Die elementarsymmetrischen Polynome

Definition (24.1)

Sei R ein Ring, $n \in \mathbb{N}$ und $R[x_1, ..., x_n]$ der Polynomring über R in n Variablen. Dann bezeichnet man für $1 \leq k \leq n$ das Polynom

$$\varepsilon_k = \sum_{1 \leq i_1 < ... < i_k \leq n} \prod_{j=1}^{k} x_{i_j}$$

als k-tes elementarsymmetrisches Polynom in $R[x_1, ..., x_n]$.

Bedeutung der elementarsymmetrischen Polynome

Satz (24.2)

Sei R ein beliebiger Ring, $n \in \mathbb{N}$ und $f \in R[x]$ ein normiertes Polynom n-ten Grades, $f = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$. Wir nehmen an, dass f über R in Linearfaktoren zerfällt, also

$$f \quad = \quad (x - \alpha_1) \cdot ... \cdot (x - \alpha_n)$$

mit geeigneten $\alpha_1, ..., \alpha_n \in R$ erfüllt ist. Dann gilt $a_k = (-1)^{n-k}\varepsilon_{n-k}(\alpha_1, ..., \alpha_n)$ für $0 \leq k < n$.

Symmetrische Polynome

Definition (24.3)

Sei R ein beliebiger Ring und $n \in \mathbb{N}$. Wir bezeichnen ein Polynom $f \in R[x_1, ..., x_n]$ als symmetrisch, wenn $\sigma(f) = f$ für alle $\sigma \in S_n$ erfüllt ist.

Def lexikographische Anordnung der Monome des Polynomrings $R[x_1, \dots, x_n]$

Für alle Tupel $(c_1, \dots, c_n) \in \mathbb{N}_0^n$ wird $c_1 + \dots + c_n$ der **Totalgrad** des Monoms $x_1^{c_1} \cdot x_2^{c_2} \cdot \dots \cdot x_n^{c_n}$ genannt.

Notation: $\operatorname{grad}(x_1^{c_1} \cdot \dots \cdot x_n^{c_n}) = c_1 + \dots + c_n$

Auf der Menge der Terme mit gleichem Totalgrad definiere eine Anordnung $\prec$ durch

$$a\, x_1^{c_1} \cdot \dots \cdot x_n^{c_n} \overset{(*)}{\prec} b\, x_1^{d_1} \cdot \dots \cdot x_n^{d_n} \iff$$

$\exists\, k \in \{1, \dots, n\}$ mit $c_l = d_l$ für $1 \le l < k$ und $c_k < d_k$

$\exists k \in \{1,\dots,n\}$ mit $c_l = d_l$ für $1 \le l < k$ und $c_k < d_k$

Auf der Gesamtheit aller Terme bzw. Monome definiere

$$t \prec t' \iff \operatorname{grad}(t) < \operatorname{grad}(t') \quad \underline{\text{oder}}$$

$$\left(\operatorname{grad}(t) = \operatorname{grad}(t') \text{ und } t \prec t' \text{ bzgl } (*)\right)$$

<u>Beispiel</u> Die kleinsten Monome in $\mathbb{R}[x_1, x_2, x_3]$ bzgl $\prec$

$$1 \prec x_3 \prec x_2 \prec x_1 \prec x_3^2 \prec x_2x_3 \prec x_1x_3 \prec x_2^2 \prec x_1x_2 \prec x_1^2 \prec x_3^3 \prec x_2x_3^2 \prec \dots$$

<u>Def.</u> In jedem Polynom von $\mathbb{R}[x_1,\dots,x_n]$ ungleich null wird der größte Term bzgl. $\prec$ der <u>Leitterm</u> des Polynoms genannt. Entsprechend definieren wir die Begriffe „Leitkoeffizient" und Leitmonom.

<u>Notation</u>: $\operatorname{lt}(f)$, $\operatorname{lc}(f)$, $\operatorname{lm}(f)$ für $f \in \mathbb{R}[x_1,\dots,x_n] \setminus \{0\}$.

Darstellung der symmetrischen Polynome

Satz (24.4)

Sei K ein Körper. Ein Polynom $f \in K[x_1, ..., x_n]$ ist genau dann symmetrisch, wenn ein Polynom $g \in K[x_1, ..., x_n]$ mit $f = g(\varepsilon_1, ..., \varepsilon_n)$ existiert.

Beweis von Satz 24.4

geg. $f \in R[x_1, \ldots, x_n]$. Zz:

f symm. $\Longleftrightarrow \exists\, g \in R[x_1, \ldots, x_n]$ mit $f = g(\varepsilon_1, \ldots, \varepsilon_n)$

„$\Longleftarrow$" klar, da die Pol. $\varepsilon_1, \ldots, \varepsilon_n$ symmetrisch sind

„$\Longrightarrow$" vollständige Induktion über die Position des Leitterms $\mathrm{lt}(f)$ bzgl. der Anordnung $\prec$.

Ind.-Anf. $f \in R \setminus \{0\}$: nichts zu zeigen, setze $g = f$.

Ind.-Schritt: Sei $f \in R[x_1, \ldots, x_n]$ nicht-

konstant. Überprüfe zunächst: Sind h, h' Monome mit $h \prec h'$, dann gilt auch $x_j h \prec x_j h'$ für $1 \leq j \leq n$. Daraus folgt unmittelbar: Sind g, g', h, h' Monome mit $g \succcurlyeq g'$ und $h \prec h'$ (wobei $g \succcurlyeq g' \iff g = g'$ oder $g \succ g'$) dann gilt $gh \prec g'h'$. Daraus folgt für bel. Polynome f, f' aus $R[x_1, \ldots, x_n]$ jeweils $lt(ff') = lt(f) \cdot lt(f')$.

Sei nun f unser vorgeg. nicht-konstantes Polynom und $lt(f) = c x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$. (*)

Da f symmetrisch ist, muss $a_1 \geq \ldots \geq a_n$ gelten.

denn: Ang. $a_k < a_{k+1}$ für ein $k \in \{1, \dots, n-1\}$.
Da f symm. ist, enthält f auch den Term, der durch Anw. der Transp. $(k\ k+1)$ auf $lt(f)$ zu Standekommt, dies ist $t' = c x_1^{a_1} \cdot \dots \cdot x_k^{a_{k+1}} \cdot x_{k+1}^{a_k} \cdot \dots \cdot x_n^{a_n}$
Es gilt $t' > lt(f)$, ein Widerspruch zur Def. des Leitterms. Wegen (*) können wir das Pol
$h = x_1^{a_1 - a_2} \cdot \dots \cdot x_{n-1}^{a_{n-1} - a_n} \cdot x_n^{a_n}$ bilden.
klar: $lt(\varepsilon_k) = x_1 \cdot \dots \cdot x_k$ für $1 \leq k \leq n$
Setze $g = h(\varepsilon_1, \dots, \varepsilon_n)$, überprüfe: Der Leitterm von $cg(\varepsilon_1, \dots, \varepsilon_n)$ stimmt mit $lt(f)$ überein
Setze $f_1 = f - cg(\varepsilon_1, \dots, \varepsilon_n)$. Dann gilt also $lt(f_1) < lt(f)$

Ind.-V. $\Rightarrow \exists\, g_1 \in R[x_1, \dots, x_n]$ mit

$f_1 = g_1(\varepsilon_1, \dots, \varepsilon_n)$ Setzen wir $g_2 =$

$cg + g_1$, dann folgt $g_2(\varepsilon_1 \dots, \varepsilon_n) =$

$cg(\varepsilon_1, \dots, \varepsilon_n) + g_1(\varepsilon_1, \dots, \varepsilon_n) = cg(\varepsilon_1, \dots, \varepsilon_n) + f_1$

$= cg(\varepsilon_1, \dots, \varepsilon_n) + f - cg(\varepsilon_1, \dots, \varepsilon_n) = f.$ □

Beispiel: Darstellung von $f = x_1^2 + x_2^2 + x_3^2 \in \mathbb{Q}[x_1, \dots, x_3]$ durch elementarsymmetrische Polynome

- $lt(f) = x_1^2$ setze $h = x_1^2 \cdot x_2^0 \cdot x_3^0 = x_1^2$

$f - h(\varepsilon_1, \varepsilon_2, \varepsilon_3) = x_1^2 + x_2^2 + x_3^2 - (x_1 + x_2 + x_2)^2 =$

$x_1^2 + x_2^2 + x_3^2 - x_1^2 - x_2^2 - x_3^2 - 2x_1x_2 - 2x_1x_3 - 2x_2x_3$

$= -2x_1x_2 - 2x_1x_3 - 2x_2x_3$

- $lt(f - h(\varepsilon_1, \varepsilon_2, \varepsilon_3)) = -2x_1x_2$, $\tilde{h} = x_1^0 \cdot x_2^1 \cdot x_3^0 = x_2$

$f - h(\varepsilon_1, \varepsilon_2, \varepsilon_3) - (-2)\,\tilde{h}(\varepsilon_1, \varepsilon_2, \varepsilon_3) =$

$-2x_1 - 2x_1x_3 - 2x_2x_3 + 2\varepsilon_2 = 0$

Ergebnis: $f = \tilde{\tilde{h}}(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ mit $\tilde{\tilde{h}} = x_1^2 - 2x_2$

Die Diskriminante eines Polynoms

Definition (24.5)

Sei K ein Körper, und sei $f \in K[x]$ gegeben durch $f = c(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$, mit $c \in K^\times$ und $\alpha_1, \ldots, \alpha_n \in K$. Dann bezeichnet man

$$\Delta(f) \quad = \quad c^2 \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

als die Diskriminante des Polynoms.

Beispiele für Diskriminanten von Polynomen

- Grad 2: Sei $f = x^2 + px + q = (x - \alpha_1)(x - \alpha_2)$

  Vieta $\Rightarrow$ $p = -\alpha_1 \alpha_2$, $q = \alpha_1 \alpha_2$

  $\Delta(f) = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 =$

  $(\alpha_1 + \alpha_2)^2 - 2\alpha_1\alpha_2 - 2\alpha_1\alpha_2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2$

  $= p^2 - 4q$

- Grad 3: $f = x^3 + ax^2 + bx + c = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$

  $\Rightarrow a = -(\alpha_1 + \alpha_2 + \alpha_3)$, $b = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$, $c = -\alpha_1\alpha_2\alpha_3$

  $\Delta(f) = (\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2$

Wichtige Beobachtung: Das Polynom

$g = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$ ist symmetrisch

(Wegen $S_3 = \langle (12), (13) \rangle$ genügt es zu überprüfen, dass g unter $\sigma = (12)$, $\tau = (13)$ unverändert bleibt. $\sigma g = (x_2 - x_1)^2 (x_2 - x_3)^2 (x_1 - x_3)^2$

$= (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 = g$

Nachweis von $\tau g = g$ analog.)

Auf Grund von Satz 24.4 besitzt g eine Darstellung durch elementarsymm. Polynome. Daraus folgt, dass $\Delta(f)$ durch

Polynom. Daraus folgt, dass $\Delta(f)$ durch

die Koeffizienten von f dargestellt werden kann.

Es gilt

$$\Delta(f) = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2$$

Spezialfall $f = x^3 + px + q$ $(a=0,\ b=p,\ c=q)$

$$\Rightarrow \Delta(f) = -4p^3 - 27q^2$$

Es gilt

- $\Delta(f) = 0 \Rightarrow$ f hat mind. eine mehrfache Nullstelle
- $\Delta(f) > 0 \Leftrightarrow$ f hat drei verschiedene reelle Nullstellen
- $\Delta(f) < 0 \Leftrightarrow$ f hat genau eine reelle und ein komplex-komplexes Paar von Nullstellen

Algebraische Unabhängigkeit der elementarsymm. Pol.

Proposition (24.6)

Sei K ein Körper. Dann sind die elementarsymmetrischen Polynome $\varepsilon_1, ..., \varepsilon_n \in K[x_1, ..., x_n]$ algebraisch unabhängig. Das bedeutet: Ist $h \in K[x_1, ..., x_n]$ ein Polynom mit $h(\varepsilon_1, ..., \varepsilon_n) = 0$, dann folgt $h = 0_K$.

Die allgemeine Gleichung

Definition (24.7)

Sei K ein Körper und $K[s_0, ..., s_{n-1}]$ ein Polynomring über K, dessen n Variablen mit $s_0, ..., s_{n-1}$ bezeichnet sind. Es sei $F = K(s_0, ..., s_{n-1})$ der Quotientenkörper dieses Polynomrings. Dann bezeichnet man

$$f \quad = \quad x^n + s_{n-1}x^{n-1} + ... + s_1x + s_0 \quad \in F[x]$$

als allgemeines Polynom und die Gleichung $f = 0$ als allgemeine Gleichung n-ten Grades über dem Körper K.

Die Galoisgruppe der allgemeinen Gleichung

Satz (24.8)

Sei E ein Zerfällungskörper des allgemeinen Polynoms f über F. Dann ist $E|F$ eine Galois-Erweiterung, mit $\mathrm{Gal}(E|F) \cong S_n$.

Beweis von Satz 24.8

geg: $F = K(s_0, \dots, s_n)$ Funktionenkörper in $s_0, \dots, s_n$ = Quotientenkörper des Polynomrings

allgem. Polynom $f = x^n + s_{n-1}x^{n-1} + \dots + s_1 x + s_0$

E Zerfällungskörper von f über F

Beh.: $E|F$ galois'sch, und $\mathrm{Gal}(E|F) \cong S_n$

Sei $K[x_1, \dots, x_n]$ ein weiterer Pol.-ring über K.

Betrachte die Operation von S_n auf den Elementen dieses Polynomrings durch Permutation der Variablen. Überprüfe: $K(x_1, \dots, x_n)^{S_n} =$

der Variablen über prüfe. $K(x_1,\dots,x_n)^{S_n} =$

$K(\varepsilon_1,\dots,\varepsilon_n)$, d.h. der Fixkörper von S_n ist genau der Teilkörper, der von den elem.-symm. Polynomen ε_k erzeugt wird. „$\supseteq$" klar, da $\varepsilon_1,\dots,\varepsilon_n$ symm.

„$\subseteq$" Sei $\alpha \in K(x_1,\dots,x_n)^{S_n}$, $\alpha = \frac{u}{v}$ mit $u, v \in K[x_1,\dots,x_n]$ teilerfremd, $v \neq 0$. $\forall \sigma \in S_n$:

$\frac{\sigma(u)}{\sigma(v)} = \sigma\left(\frac{u}{v}\right) = \frac{u}{v} \Rightarrow \sigma(u)v = \sigma(v)u \Rightarrow$

$v \mid \sigma(v)u$, v, u teilerfremd $\Rightarrow v \mid \sigma(v)$ $\xrightarrow{v, \sigma(v)}$ haben denselben Grad

$v = \sigma(v)$, damit auch $u = \sigma(u)$, für jedes $\sigma \in S_n$ $\Rightarrow u, v$ sind symmetrische Pol.

$\xrightarrow{\text{Satz 24.4}}$ $\exists u_1, v_1 \in K[x_1,\dots,x_n]$ mit $u = u_1(\varepsilon_1,\dots,\varepsilon_n)$, $v = v_1(\varepsilon_1,\dots,\varepsilon_n)$ $\Rightarrow \alpha = \frac{u_1(\varepsilon_1,\dots,\varepsilon_n)}{v_1(\varepsilon_1,\dots,\varepsilon_n)} \in K(\varepsilon_1,\dots,\varepsilon_n)$