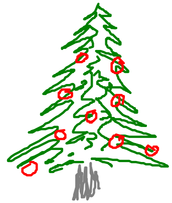
7.2 Grad eines Polynoms



Definition: Der *Grad* eines Polynom $F(X) = \boxed{\sum'_{i \geqslant 0} a_i X^i}$ über einem Körper K ist

$$\deg(F) := \begin{cases} \max\{i \geqslant 0 \mid a_i \neq 0\} & \text{falls } F \neq 0, \\ -\infty & \text{falls } F = 0. \end{cases}$$

Ein Polynom vom Grad $\leqslant 0$ heisst *konstant*, eines vom Grad > 0 heisst *nichtkonstant.* Ein Polynom vom Grad $\leqslant 1$ heisst *linear*, eines vom Grad $\leqslant 2$ *quadratisch*, eines vom Grad $\leqslant 3$ *kubisch.* Ein Polynom vom Grad $n \geqslant 0$ mit höchstem Koeffizienten $a_n = 1$ heisst *normiert.* Der Koeffizient a_0 von $X^0 = 1$ in F heisst der *konstante Koeffizient von F.*

Bsp.: $F = 15 = 15 \cdot X^0$ konstant
$F = aX + b$ linear
$F = X^2 + 1$ quadratisch.

Proposition: Für je zwei Polynome F und G über K und jedes $\lambda \in K^\times$ gilt:

$$\begin{aligned} \deg(F+G) &\leqslant \max\{\deg(F), \deg(G)\}, \\ \deg(F \cdot G) &= \deg(F) + \deg(G), \\ \deg(\lambda \cdot F) &= \deg(F). \end{aligned}$$

Beweis:

$F = 0 \Rightarrow F \cdot G = 0$

$\deg(FG) = -\infty = -\infty + \deg(G)$

Analog wenn $G = 0$.

Sei jetzt $F = \sum_{i=0}^{m} a_i X^i$ mit $a_m \neq 0$ und $G = \sum_{j=0}^{n} b_j X^j$ mit $b_n \neq 0$. $\Rightarrow$ $\deg(F) = m$, $\deg(G) = n$.

$\Rightarrow \quad F + G = \sum_{i \geq 0} (a_i + b_i) X^i \quad$ mit $\quad a_i = b_i = 0$ für $i > \max\{m, n\}$.

$\Rightarrow \quad a_i + b_i = 0$.

$\Rightarrow \quad \deg(F + G) \leq \max\{m, n\}$.

$$F \cdot G = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j \cdot X^{i+j} = \underbrace{a_m b_n}_{\neq 0} X^{m+n} + (\text{kleinere Terme})$$

$\Rightarrow \deg(F \cdot G) = m + n$.

$$\lambda F = \sum_{i=0}^{m} (\lambda a_i) X^i$$ mit $\lambda a_m \neq 0 \Rightarrow \deg(\lambda F) = m$.

q.e.d.

Proposition: Für je drei Polynome F, G, H über K mit $H \neq 0$ gilt:

$$F \cdot G = 0 \;\Leftrightarrow\; (F = 0) \vee (G = 0), \qquad \checkmark$$
$$FH = GH \;\Leftrightarrow\; F = G.$$

Bew.: $F = 0$ oder $G = 0 \Rightarrow F \cdot G = 0$

$F \neq 0$ und $G \neq 0 \Rightarrow \deg(F), \deg(G) \geq 0 \Rightarrow \deg(FG) \geq 0 \Rightarrow FG \neq 0$.

$F = G \Rightarrow FH = GH$

$FH = GH \Rightarrow (F - G)H = FH - GH = 0 \Rightarrow F - G = 0 \Rightarrow F = G$. qed.

Proposition: Der Ring $K[X]$ ist ein Vektorraum über K, isomorph zu dem Folgenraum F_0 aus §4.2. Eine Basis von $K[X]$ ist $\{X^i \mid i \geqslant 0\}$. Die Polynome vom Grad $\leqslant n$ bilden einen Unterraum der Dimension $n+1$ mit Basis $\{X^i \mid 0 \leqslant i \leqslant n\}$.

$$\sum_{i \geq 0}{}' a_i X^i \longleftrightarrow (a_i)_{i \geq 0} \in K^{(\mathbb{Z}^{\geq 0})}$$

7.3 Nullstellen

Satz: Für je zwei Polynome F und $G \in K[X]$ mit $G \neq 0$ existieren eindeutige Polynome Q und $R \in K[X]$ mit $\deg(R) < \deg(G)$ und $F = Q \cdot G + R$.

Diese *Polynomdivision mit Rest* erfolgt von Hand wie die Division ganzer Zahlen.

Beweis: Sei $F = QG + R = Q'G + R'$ für $Q, Q', R, R' \in K[X]$ und $\deg(R), \deg(R') < \deg(G)$.

$\Rightarrow (Q - Q')G = R' - R$ mit $\deg(R' - R) < \deg(G)$.

$\deg(R' - R) = \deg(G) + \deg(Q - Q')$

$\Rightarrow \deg(Q - Q') < 0 \Rightarrow Q - Q' = 0 \Rightarrow Q = Q'$.

$\Rightarrow R = R'$.

$\Rightarrow$ Eindeutigkeit.

Existenz: Induktion über $\deg(F)$. Sei $G = \sum_{i=0}^{m} b_i X^i$ mit $b_m \neq 0$.

Falls $\deg(F) < m \Rightarrow$ Setze $Q := 0$ und $R := F \Rightarrow$ OKAY!

Sonst schreibe $F = \sum_{i=0}^{n} a_i X^i$ mit $a_n \neq 0$ und $n \geq m$.

Setze $F' := F - \frac{a_n}{b_m} \cdot X^{n-m} \cdot G = \left(a_n X^n + \text{kleinere Terme}\right) - \underbrace{\frac{a_n}{b_m} X^{n-m} \cdot \left(b_m X^m + \ldots\right)}_{\left(a_n X^n + \text{kleinere Terme}\right)}$

$\Rightarrow \deg(F') < n$. Nach IV existieren $Q', R' \in K[X]$

mit $\deg(R') < m$ und $F' = Q'G + R' \Rightarrow F = \left(Q' + \frac{a_n}{b_m} X^{n-m}\right) \cdot G + R'$ qed.

Sei nun $F \in K[X]$ beliebig.

Definition: Ein Element $\lambda \in K$ mit $F(\lambda) = 0$ heisst eine *Nullstelle von F.*

Proposition: Ein Element $\lambda \in K$ ist eine Nullstelle von F genau dann, wenn ein Polynom G über K existiert mit $F(X) = (X - \lambda) \cdot G(X)$.

Bew.: Schreibe $F(X) = Q(X) \cdot (X - \lambda) + a$ mit $Q \in K[X]$ und $a \in K$.

Dann ist $F(\lambda) = Q(\lambda) \cdot (\lambda - \lambda) + a = a$.

$\Rightarrow$ λ Nullstelle gdw. $a = 0$.

qed.

Definition: Für jedes $\lambda \in K$ heisst

$$\mu_\lambda \; := \; \sup \left\{ m \geqslant 0 \;\middle|\; \exists\, G \in K[X] \colon F(X) = (X - \lambda)^m \cdot G(X) \right\} \; \in \; \mathbb{Z}^{\geqslant 0} \cup \{\infty\}$$

die *Nullstellenordnung von F in λ.* Ist $\mu_\lambda > 0$, so heisst λ eine *Nullstelle der Vielfachheit* oder *Multiplizität μ_λ von F.*

Bemerkung: Es gilt $\mu_\lambda \leqslant \deg(F)$ falls $F \neq 0$ ist, und $\mu_\lambda = \infty$ falls $F = 0$ ist.

≥ 0 falls $F \neq 0$.

$\deg(F) = \deg((X-\lambda)^m) + \deg(G) = m + \deg(G) \geq m.$

Satz: Jedes von Null verschiedene Polynom F über K lässt sich schreiben in der Form

$$F(X) \;=\; (X-\lambda_1)^{\mu_1}\cdots(X-\lambda_r)^{\mu_r}\cdot G(X)$$

mit geeigneten $r \geqslant 0$ und $\mu_i \geqslant 1$ und paarweise verschiedenen $\lambda_i \in K$, sowie einem Polynom G über K ohne Nullstellen in K. Dabei sind $\lambda_1, \ldots, \lambda_r$ genau die Nullstellen von F in K und $\mu_1, \ldots, \mu_r$ deren Nullstellenordnungen. Ausserdem sind r und G, sowie die Paare (λ_i, μ_i) bis auf Permutation der i, eindeutig bestimmt.

Definition: Ist in der obigen Zerlegung G eine Konstante in $K^\times$, so sagen wir, dass *F über K in Linearfaktoren zerfällt.*

Folge: Für jedes von Null verschiedene Polynom F über K ist die Anzahl der Nullstellen von F in K, mit Vielfachheiten gezählt, kleiner oder gleich $\deg(F)$.

Bew.: $\deg(F) = \mu_1 + \ldots + \mu_r + \deg(G) \geq \mu_1 + \ldots + \mu_r$ q.e.d.

Proposition: Ist K ein unendlicher Körper, so ist jedes Polynom F über K durch die Polynomfunktion $K \to K$, $x \mapsto F(x)$ eindeutig bestimmt.

Bew.: Seien $F, G \in K[X]$ mit $F(x) = G(x)$ für alle $x \in K$.
Dann gilt $\forall x \in X: (F-G)(x) = 0$.
$\Rightarrow F-G$ hat alle $x \in K$ als Nullstellen.
$|K| = \infty \Rightarrow F-G = 0 \Rightarrow F = G$. qed.

Satz: Für jedes normierte Polynom $F \in \mathbb{Z}[X]$ gilt: Jede Nullstelle von F in $\mathbb{Q}$ liegt schon in $\mathbb{Z}$ und teilt den konstanten Koeffizienten von F.

Folge: Es gibt einen effektiven Algorithmus, der für jedes Polynom in $\mathbb{Q}[X]$ alle Nullstellen in $\mathbb{Q}$ bestimmt.

Beweis: $F = \sum_{i=0}^{n} a_i X^i$ mit $a_i \in \mathbb{Z}$ und $a_n = 1$.

Sei $\lambda = \frac{b}{c}$ mit $b, c \in \mathbb{Z}$, $c > 0$ teilerfremd, $F(\lambda) = 0$.

$$0 = c^n \cdot F(\lambda) = \sum_{i=0}^{n} a_i c^n \cdot \frac{b^i}{c^i} = \sum_{i=0}^{n} a_i \cdot b^i \cdot c^{n-i} = a_n b^n + \sum_{i=0}^{n-1} (a_i b^i c^{n-i})$$
$$= b^n + \left(\sum_{i=0}^{n-1} a_i b^i c^{n-i-1}\right) c$$

$\Rightarrow c \mid b^n$. Da b, c teilerfremd sind, folgt $c = 1$.

$$0 = \sum_{i=0}^{n} a_i b^i = a_0 + \left(\sum_{i=1}^{n} a_i b^{i-1}\right) b \Rightarrow b \mid a_0.$$

qed.

Algorithmus: $F = \sum_{i=0}^{n} a_i X^i$ OBdA normiert.

$a_i \in \mathbb{Q}$, Wähle $b \in \mathbb{Z}^{>0}$ mit $\forall i: b a_i \in \mathbb{Z}$

Ersetze F durch: $b^n \cdot F\left(\frac{X}{b}\right) = \sum_{i=0}^{n} a_i \cdot b^n \cdot \frac{X^i}{b^i} = \sum_{i=0}^{n} \underbrace{a_i b^{n-i}}_{\in \mathbb{Z}} X^i \in \mathbb{Z}[X]$ normiert.

$F \in \mathbb{Z}[X]$ normiert, $F(0) = 0 \leadsto$ Schreibe $F(X) = (X-0) \cdot G(X)$

Sonst teste alle Teiler von $F(0)$.

Bsp.: $\left.\begin{array}{l} F = X^3 - 7X - 2 \\ \text{Teste } \pm 1, \pm 2 \end{array}\right\} \Rightarrow$ keine Nullstellen in $\mathbb{Q}$.

7.4 Algebraisch abgeschlossene Körper

Satz: Für jeden Körper K sind äquivalent:

(a) Jedes nichtkonstante Polynom über K besitzt eine Nullstelle in K.

(b) Jedes Polynom über K zerfällt in Linearfaktoren über K.

(c) Jedes Polynom vom Grad $n \geqslant 0$ über K besitzt, mit Vielfachheiten gezählt, genau n Nullstellen in K.

Definition: Ein Körper mit den obigen Eigenschaften heisst *algebraisch abgeschlossen.*

Bew.: Sei $F \neq 0$. Schreibe $F(X) = (X-\lambda_1)^{\mu_1} \cdots (X-\lambda_r)^{\mu_r} \cdot G(X)$

für G ohne Nullstellen.

(a) $\Rightarrow$ (b): Dann ist G konstant und $G \neq 0 \Rightarrow \deg(G) = 0$

(a) $\Rightarrow$ (c): $r_1 + \ldots + r_r = \mu_1 + \ldots + \mu_r + \deg(G) = \deg(F)$.

(b) $\Rightarrow$ (a) dann ist $r > 0$

(c) $\Rightarrow$ (a) $n > 0 \Rightarrow$ existiert Nullstelle. qed.

Beispiel: Ist K ein endlicher Körper, so ist $F(X) := 1 + \prod_{\lambda \in K}(X - \lambda)$ ein Polynom vom Grad $|K| > 0$ über K ohne Nullstellen in K. Also ist K nicht algebraisch abgeschlossen.

Dann ist $\forall \lambda \in K : F(\lambda) = 1$.

Satz: Jeder Körper ist in einem algebraisch abgeschlossenen Körper enthalten.

(Beweis in der Vorlesung Algebra I-II.)

Fundamentalsatz für die Algebra: Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Beispiel: Der Körper $\mathbb{R}$ ist nicht algebraisch abgeschlossen. X^2+1 hat keine Nullstellen in $\mathbb{R}$.

Proposition: Für jedes Polynom F über $\mathbb{R}$ und jede Nullstelle $\lambda \in \mathbb{C}$ von F ist die komplex Konjugierte $\overline{\lambda}$ eine Nullstelle von F derselben Multiplizität wie λ.

Bew.: $F(X) = \sum_{k \geq 0}' a_k X^k$ mit $a_k \in \mathbb{R}$ und $F(\lambda) = 0 \Rightarrow F(\overline{\lambda}) = \sum_k' a_k \overline{\lambda}^k = \overline{\left(\sum_k' a_k \lambda^k\right)} = \overline{0} = 0$. qed

Satz: Jedes Polynom über $\mathbb{R}$ ist ein Produkt von Polynomen vom Grad $\leqslant 2$ über $\mathbb{R}$.

Bew.: Induktion über $\deg(F)$; $\lambda \in \mathbb{C}$ Nullstelle von F.

$\lambda \in \mathbb{R} \Rightarrow F(X) = (X-\lambda) \cdot G(X)$

$\lambda \notin \mathbb{R} \Rightarrow F(X) = \underbrace{(X-\lambda)(X-\overline{\lambda})}_{X^2-(\lambda+\overline{\lambda})X+\lambda\overline{\lambda} \in \mathbb{R}[X]} \cdot G(X) + R(X)$ mit $\deg(R) < 2$ und $R \in \mathbb{R}[X]$.

Dann ist $R(\lambda) = R(\overline{\lambda}) = 0$
$\Rightarrow R = 0$. qed