1.4 Polynome

a) Wurzeln

<u>Def.:</u> Seien $n \geq 2$ ($n \in \mathbb{N}$) fest, K ein Körper und $a \in K$. Eine Zahl $b \in K$ heißt n-te Wurzel von a, falls $b^n = a$.

<u>Bsp.:</u>

(1) Wegen $1^n = 1$ in jedem Körper hat 1 mindestens eine n-te Wurzel.

(2) Für n gerade gilt $(-1)^n = 1$. Insbesondere sind ± 1 stets Quadratwurzeln ($n=2$) von 1.

(3) Sei $K = \mathbb{Q}$. Dann hat 2 keine n-ten Wurzeln in $\mathbb{Q}$. ($\sqrt{2}$ ist irrational).

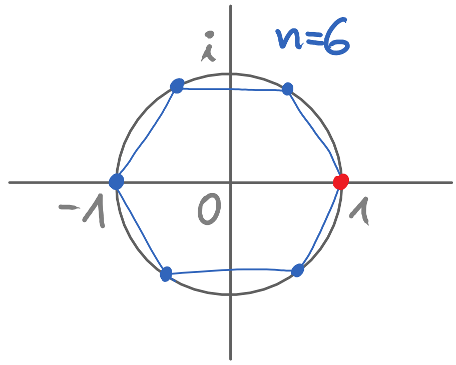
(4) Sei $K = \mathbb{R}$. Wegen $b^2 \geq 0$ für alle $b \in \mathbb{R}$ haben negative reelle Zahlen ($a<0$) keine Quadratwurzeln (ebenso für n gerade).
Zu $a \geq 0$ gibt es genau ein $b \geq 0$, so daß $b^n = a$. Die Zahl b wird <u>die</u> n-te Wurzel von a genannt und mit $\sqrt[n]{a}$ oder $a^{1/n}$ bezeichnet.

Die Abbildung $\sqrt[n]{\cdot} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $a \mapsto \sqrt[n]{a}$ ist monoton, d.h. $a < b \Rightarrow \sqrt[n]{a} < \sqrt[n]{b}$.

(5) Sei $K=\mathbb{C}$. Dann hat $\zeta^n=1$ genau n Lösungen:

$\zeta_k := e^{2\pi i k/n}$, $\quad k=0,1,\dots,n-1$.

Sie heißen Einheitswurzeln, liegen auf dem Einheitskreis $|z|=1$ und bilden ein regelmäßiges n-Eck mit 1 als Ecke:



(6) Für $a=re^{i\varphi}\in\mathbb{C}\setminus\{0\}$ hat $z^n=a$ genau n Lösungen:

$z_k = r^{1/n} e^{i\varphi/n}\zeta_k$, $\quad k=0,\dots,n-1$.

Bsp.: $\quad a=-1=e^{i\pi}$, $n=2$.

Dann ist $z_0=e^{i\pi/2}=i$ und $z_1=e^{i3\pi/2}=-i$, also hat -1 in $\mathbb{C}$ die Quadratwurzeln $\pm i$.

Die Wurzeln von $a\in\mathbb{C}\setminus\{0\}$ liegen auf einem Kreis mit Radius $|a|^{1/n}$ und bilden ebenfalls ein regelmäßiges n-Eck mit $|a|^{1/n}e^{i\varphi/n}$ als Ecke.

(7) Seien ζ_k, $k=0,1,\dots,n-1$, die n-ten Einheitswurzeln. Dann gilt: $\displaystyle\sum_{k=0}^{n-1}\zeta_k=0$ für $n\geq 2$.

Bew.: $\zeta_k=z^k$ mit $z=e^{2\pi i/n}$ $\Rightarrow$ $z\neq 1$ und $z^n=1$.

$(1-z)(1+z+\dots+z^{n-1}) = 1-z^n = 0$ $\quad\square$

b) Polynomringe

<u>Def.:</u> Sei K ein Körper und t eine Variable. Ein Polynom über K (d.h. mit Koeffizienten in K) ist ein Ausdruck der Form $P(t) = a_0 + a_1 t + \ldots + a_n t^n$, wobei $a_0, \ldots, a_n \in K$ und $n = 0, 1, 2, \ldots$ Das Polynom P ist eindeutig durch die Folge $(a_0, \ldots, a_n)$ charakterisiert. Der Grad von P ist definiert als

$$\deg P = \max\{\nu \in \mathbb{N}_0 \mid a_\nu \neq 0\};$$

für das Nullpolynom $P = 0$ setzt man $\deg P = \infty$.
Die Menge der Polynome über K wird mit $K[t]$ bezeichnet.

<u>Bsp.:</u> Polynome vom Grad n

i) $n=0$: Konstantes Polynom, $P = 1$
ii) $n=1$: lineares Polynom, $Q = 2t - 3$
iii) $n=2$: quadratisches Polynom, $R = t^2 + 1$

<u>Bem.:</u>

(1) Addition von $P, Q \in K[t]$:

$$P = a_0 + a_1 t + \ldots + a_n t^n, \quad Q = b_0 + b_1 t + \ldots + b_m t^m$$

Sei $m = n$ (sonst mit $b_{m+1} = \ldots = b_n = 0$ auffüllen). Dann:

$$P + Q := (a_0 + b_0) + (a_1 + b_1) t + \ldots + (a_n + b_n) t^n.$$

(2) Multiplikation von $P, Q \in K[t]$:

Ausmultiplizieren (Distributivgesetz)

$$P \cdot Q := c_0 + c_1 t + \ldots + c_{n+m} t^{n+m}, \quad c_k = \sum_{i+j=k} a_i b_j$$

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

$$\vdots$$

$$c_{n+m} = a_n b_m$$

Bsp.: $P = t^2 + 1$, $Q = 2t - 3$

$$P + Q = t^2 + 2t - 2$$

$$P \cdot Q = 2t^3 - 3t^2 + 2t - 3$$

Es gilt: $\deg(P \cdot Q) = \deg P + \deg Q$

Bew.: $a_n b_m \neq 0$ falls $a_n, b_m \neq 0$. $\square$

(3) $K[t]$ ist kein Körper, da keine Division erklärt werden kann. Aber $+$ und $\cdot$ sind kommutativ und assoziativ. $\Rightarrow$ $K[t]$ ist ein kommutativer Ring.

Erinnerung: Division mit Rest

Seien $a, b \in \mathbb{Z}$ und $b \neq 0$. Dann ist $a = b \cdot q + r$ mit eindeutig bestimmten $q, r \in \mathbb{Z}$, wobei $0 \leq r < |b|$.

Bsp.: $a = 23$, $b = 3$. Dann ist $23 = 3 \cdot 7 + 2$

bzw. $$\frac{23}{3} = 7 + \frac{2}{3}.$$

Satz: (Polynomdivision)

Zu $P, Q \in K[t]$ gibt es eindeutig bestimmte Polynome $q, r \in K[t]$, so daß

(i) $P = Q \cdot q + r$,

(ii) $\deg r < \deg Q$, falls $r \neq 0$.

Beweis: s. Fischer, §1.3.7 (S.59)

Wähle $q \in K[t]$, so daß $\deg(P - Q \cdot q)$ minimal wird und setze $r = P - Q \cdot q$. (Sonderfall: $P = Q \cdot q$)

Bsp.: $P = t^2 + 1$, $Q = 2t - 1$

$$(t^2 \quad + 1) : (2t - 1) = \underbrace{\frac{1}{2}t + \frac{1}{4}}_{q} + \underbrace{\frac{5}{8t - 4}}_{\frac{5/4}{Q}}$$

$$\begin{array}{l} t^2 - \frac{1}{2}t \\ \hline \quad \frac{1}{2}t + 1 \\ \quad \frac{1}{2}t - \frac{1}{4} \\ \hline \qquad \frac{5}{4} =: r \end{array}$$

$\deg(r) = 0 < \deg(Q) = 1$

c) Nullstellen

Def.: Sei $P \in K[t]$ ein Polynom. Dann heißt $\lambda \in K$ Nullstelle von P, falls $P(\lambda) = 0$.

Bsp.: $P = t^2 + 1$. Als Element von $\mathbb{R}[t]$ hat P keine Nullstellen, da $P(\lambda) \geq 1$ für alle $\lambda \in \mathbb{R}$.
Aber $P \in \mathbb{C}[t]$ hat 2 Nullstellen:
$$P(t) = (t-i)(t+i) \Rightarrow \lambda_{1/2} = \pm i.$$

Lemma: (Abspaltung einer Nullstelle)
Sei $\lambda \in K$ eine Nullstelle von $P \in K[t]$. Dann gibt es genau ein $Q \in K[t]$ mit
(i) $P = (t-\lambda) \cdot Q$,
(ii) $\deg Q = (\deg P) - 1$.

Bew.: dividiere P mit Rest durch $(t-\lambda)$, also gibt es eindeutig bestimmte $Q, r \in K[t]$ mit
$$P = (t-\lambda) \cdot Q + r \quad \text{und} \quad \deg r < \deg(t-\lambda) = 1.$$
Also ist $r = a_0$ mit $a_0 \in K$. Wegen $P(\lambda) = 0$ gilt:
$$0 = (\lambda - \lambda) \cdot Q(\lambda) + r = 0 + a_0 \Rightarrow r = 0.$$
Teil (ii) folgt aus $\deg P = \deg(t-\lambda) + \deg Q$. $\square$

→ direkte Folge, „Zugabe"

Korollar 1: Seien K ein beliebiger Körper und $P \in K[t]$ ein Polynom vom Grad $n < \infty$. Dann hat P höchstens n Nullstellen.

Bew.: Induktion in n. Setze $\mathcal{N} := \{\lambda \in K \mid P(\lambda) = 0\}$.

- Induktionsanfang: Für $\deg P = 0$ ist $P = a_0 \neq 0$ konstant. $\Rightarrow$ $\mathcal{N} = \emptyset$, wie behauptet.
- Induktionsannahme: Sei $n = \deg P \geq 1$, und sei die Aussage für alle $Q \in K[t]$ mit $\deg Q \leq n-1$ bewiesen.
- Induktionsschritt: Wenn $\mathcal{N} = \emptyset$, dann ist die Aussage richtig. Sei $\lambda \in \mathcal{N}$, dann gibt es ein $Q \in K[t]$ mit $\deg Q = n-1$, so daß $P = (t-\lambda)\cdot Q$.

→ aber evtl. nicht alle: $Q(\lambda) = 0$.

$\mathcal{N} \setminus \{\lambda\}$ sind auch Nullstellen von Q.

Anzahl der Elemente

Induktionsannahme $\Rightarrow$ $\ell := |\mathcal{N} \setminus \{\lambda\}| \leq n-1$

Also besitzt P höchstens $\ell + 1 \leq n$ Nullstellen. □

Korollar 2: Für Polynome $P, Q \in K[t]$ sind folgende Aussagen äquivalent:

(i) $P(\lambda) = Q(\lambda)$ für unendlich viele $\lambda \in K$.

(ii) P und Q haben dieselben Koeffizienten ($P = Q$).

<u>Bew.:</u> (ii) $\Rightarrow$ (i) ist klar. Sei $r := P - Q$. Wegen (i) ist $r(\lambda) = 0$ für alle $\lambda \in K$, also hat r unendlich viele Nullstellen. Nach Korollar 1 ist $\operatorname{grad} r = \infty$ bzw. $r = 0$, d. h. $P = Q$. $\square$

<u>Bem.:</u>

(1) Koeffizientenvergleich: $P, Q \in \mathbb{R}[t]$ der Form $P = t^2 + at - 1$ und $Q = ct^3 + t^2 + 3t + b$.
$P(\lambda) = Q(\lambda)$ für alle $\lambda \in \mathbb{R} \Leftrightarrow a = 3,\ b = -1,\ c = 0$.

(2) Ist K ein unendlicher Körper, z.B. $\mathbb{R}$ oder $\mathbb{C}$, dann können wir ein Polynom $P \in K[t]$ mit der Abbildung $K \to K,\ t \mapsto P(t)$, identifizieren.