7.4 Resultante und Diskriminante

7.4.1 Definition: Die *Sylvestermatrix* zweier Polynome der Form $f(X) = \sum_{i=0}^{m} a_i X^i$ und $g(X) = \sum_{j=0}^{n} b_j X^j$ über einem Ring R ist die $(m+n) \times (m+n)$-Matrix

$$\mathrm{Sylv}_{f,g} := \left(\begin{array}{ccccccccc} a_m & \dots & \dots & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & a_m & \dots & \dots & \dots & a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & 0 \\ 0 & \dots & 0 & a_m & \dots & \dots & \dots & a_1 & a_0 \\ \hline b_n & \dots & \dots & b_1 & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_n & \dots & \dots & b_1 & b_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & b_n & \dots & \dots & b_1 & b_0 \end{array}\right)$$

in der die ersten n Zeilen aus den Koeffizienten von f und die restlichen m Zeilen aus den Koeffizienten von g gebildet sind. Die Determinante der Sylvestermatrix heisst die *Resultante von f und g* und wird bezeichnet mit $\mathrm{Res}_{f,g} \in R$.

Offenbar ist die Resultante ein ganzzahliges Polynom in $a_0, \dots, a_m, b_0, \dots, b_n$, und zwar homogen vom Grad n in $a_0, \dots, a_m$ und homogen vom Grad m in $b_0, \dots, b_n$.

7.4.2 Proposition: Es gilt $\mathrm{Res}_{g,f} = (-1)^{mn} \mathrm{Res}_{f,g}$.

Beweis: $\mathrm{Syl}_{g,f}$ entsteht aus $\mathrm{Syl}_{f,g}$ durch $m \cdot n$ - malige Vertauschung zweier Zeilen

ggd.

7.4.3 Proposition: Seien $f, g \in K[X]$ vom Grad m bzw. n für einen Körper K. Dann ist $\mathrm{Res}_{f,g} = 0$ genau dann, wenn f und g einen gemeinsamen Teiler vom Grad > 0 haben.

Beweis: Sei $f = \sum a_i X^i$, $g = \sum b_j X^j$ $\Rightarrow$ $\mathrm{Syl}_{f,g} = \left(\begin{cases} a_{m-j+i} & i \le n \\ b_{i-j} & i > n \end{cases} \right)_{1 \le i,j \le n+m}$

Setze $a_i := 0$ für $i < 0$ oder $i > m$.
$b_j := 0$ für $j < 0$ oder $j > n$.

$\mathrm{Res}_{f,g} = 0 \iff$ die Zeilen von $\mathrm{Syl}_{f,g}$ sind lin. abh.

$\iff \exists (c_1, \dots, c_n, d_1, \dots, d_m) \in K^{n+m} \setminus \{0\}$

$\forall 1 \le j \le n+m$: $\sum_{i=1}^{n} c_i a_{m+j-i} = \sum_{i=1}^{m} d_i b_{i+n-j}$

$\Rightarrow$ $\sum_{j=1}^{m+n} \left(\sum_{i=1}^{n} c_i a_{m-j+i} \right) X^{m+n-j} = \sum_{j=1}^{m+n} \left(\sum_{i=1}^{m} d_i b_{i+n-j} \right) X^{m+n-j}$

$\| \; m-j+i = k$
$m+n-j = m-j+i-i+n = k-i+n$

$\| \; i+n-j = k$
$m+n-j = m+k-i$

$$\sum_{i,k} c_i a_k X^{k-i+n} = \sum_{i,k} d_i b_k X^{m+k-i}$$

$$\left(\sum_{i=1}^{n} c_i X^{n-i}\right) \cdot \left(\sum_k a_k X^k\right) = \left(\sum_{i=1}^{m} d_i X^{m-i}\right) \cdot \left(\sum_k b_k X^k\right)$$

u $\quad f$ $\quad v$ $\quad g$

$\Leftrightarrow \exists\, u, v \in K[X]$, nicht beide $= 0$, mit $\deg(u) < n$ und $\deg(v) < m$

und $\boxed{u \cdot f = v \cdot g}$.

$\deg(f) = m > \deg(v)$
$\deg(g) = n > \deg(u)$

$\Leftrightarrow$ f, g nicht teilerfremd. qed.

7.4.4 Proposition: Für alle Polynome der Form $f(X) = a_m \prod_{i=1}^{m}(X - \alpha_i)$ und $g(X) = b_n \prod_{j=1}^{n}(X - \beta_j)$ gilt

$$\mathrm{Res}_{f,g} \;=\; a_m^n \cdot b_n^m \cdot \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j).$$

Beweis: Gültig für a_m, b_n, alle α_i, β_j unabhängige Variable über $\mathbb{Z}$.

Setze in $R := \mathbb{Z}[a_m, b_n, (\alpha_i)_i, (\beta_j)_j]$.

	Lösungen mit auf in a_m	in b_n	Grad in $\alpha_1, \dots, \alpha_m$	Grad in $\beta_1, \dots, \beta_n$
n Zeilen mit Sylv$_{f,g}$	1	0	m	0
m Zeilen . –	0	1	0	n
$\mathrm{Res}_{f,g}$	n	m	$m \cdot n$	$m \cdot n$

7.4.5 Proposition: Für alle Polynome der Form $f(X) = a_m \prod_{i=1}^{m}(X - \alpha_i)$ und $g(X) = \sum_{j=0}^{n} b_j X^j$ gilt

$$\mathrm{Res}_{f,g} \;=\; a_m^n \cdot \prod_{i=1}^{m} g(\alpha_i).$$

Beweis: Falls $g(X) = b_n \cdot \prod_{j=1}^{n}(X - \beta_j)$

ist $\mathrm{Res}_{f,g} = a_m^n \cdot \prod_{i=1}^{m}\left(b_n \cdot \prod_{j=1}^{n}(\alpha_i - \beta_j)\right) = a_m^n \prod_{i=1}^{m} g(\alpha_i)$

Einsetzen ist ein Homo $\mathbb{Z}[a_m, (\alpha_i)_i, (b_j)_j] \longrightarrow \mathbb{Z}[a_m, (\alpha_i)_i, b_n, (\beta_j)_j]$ injektiv! geht.

$b_j = b_n \cdot s_{n-j}(\beta)$

$\forall i,j$:
Nach Einsetzen von β_j für α_i werden die Polynome nicht mehr teilerfremd $\Rightarrow \operatorname{Res}_{f,g} = 0$.

$\Rightarrow \alpha_i - \beta_j \mid \operatorname{Res}_{f,g}$ in R.

Die $\alpha_i - \beta_j$ für alle Paare (i,j) sind paarweise teilerfremd in R.

$$\Rightarrow a_m^n \cdot b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) \mid \operatorname{Res}_{f,g}.$$

Grad in $\alpha_1 \dots \alpha_m$: mn.

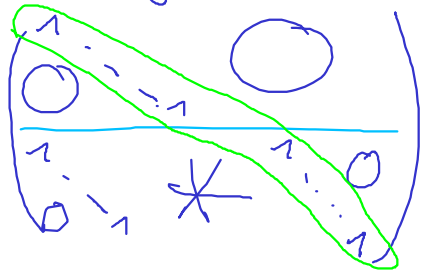
Grad in $\beta_1, \dots, \beta_n$: mn.

$\Rightarrow$ das Polynom hat Grad 0 in allen Variablen $\Rightarrow$ ist $= c \in \mathbb{Z}$.

Also $\boxed{\operatorname{Res}_{f,g} = c \cdot a_m^n \cdot b_n^m \prod_{i,j} (\alpha_i - \beta_j)}$

Für $f = X^m$ und $g = (X+1)^n$

ist $\operatorname{Res}_{f,g} = \det$



$= 1$

$\Rightarrow c = 1$.

$$a_m^n \cdot b_n^m \cdot \prod_{i,j} (\alpha_i - \beta_j) = 1.$$

$1 \quad 1 \quad \quad 0 \quad -1$

ged.

$f(X) = \sum_{i=0}^{m} a_i X^i \Rightarrow f'(X) = \sum_{i=1}^{m} a_i \, i \, X^{i-1} = \sum_{i=0}^{m-1} a_{i+1} \cdot (i+1) \cdot X^i = m \cdot a_m X^{m-1} + \ldots$

Im Spezialfall $g = f'$ ist $n = m - 1$ und $b_{m-1} = ma_m$; also ist die erste Spalte der Sylvestermatrix $\mathrm{Sylv}_{f,f'}$ durch a_m teilbar. Es existiert daher ein eindeutiges ganzzahliges Polynom P_f in $a_0, \ldots, a_m$ mit $\mathrm{Res}_{f,f'} = a_m P_f$.

7.4.6 Definition: Die *Diskriminante* eines Polynoms $f(X) = \sum_{i=0}^{m} a_i X^i$ vom Grad m über einem Ring R ist

$$\mathrm{Disc}_f \;:=\; (-1)^{\frac{m(m-1)}{2}} P_f \;\in\; R.$$

7.4.7 Proposition: Für jedes Polynom der Form $f(X) = a_m \prod_{i=1}^{m} (X - \alpha_i)$ gilt

$$\mathrm{Disc}_f \;=\; a_m^{2m-2} \cdot \prod_{1 \leqslant i < j \leqslant m} (\alpha_i - \alpha_j)^2.$$

Beweis: $\forall i: \; f'(X) = \sum_{k=1}^{m} a_m \cdot \prod_{i \neq k} (X - \alpha_i)$

$\Rightarrow f'(\alpha_j) = \sum_{k=1}^{m} a_m \cdot \prod_{i \neq k} (\alpha_j - \alpha_i) = a_m \cdot \prod_{i \neq j} (\alpha_j - \alpha_i)$

$\Rightarrow a_m \cdot \mathrm{Disc}\, f =$
$= (-1)^{\frac{m(m-1)}{2}} \cdot \mathrm{Res}_{f,f'}$
$= (-1)^{\frac{m(m-1)}{2}} \cdot a_m^{m-1} \cdot \prod_i f'(\alpha_i)$
$= (-1)^{\frac{m(m-1)}{2}} \cdot a_m^{m-1} \cdot a_m^m \cdot \prod_{i \neq j} (\alpha_j - \alpha_i)$
$= a_m^{2m-1} \cdot \prod_{i<j} (\alpha_j - \alpha_i)^2.$

7.4.8 Folge: Ein Polynom f über einem Körper ist separabel genau dann, wenn $\mathrm{Disc}_f \neq 0$ ist.

7.4.9 Anwendung: Für jedes normierte Polynom $f \in \mathbb{Z}[X]$ ist $\mathrm{Disc}_f \in \mathbb{Z}$, und für eine beliebige Primzahl p ist $f \bmod (p)$ separabel in $\mathbb{F}_p[X]$ genau dann, wenn $p \nmid \mathrm{Disc}_f$ ist.

$\mathrm{Disc}_f \bmod (p) = \mathrm{Disc}_{f \bmod (p)}$

$\mathrm{Syl}_{f,f'} = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}$

$\det = ab^2 + 4a^2c - 2ab^2$
$= a(4ac - b^2)$
$\Rightarrow \mathrm{Disc}_f = b^2 - 4ac.$

7.4.10 Beispiel: In kleinen Graden ist

$f(X)$	Disc_f
$aX + b$	1
$aX^2 + bX + c$	$b^2 - 4ac$
$aX^3 + bX^2 + cX + d$	$b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$

7.4.11 Bemerkung: Resultante und Diskriminante kann man auch als symmetrische Funktionen der Nullstellen konstruieren. Der obige Weg liefert aber schneller die richtigen Formeln, insbesondere für nicht normierte Polynome.

Bsp.: $f(X) = X^3 + aX + b$

$\Rightarrow \mathrm{Syl}_{f,f'} = \begin{pmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{pmatrix}$ -3 -3

$\Rightarrow \mathrm{Res}_{f,f'} = \det \begin{pmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 0 & 0 & -2a & -3b & 0 \\ 0 & 0 & 0 & -2a & -3b \\ 0 & 0 & 3 & 0 & a \end{pmatrix}$

$= 4a^3 + 27b^2$

$\mathrm{Disc}_f = (-1)^{\frac{3(3-1)}{2}} \cdot \mathrm{Res}_{f,f'} = -4a^3 - 27b^2.$

7.5 Explizite Konstruktion der Zwischenkörper

Sei L/K endlich galoissch mit Galoisgruppe Γ, und sei $\Gamma' < \Gamma$ eine Untergruppe. Um den zugehörigen Zwischenkörper $L^{\Gamma'}$ zu beschreiben, verschafft man sich zuerst geeignete Elemente $b_1, \ldots, b_k \in L^{\Gamma'}$, die man entweder vermittels expliziter Erzeugenden von L errät oder durch eine Γ'-invariante Konstruktion findet. Wenn dann $[K(b_1, \ldots, b_k)/K] = [\Gamma : \Gamma']$ ist, so folgt direkt $K(b_1, \ldots, b_k) = L^{\Gamma'}$. In der Praxis genügt dafür oft schon ein einzelnes Element b_1.

7.5.1 Beispiel: Sei $\Gamma < S_n$ die Galoisgruppe eines normierten separablen Polynoms $f \in K[X]$ mit den Nullstellen $a_1, \ldots, a_n \in L$. Betrachte die Quadratwurzel der Diskriminante

$$b := \prod_{1 \leqslant i < j \leqslant n} (a_i - a_j) \in L.$$

Bem.: 2 Charakteristik 2 ist die einzige symmetrische Ausnahme
$n=2$: $a_1 + a_2 = s_1$
$n=3$: ...

Sei ausserdem $\mathrm{char}(K) \neq 2$. Dann ist $\Gamma < A_n$ genau dann, wenn $b \in K$ ist. Andernfalls ist $K(b)$ der Zwischenkörper vom Grad 2 über K, welcher der Untergruppe $\Gamma \cap A_n < \Gamma$ entspricht.

Bem.: $\forall \sigma \in \Gamma$: $\sigma(b) = \prod_{i<j} (\sigma(a_i) - \sigma(a_j)) = \prod_{i<j} (a_{\sigma i} - a_{\sigma j})$

$= (-1)^{\#\{\text{Fehlstände in } \sigma\}} \cdot \prod_{i<j} (a_i - a_j) = \mathrm{sgn}(\sigma) \cdot b$.

f separabel $\Rightarrow b \neq 0$. Folglich $\sigma(b) = b \Leftrightarrow \sigma \in A_n$.

Fall 1: $\Gamma < A_n \Rightarrow \forall \sigma \in \Gamma : \sigma(b) = b \Rightarrow b \in K$.

Fall 2: $\Gamma \not< A_n \Rightarrow \exists \sigma \in \Gamma : \sigma(b) \neq b \Rightarrow b \notin K$ aber $b \in L^{\Gamma \cap A_n}$

Wegen $[L^{\Gamma \cap A_n}/K] = [\Gamma : \Gamma \cap A_n] = 2$. folgt: $L^{\Gamma \cap A_n} = K(b)$. Zusl.