WOLFGANG K. SEILER
*Tel.* 2515



*6. März 2020*

# 3. Übungsblatt Computeralgebra

**Aufgabe 1:** *(6 Punkte)*

*a)* Berechnen Sie für die beiden Polynome $f = X^6 + 4X^5 + 9X^4 + 16X^3 + 25X^2 + 36X + 49$ und $g = 2X^5 + 3X^4 + 5X^3 + 7X^2 + 11X + 13$ aus $\mathbb{Z}[X]$ die Resultante von $f \bmod 2$ und $g \bmod 2$!

**Lösung:** $f \bmod 2 = X^6 + X^4 + X^2 + 1$ und $g \bmod 2 = X^4 + X^3 + X^2 + X + 1$; die Resultante ist also

$$\begin{vmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1
\end{vmatrix}.$$

Subtrahiert man die erste Zeile von der fünften, steht in der ersten Spalte nur noch ganz oben eine Eins; die Determinante wird dann durch Entwicklung nach der ersten Spalte zur Determinante, bei der die erste Zeile und die erste Spalte gestrichen sind, also

$$\begin{vmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1
\end{vmatrix}.$$

Damit kann man durch Subtraktion der ersten Zeile von der vierten und der fünften genauso weitermachen und erhält

$$\begin{vmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1
\end{vmatrix}.$$

Im nächsten Schritt kommen wir genauso auf

$$\begin{vmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{vmatrix}, \text{ dann } \begin{vmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{vmatrix}.$$

Hier können wir, da es modulo zwei keine Vorzeichen gibt, einfach die erste Spalte und die vierte Zeile streichen, um dann beim nächsten Schritt wieder wie gewohnt weiterzumachen:

$$\begin{vmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{vmatrix} \quad \text{und} \quad \begin{vmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{vmatrix}.$$

Subtraktion der zweiten von der ersten Zeile sorgt dafür, daß in der zweiten Spalte nur noch eine Eins steht; wir erhalten also die $3 \times 3$-Determinante, die wir nach der Regel von SARRUS ausrechnen können:

$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{vmatrix} = 0 + 0 + 1 + 0 + 1 + 1 = 1\,.$$

Die Resultante ist also gleich eins.

*b)* Was ist der ggT von $f$ und $g$ in $\mathbb{Z}[X]$ ?

**Lösung:** Ein gemeinsamer Teiler $h$ positiven Grades müßte als Teiler von $f$ den führenden Koeffizienten eins oder minus eins haben; damit hätte auch $h \bmod 2$ positiven Grad und wäre Teiler von $f \bmod 2$ und $g \bmod 2$. Einen solchen Teiler kann es aber nicht geben, da die Resultante nicht verschwindet.

*c)* Geben Sie eine obere Schranke für $|\mathrm{Res}_X(f, g)|$ an!

**Lösung:** $f$ hat die Höhe 49, $g$ hat Höhe 13. Die Resultante ist also die Determinante einer $11 \times 11$-Matrix mit fünf Zeilen, deren Einträge höchstens Betrag 49 haben, und sechs Zeilen mit Betragsschranke 13. Eine Schranke für den Betrag ist daher

$$11! \cdot 49^5 \cdot 13^6 = 54\,424\,723\,587\,048\,323\,308\,800\,.$$

(Tatsächlich ist $\mathrm{Res}_X(f, g) = 624\,424\,145$ erheblich kleiner.)

**Aufgabe 2:** *(6 Punkte)*

*a)* Bestimmen Sie die Inhalte der beiden Polynome

$$f = 12X^5 + 90X^4 + 78X^2 + 18X + 36 \quad \text{und} \quad g = (15X - 5)(12X - 24)$$

aus $\mathbb{Z}[X]$ !

**Lösung:** Der ggT von zwölf und neunzig ist sechs, und sechs ist auch ein Teiler von 78, 18 und 36. Somit ist $I(f) = 6$.

$$g = 5 \cdot (3X - 1) \cdot 12 \cdot (X - 2) = 60 \cdot (3X - 1)(X - 2) = 60 \cdot (3X^2 - 7X + 2)$$

hat den Inhalt sechzig.

*b)* Was sind die primitiven Anteile $f^*$ und $g^*$ von $f$ und $g$ ?

**Lösung:** $f^* = 2X^5 + 15X^4 + 13X^2 + 3X + 6$ und $g^* = (3X-1)(X-2) = 3X^2 - 7X + 2$.

*c)* Bestimmen Sie $\operatorname{ggT}(f^*, g^*)$ !

**Lösung:** $g^*$ hat die beiden Nullstellen $x = 2$ und $x = \frac{1}{3}$. Da alle Terme in $f^*$ positiv sind, ist $f^*(x)$ in beiden Fällen positiv, so daß keiner der beiden Linearfaktoren Teiler von $f^*$ sein kann. Somit ist $\operatorname{ggT}(f^*, g^*) = 1$.

*d)* Was ist $\operatorname{ggT}(f, g)$ ?

**Lösung:** Da die primitiven Anteile teilerfremd sind, ist der ggT von $f$ und $g$ gleich dem ggT der Inhalte, also sechs.

**Aufgabe 3:** *(4 Punkte)*

*a)* Betrachten Sie $f = X^2Y^3 + X^2Y + X^2 + 2XY^3 + X + Y^3 - Y - 2$ als Polynom in $Y$ über $\mathbb{Z}[X]$ und berechnen Sie den Inhalt und den primitiven Anteil von $f$ !

**Lösung:** Als Polynom in $Y$ über $\mathbb{Z}[X]$ ist

$$f = (X^2+2X+1)Y^3 + (X^2-1)Y + (X^2+X-2) = (X+1)^2Y^3 + (X+1)(X-1)Y + (X-1)(X+2)\,.$$

Die drei Koeffizienten haben keinen gemeinsamen Teiler positiven Grades; der Inhalt ist also eins und $f$ selbst ist primitiv.

*b)* Betrachten Sie $f$ nun als Polynom in $X$ über $\mathbb{Z}[Y]$, und berechnen Sie wieder Inhalt und primitiven Anteil!

**Lösung:** Nun sortieren wir nach $X$-Potenzen und erhalten

$$f = (Y^3 + Y + 1)X^2 + (2Y^3 + 1)X + (Y^3 - Y - 2)\,.$$

Ein gemeinsamer Teiler von $Y^3 + Y + 1$ und $Y^3 - Y - 2$ ist auch ein Teiler der Differenz $2Y + 3$; da keines der beiden Polynome an deren Nullstelle $-\frac{2}{3}$ verschwindet, sind die beiden teilerfremd, und somit ist auch hier der Inhalt gleich eins und $f$ selbst ist der primitive Anteil.

**Aufgabe 4:** *(4 Punkte)*

Die beiden Polynome $f, g \in k[X, Y]$ seien aufgefaßt als Polynome in $Y$ über $k[X]$. Zeigen Sie:

*a)* Wenn $\deg \operatorname{ggT}\big(f(x, Y), g(x, Y)\big) < \deg_Y \operatorname{ggT}(f, g)$ für ein $x \in k$, so ist $x$ eine Nullstelle sowohl des führenden Koeffizienten von $f$ als auch des führenden Koeffizienten von $g$.

**Lösung:** $h$ sei der ggT von $f$ und $g$ in $k[X, Y]$. Für jedes $x \in k$ ist dann $h(x, Y)$ in $k[Y]$ ein Teiler sowohl von $f(x, Y)$ als auch von $g(x; Y)$, ist also ein Teiler von $\operatorname{ggT}\big(f(x, Y), g(x, Y)\big)$. Somit ist $\deg h(x, Y) \le \deg \operatorname{ggT}\big(f(x, Y), g(x, Y)\big)$. Falls dieser Grad kleiner ist als der $Y$-Grad von $h$, hat also auch $h(x, Y)$ einen kleineren Grad als $\deg_Y h$, und das ist genau dann der Fall, wenn der Koeffizient von $Y^{\deg_Y h}$ an der Stelle $x$ verschwindet.

*b)* Es gibt höchstens endlich viele $x \in k$, für die $\deg \operatorname{ggT}\big(f(x, Y), g(x, Y)\big) > \deg_Y \operatorname{ggT}(f, g)$ ist.

**Lösung:** Sei wieder $h = \operatorname{ggT}(f, g)$. Dann sind $f_0 = f/h$ und $g_0 = g/h$ zwei zueinander teilerfremde Polynome aus $k[X, Y]$. Für jedes $x \in k$ ist $h(x, Y)$ ein Teiler von $f(x, Y)$

und $g(x, Y)$; der größte gemeinsame Teiler von $f(x, Y)$ und $g(x, Y)$ ist $h(x, Y)$ mal dem ggT von $f_0(x, Y)$ und $g_0(x, Y)$. Falls $\deg\Big(\mathrm{ggT}\big(f(x, Y), g(x, Y)\big)\Big) > \deg_Y\big(\mathrm{ggT}(f, g)\big)$ ist, müssen daher die Polynome $f_0(x, Y)$ und $g_0(x, Y)$ in $k[Y]$ einen gemeinsamen Teiler positiven Grades haben. Dies ist genau dann der Fall, wenn ihre Resultante verschwindet. Falls $\deg f_0(x, Y) = \deg_Y f_0$ und $\deg g_0(x, Y) = \deg_Y g_0$ ist, ist diese Resultante gleich dem Wert des Polynoms $\mathrm{Res}_Y(f_0, g_0) \in k[X]$ an der Stelle $x$. Da ein Polynom in einer Veränderlichen über einem Körper höchstens endlich viele Nullstellen hat, gibt es höchstens viele $x \in k$, für die das der Fall ist. Falls $\deg f_0(x, Y) \neq \deg_Y f_0$ oder $\deg g_0(x, Y) \neq \deg_Y g_0$ ist, kann man die Resultante nicht so berechnen, aber die Anzahl der betroffenen $x \in k$ ist ebenfalls endlich, da es sich um die Nullstellen der führenden Koeffizienten von $f_0$ und $g_0$ aufgefaßt als Elemente von $k[X][Y]$ handelt.