WOLFGANG K. SEILER
Tel. 2515

B6, B4.18

6. März 2020

3. Übungsblatt Elliptische Kurven

Aufgabe 1: *(4 Punkte)*
Zeigen Sie:

a) Jedes Polynom $f \in k[X_1, \ldots, X_n]$ läßt sich in eindeutiger Weise als Summe homogener Polynome verschiedener Grade darstellen.

Lösung: f ist eine Linearkombination von Monomen $X_1^{e_1} \cdots X_n^{e_n}$. Für jedes $d \in \mathbb{N}_0$ sei f_d die Teilsumme aus jenen Monomen, für die $e_1 + \cdots + e_n = d$ ist. Dann ist f_d homogen vom Grad d, und f ist die Summe der f_d. Da ein Polynom eine endlich Summe von Monomen ist, gibt es nur endlich viele von Null verschiedene Summanden f_d. Die Darstellung ist eindeutig, denn ein homogenes Polynom vom Grad d ist nach Definition eine Linearkombination von Monomen mit $e_1 + \cdots + e_n = d$.

b) Jeder Teiler eines homogenen Polynoms ist selbst homogen.

Lösung: g sei ein Teiler des homogenen Polynoms f. Dann gibt es ein Polynom h, so daß $f = gh$ ist. Der minimale Grad eines in G vorkommenden Monoms sei d, und g_1 sei die Teilsumme aller Terme vom Grad d. Dann ist $g = g_1 + g_2$, wobei in g_2, falls es nicht verschwindet, nur Terme vom Grad größer d vorkommen. Entsprechend schreiben wir $h = h_1 + h_2$, wobei in h_1 nur Monome des minimalen Grads e vorkommen und in h_2, falls ungleich dem Nullpolynom, nur solche mit größerem Grad. Dann ist $f = g_1h_1 + g_1h_2 + g_2h_1 + g_2h_2$ mit einem homogenen Polynom g_1h_1 vom Grad $d + e$. Da f homogen ist und $g_1h_1 \neq 0$ muß dann auch f den Grad $d + e$ haben, und da in den restlichen Summanden nur Monome größeren Grades stehen, müssen diese verschwinden. Somit ist $g = g_1$ homogen vom Grad d.

Aufgabe 2: *(6 Punkte)*

a) Zerlegen Sie das Polynom $F = X^4Y^2 - 6X^3Y^3 + 11X^2Y^4 - 6XY^5 \in \mathbb{Z}[X, Y]$ in seine irreduziblen Bestandteile!

Lösung: $F = XY^2(X^3 - 6X^2Y + 11XY^2 - 6Y^3)$. In der klammer steht ein homogenes Polynom vom Grad drei; Dehomogenisieren macht daraus $x^3 - 6x^2 + 11x - 6$. Nach dem Wurzelsatz von VIÈTE sind Summe und Produkt der drei Nullstellen jeweils gleich sechs; es bietet sich daher an, die Zahlen $1, 2$ und 3 zu testen. Alle drei sind Nullstellen, d.h.

$$x^3 - 6x^2 + 11x - 6 = (x - 1)(x - 2)(x - 3)\,.$$

Homogenisieren macht daraus

$$X^3 - 6X^2Y + 11XY^2 - 6Y^3 = (X - Y)(X - 2Y)(X - 3Y)\,,$$

also ist $F = X(X - Y)(X - 2Y)(X - 3Y)Y^2$.

b) Bestimmen Sie die Nullstellen von $G = X^2Y^3(3X - 2Y)(5X - 10Y)(4Y - 6X)(Y - 3X) \in \mathbb{Z}[X, Y]$ in $\mathbb{P}^1(\mathbb{Q})$!

Lösung: Wegen des Faktors X^2 ist $(0:1)$ eine doppelte Nullstelle, und wegen Y^3 ist $(1:0)$ eine dreifache. Die verbleibenden vier Linearfaktoren führen zu den einfachen Nullstellen $(2:3)$, $(2:1)$, $(3:2)$ und $(3:1)$.

Aufgabe 3: *(3 Punkte)*
Zeigen Sie, daß sich jedes homogene Polynom $F \in \mathbb{R}[X,Y]$ als Produkt linearer und quadratischer homogener Polynome aus $\mathbb{R}[X,Y]$ schreiben läßt!

Lösung: F sein homogen vom Grad d. Wir nehmen zunächst an, daß F nicht durch Y teilbar ist; dann ist $f(X,1)$ ein Polynom aus $\mathbb{R}[X]$. Wegen des Fundamentalsatzes der Algebra zerfällt dieses in lineare und quadratische Faktoren; durch Homogenisieren bekommen wir daher ein Darstellung von F als Produkt homogener linearer und quadratischer Polynome. Falls F durch Y teilbar ist, läßt sich F schreiben als Produkt einer Y-Potenz mal einem homogenen Polynom F^*, das nicht durch Y teilbar ist; F^* läßt sich in der gewünschten Weise zerlegen, und die Y-Potenz ist Produkt von linearen homogenen Polynomen Y.

Aufgabe 4: *(4 Punkte)*

a) Berechnen Sie die Resultante der beiden homogenen Polynome

$$f = 2XY + 3Y^2 \quad \text{und} \quad g = 4X^2 + 5XY\,!$$

Lösung: Beide Polynome haben Grad zwei; somit ist

$$\operatorname{Res}(f,g) = \begin{vmatrix} 0 & 2 & 3 & 0 \\ 0 & 0 & 2 & 3 \\ 4 & 5 & 0 & 0 \\ 0 & 4 & 5 & 0 \end{vmatrix} = 4 \cdot \begin{vmatrix} 2 & 3 & 0 \\ 0 & 2 & 3 \\ 4 & 5 & 0 \end{vmatrix} = 4 \cdot (-3) \cdot \begin{vmatrix} 2 & 3 \\ 4 & 5 \end{vmatrix} = 4 \cdot (-3) \cdot (-2) = 24\,.$$

b) Berechnen Sie $\operatorname{Res}_X(f,g)$, wobei f und g als Polynome in X über $\mathbb{Z}[Y]$ aufgefaßt werden sollen.

Lösung: $f = 2Y \cdot X + 3Y^2$ ist ein lineares Polynom in X, während $g = 4X^2 + 5Y \cdot X$ ein quadratisches ist. Die Resultante ist daher

$$\operatorname{Res}_X(f,g) = \left| \begin{pmatrix} 2Y & 3Y^2 & 0 \\ 0 & 2Y & 3Y^2 \\ 4 & 5Y & 0 \end{pmatrix} \right| = -3Y^2 \cdot \begin{vmatrix} 2Y & 3Y^2 \\ 4 & 5Y \end{vmatrix} = -3Y^2 \cdot (-2Y^2) = 6Y^4\,.$$

c) Berechnen Sie $\operatorname{Res}_Y(f,g)$, wobei f und g als Polynome in Y über $\mathbb{Z}[X]$ aufgefaßt werden sollen!

Lösung: $f = 3Y^2 + 2X \cdot Y$ ist ein quadratisches Polynom in Y und $g = 5X \cdot Y + 4X^2$ ein lineares. Die Resultante ist daher

$$\operatorname{Res}_Y(f,g) = \left| \begin{pmatrix} 3 & 2X & 0 \\ 5X & 4X^2 & 0 \\ 0 & 5X & 4X^2 \end{pmatrix} \right| = 4X^2 \cdot \begin{vmatrix} 3 & 2X \\ 5X & 4X^2 \end{vmatrix} = 4X^2 \cdot 2X^2 = 8X^4\,.$$

Aufgabe 5: *(3 Punkte)*

$R = k[T]$ sei der Polynomring in einer Veränderlichen T.

a) $f, g \in R[X]$ seien zwei Polynome. Für welche $t \in k$ ist

$$\mathrm{Res}_X(f,g)(t) = \mathrm{Res}_X\big(f(t,X), g(t,X)\big) \ ?$$

Lösung: Dies ist genau dann der Fall, wenn der X-Grad von f gleich dem von $f(t,X)$ ist und der von g gleich dem von $g(t,X)$, d.h. wenn die führenden Koeffizienten von f und g, geschrieben als Polynome in X mit Polynomen in T als Koeffizienten, beide an der Stelle t nicht verschwinden. In diesem Fall haben die SYLVESTER-Matrizen dieselbe Form, wobei die Einträge in der von f und g Polynome in T sind, in der von $f(t,X)$ und $g(t,X)$ dagegen die Werte dieser Polynome an der Stelle t. Für das Ergebnis ist es gleichgültig, ob man zuerst die Determinante berechnet und dann den Wert t einsetzt oder umgekehrt.

b) $f, g \in R[X,Y]$ seien zwei homogene Polynome. Für welche $t \in k$ ist

$$\mathrm{Res}(f,g)(t) = \mathrm{Res}\big(f(t,X,Y), g(t,X,Y)\big) \ ?$$

Lösung: Da f und g in X und Y homogene Polynome sind, sind $f(t,X,Y)$ und $g(t,X,Y)$ auch wieder homogene Polynome derselben Grade – es sei denn, eines oder gar beide verschwinden identisch. Falls weder $f(t,X,Y)$ noch $g(t,X,Y)$ das Nullpolynom ist, haben also die SYLVESTER-Matrizen den gleichen Aufbau, so daß die Gleichung gilt.