Zu §6.4: Resultante & Diskriminante

Def.: Zu $f(X) = \sum_{i=0}^{m} a_i X^i$ und $g(X) = \sum_{j=0}^{n} b_j X^j \in R[X]$ ist die **Sylvestermatrix**

$$Sylv_{f,g} := \begin{pmatrix} a_m & \cdots & & a_0 & 0 \\ 0 & \ddots & & & \ddots \\ & a_m & \cdots & & a_0 \\ b_n & & \ddots & & 0 \\ & \ddots & & b_0 & \\ 0 & & b_n & \cdots & b_0 \end{pmatrix} \begin{matrix} \} n \\ \\ \\ \} m \\ \\ \end{matrix}$$

Die **Resultante** von f, g ist $Res_{f,g} := \det(Sylv_{f,g}) \in R$.

Prop. Für $f, g \in K[X]$, für K Körper, wie oben gilt:

$$Res_{f,g} = 0 \iff ggT(f,g) \neq 1.$$

Beweis: Setze $a_i := 0$ für $i \notin [0,m]$ und $b_j := 0$ für $j \notin [0,n]$.

Dann ist $Sylv_{f,g} = \left(\begin{cases} a_{i-j+m} & i \leq n \\ b_{i-j} & i > n \end{cases} \right)_{i,j=1,\ldots,m+n}$

Da die Matrix Koeffizienten in einem Körper hat, gilt

$\det(Sylv_{f,g}) = 0 \iff$ Zeilen von $Sylv_{f,g}$ linear abhängig

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

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

Diese Gleichungen alle zusammengenommen sind äquivalent zu

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

$$\left\| \leftarrow i-j+m=k \right. \qquad \left\| \leftarrow i+n-j=k \right.$$

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

$$\left\| \right. \qquad \left\| \right.$$

$$\underbrace{\left(\sum_{i=1}^{n} c_i X^{n-i} \right)}_{=:h} \underbrace{\left(\sum_{k} a_k X^k \right)}_{f} \qquad \underbrace{\left(\sum_{i=1}^{m} d_i X^{m-i} \right)}_{=:k} \underbrace{\left(\sum_{k} b_k X^k \right)}_{g}$$

Also ... $\iff \exists\, h, k \in K[X]$, nicht beide 0, mit $hf = kg$

und $\deg(h) < n = \deg(g)$

und $\deg(k) < m = \deg(f)$

$\iff ggT(f,g) \neq 1$

↑ eindeutige Primfaktorzerlegung in $K[X]$. qed.

Prop.: Für alle $f(X) = a_m \cdot \prod_{i=1}^{m} (X-\alpha_i)$ und $g(X) = b_n \cdot \prod_{j=1}^{n} (X-\beta_j)$

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

- **Beweis:** Beide Seiten sind ganzzahlige Polynome in $a_m, \alpha_1, \dots, \alpha_m, b_n, \beta_1, \dots, \beta_n$. Es genügt also die Aussage zu beweisen in dem Fall, dass diese Unbestimmten unabhängige Variable sind; den allgemeinen Fall erhält man dann durch Einsetzen. Wir rechnen also in dem Polynomring $R := \mathbb{Z}[a_m, \alpha_1, \dots, \alpha_m, b_n, \beta_1, \dots, \beta_n]$.
- Zuerst bestimmen wir den Grad von $\operatorname{Res}_{f,g}$:

	Grad in a_m	Grad in $\alpha_1, \dots, \alpha_m$	Grad in b_n	Grad in $\beta_1, \dots, \beta_n$
n-fache von $\operatorname{Sylv}_{f,g}$	1	m	0	0
m-fache von $\operatorname{Sylv}_{f,g}$	0	0	1	n
$\operatorname{Res}_{f,g}$	n	$\leq mn$	m	$\leq mn$

- Für alle i,j wird $\operatorname{Res}_{f,g}$ zu Null nach Einsetzen von $\alpha_i := \beta_j$, wegen voriger Proposition, da dann f, g eine gemeinsame Nullstelle bekommen. Also gilt $\alpha_i - \beta_j \mid \operatorname{Res}_{f,g}$.
- Da die Polynome $\alpha_i - \beta_j$ für alle i,j wie a_m, b_n paarweise irreduzibel in R sind, folgt

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

für ein $\lambda \in R$. Aus Gradgründen muss jetzt also $\lambda \in \mathbb{Z}$ sein.
- Schließlich bestimmen wir λ durch Einsetzen eines Spezialfalls:
Für $f = X^m$ und $g = (X+1)^n$ sind $a_m = b_n = 1$ und $\alpha_i = 0$ und $\beta_j = -1$ und $\operatorname{Res}_{f,g} = \det \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ * & & & 1 \end{pmatrix} = 1$

sowie $R(Y^5) = (0-(-1))^{mn} \cdot \lambda = \lambda$

$\Rightarrow \lambda = 1$.

qed.

Def.: $\deg(f) = m \Rightarrow \mathrm{Disc}_f$ definiert durch

$$a_m \cdot \mathrm{Disc}_f = (-1)^{\frac{m(m-1)}{2}} \cdot \mathrm{Res}_{f,f'}$$

Prop.: Für jedes $f(X) = a_m \prod_{i=1}^{m} (X - \alpha_i)$ gilt

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

Beweis: Für jedes i schreibe $f(X) = (X - \alpha_i) \cdot g_i(X)$

$$\Rightarrow f'(X) = g_i(X) + (X - \alpha_i) \cdot g_i'(X)$$
$$\Rightarrow f'(\alpha_i) = g_i(\alpha_i)$$

Dann ist

$$a_m \cdot \mathrm{Disc}_f = (-1)^{\frac{m(m-1)}{2}} \cdot \mathrm{Res}_{f,f'} = (-1)^{\frac{m(m-1)}{2}} \cdot a_m^{m-1} \cdot \prod_{i=1}^{m} f'(\alpha_i)$$

$$= (-1)^{\frac{m(m-1)}{2}} \cdot a_m^{m-1} \cdot \prod_{i=1}^{m} \Big(a_m \cdot \prod_{\substack{1 \le j \le m \\ j \ne i}} (\alpha_i - \alpha_j) \Big)$$

$$= (-1)^{\frac{m(m-1)}{2}} \cdot a_m^{2m-1} \cdot \prod_{\substack{i,j = 1..m \\ i \ne j}} (\alpha_i - \alpha_j)$$

$$\overset{!}{=} a_m^{2m-1} \cdot \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j)^2 \quad . \qquad \text{qed.}$$

Beispiel: $f(X) = aX^2 + bX + c \Rightarrow f'(X) = 2aX + b$

$$\Rightarrow a \cdot \mathrm{Disc}_f = -\det \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2 & b \end{pmatrix} = \ldots = a(b^2 - 4ca)$$

Beispiel: $f(X) = X^3 + aX + b \Rightarrow f'(X) = 3X^2 + a$

$$\Rightarrow \mathrm{Disc}_f = -\det \begin{pmatrix} 1 & 0 & a & b & \\ & 1 & 0 & a & b \\ 3 & 0 & a & & \\ & 3 & 0 & a & \\ & & 3 & 0 & a \end{pmatrix} = \ldots = -4a^3 - 27b^2$$

Anmerkung: Sei $f \in \mathbb{R}[X]$ normiert. Dann ist $\mathrm{Disc}_f \in \mathbb{Z}$ und

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

$\Rightarrow f \bmod p$ separabel $\iff p \nmid \mathrm{Disc}_f$.

Bem.: Die obige Definition von Diskriminante und Resultante eignet sich nur schlecht zur expliziten Berechnung, da Δ und P nur indirekt angegeben sind. Es gehts aber auch direkter.
Zum Vergleich betrachten wir zuerst die

Prop.: Vandermondesche Determinante:
Für $\lambda_1, \dots, \lambda_n \in R$ gilt

$$\det \begin{pmatrix} 1 & \cdots & 1 \\ \lambda_1 & \cdots & \lambda_n \\ \lambda_1^2 & \cdots & \lambda_n^2 \\ \lambda_1^{n-1} & \cdots & \lambda_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} (\lambda_j - \lambda_i)$$

Beweis: Es genügt, dies für unabhängige Variable X_i anstelle von λ_i zu beweisen, also in $\mathbb{Z}[X_1, \dots, X_n]$, und danach beliebige λ_i einzusetzen.
Setzen wir dann zwei Variable $X_i = X_j$ gleich, so werden zwei Spalten identisch und somit die Determinante 0. Folglich teilt $X_j - X_i$ die Determinante. Für alle $1 \le i < j \le n$ sind die $X_j - X_i$ paarweise inäquivalente Primelemente, und der Ring $\mathbb{Z}[X_1, \dots, X_n]$ ist faktoriell. Also ist die rechte Seite ein Teiler der linken Seite. Da beide Polynome denselben Grad $\frac{n(n-1)}{2}$ sind, ist der Faktor ein Element $c \in \mathbb{Z}$. Diesen Wert bestimmen wir als Koeffizienten von $1 \cdot X_2 \cdot X_3^2 \cdots X_n^{n-1}$, was $c = 1$ ergibt, qed.