_n]$. ged.

4.6.11 Beispiel: Für jeden Körper K ist $X^3 - Y^5$ irreduzibel in $K[X,Y]$.

Beweis: $f := X^3 - Y^5 \in K[Y][X]$
In $K(Y)[X]$ ist f reduzibel g.d.w. es eine Nullstelle hat. (faktoriell)
Eine Nullstelle ist ein $g \in K(Y)$ mit $g^3 = Y^5$. Da $K(Y) = \mathrm{Quot}(K[Y])$, müsste $g = u \prod_{i=1}^{n} p_i^{\nu_i}$ (eindeutig)
mit $u \in K[Y]^\times$, $p_i \in K[Y]$ und $\nu_i \in \mathbb{Z}$ $\Rightarrow$ $Y^5 = u^3 \prod_{i=1}^{n} p_i^{3\nu_i}$ $\Rightarrow$ Widerspruch, da kein $3\nu_i = 5$ sein kann.

Ansonsten ist $I(f) \sim ggT(1, -Y^5) \sim 1$ in $K[Y]$ $\Rightarrow$ f primitiv

$\Rightarrow$ f prim in $K[X][Y]$ ✓. q.e.d.

Bsp.: $f(X) = 2 + 16X + 70X^2$

$= 2 \cdot (1 + 8X + 35X^2)$

$\frac{-8 \pm \sqrt{64 - 140}}{2} \notin \mathbb{Q}$.

irred. in $\mathbb{Z}[X]$ (↑ zu 2)

primitiv (↑ zu $(1 + 8X + 35X^2)$), keine Nullstelle in $\mathbb{Q}$.

Primfaktorzerlegung von f.