Wolfgang K. Seiler
Tel. 2515

B6, B4.18

24. April 2020

8. Übungsblatt Computeralgebra

Aufgabe 1: *(6 Punkte)*
Ordnen Sie die Terme des Polynoms

$$f = 5X^4YZ + 7X^2Y^2Z^2 + 9Y^4Z^2 + 11X^3Y^3 + 13X^5 + 15X^3Z^3 \in \mathbb{Q}[X, Y, Z]$$

der Größe nach

a) für die lexikographische Ordnung

Lösung: Hier kommt es in erster Linie auf den Exponenten von X an; nur wenn zwei Monome den gleichen X-Exponenten haben, müssen wir auch die weiteren betrachten. Die höchste vorkommende X-Potenz ist X^5, also ist $13X^5$ der führende Term. Auch der Exponent vier kommt nur einmal vor, also steht $5X^4YZ$ an zweiter Stelle. X^3 kommt sowohl in X^3Y^3 als auch in X^3Z^3 vor; da Y vor Z kommt, ist $11X^3Y^3$ der drittgrößte und $15X^3Z^3$ der viertgrößte Term. X^2 steht nur in einem Monom, und auch genau ein Monom enthält kein X. Mit lexikographisch angeordneten Monomen ist also

$$f = 13X^5 + 5X^4YZ + 11X^3Y^3 + 15X^3Z^3 + 7X^2Y^2Z^2 + 9Y^4Z^2 .$$

b) für die graduiert lexikographische Ordnung

Lösung: Hier ist der Gesamtgrad eines Monoms das erste Ordnungskriterien; mit Ausnahme von X^5 haben alle vorkommenden Monome den Grad sechs. Diese werden also lexikographisch angeordnet und stehen alle vor X^5. Mit graduiert lexikographisch angeordneten Monomen ist also

$$f = 5X^4YZ + 11X^3Y^3 + 15X^3Z^3 + 7X^2Y^2Z^2 + 9Y^4Z^2 + 13X^5 .$$

c) für die invers lexikographische Ordnung

Lösung: Hier ist der Exponent von Z das erste Ordnungskriterium. Der maximale Exponent ist drei und kommt genau einmal vor. Z^2 steht in $X^2Y^2Z^2$ und Y^4Z^2; wegen des höheren Y-Exponenten kommt Y^4Z^2 als erstes. Linear steht Z nur in $5X^4YZ$, gar nicht in X^3Y^3 und X^5, wobei X^3Y^3 wegen der Y-Potenz zuerst kommt. Geordnet ist also

$$f = 15X^3Z^3 + 9Y^4Z^2 + 7X^2Y^2Z^2 + 5X^4YZ + 11X^3Y^3 + 13X^5 .$$

d) für die graduiert invers lexikographische Ordnung!

Lösung: Hier ist wieder der Grad das erste Ordnungskriterium, d.h. $13X^5$ steht an letzter Stelle. Alle anderen Monome haben Grad sechs; hier ist nun die inverse lexikographische Ordnung maßgebend, allerdings in umgekehrter Reihenfolge. Das Ergebnis ist also

$$f = 11X^3Y^3 + 5X^4YZ + 7X^2Y^2Z^2 + 9Y^4Z^2 + 15X^3Z^3 + 13X^5 .$$

Aufgabe 2: *(5 Punkte)*
Im Polynomring $\mathbb{Q}[X,Y]$ sei

$$f = X^2Y^4 + Y^8 + X^3Y^2 - Y^2 - 6X, \quad f_1 = XY - 2 \quad \text{und} \quad f_2 = Y^3 - 1\,.$$

a) Wenden Sie den Divisionsalgorithmus an auf die Division von f durch f_1, f_2 bezüglich der lexikographischen Ordnung!

Lösung: Die führenden Terme von f_1 und f_2 sind bezüglich jeder Monomordnung XY und Y^3, denn das Monom 1 ist ja bezüglich jeder Monomordnung das kleinste.
Bezüglich der lexikographischen Ordnung ist X^3Y^2 der führende Term von f, denn in keimen anderen Monom kommt X in der dritten oder einer höheren Potenz vor. Er ist teilbar durch XY mit Quotient X^2Y; somit setzen wir

$$p \leftarrow f - X^2Yf_1 = X^2Y^4 + Y^8 - Y^2 - 6X + 2X^2Y \quad \text{und} \quad a_1 \leftarrow X^2Y\,.$$

Der führende Term von p ist X^2Y^4; auch das ist durch XY teilbar, jetzt mit Quotient XY^3, also

$$p \leftarrow p - XY^3f_1 = Y^8 - Y^2 - 6X + 2X^2Y + 2XY^3 \quad \text{und} \quad a_1 \leftarrow a_1 + XY^3 = X^2Y + XY^3\,.$$

Führender Term des neuen p ist $2X^2Y = 2X \cdot XY$, d.h.

$$p \leftarrow p - 2Xf_1 = Y^8 - Y^2 - 2X + 2XY^3 \quad \text{und} \quad a_1 \leftarrow a_1 + 2X = X^2Y + XY^3 + 2X\,.$$

Nun ist $2XY^3 = 2Y^2 \cdot XY$ der führende Term von p, und

$$p \leftarrow p - 2Y^2f_1 = Y^8 + 3Y^2 - 2X \quad \text{und} \quad a_1 \leftarrow a_1 + 2Y^2 = X^2Y + XY^3 + 2X + 2Y^2\,.$$

Führender Term von p ist nun $-2X$, was weder durch XY noch durch Y^3 teilbar ist und damit in den Rest wandert:

$$p \leftarrow p + 2X = Y^8 + 3Y^2 \quad \text{und} \quad r \leftarrow -2X\,.$$

Der führende Term Y^8 ist nicht durch XY teilbar, aber durch Y^3, also subtrahieren wir Y^5f_2:

$$p \leftarrow p - Y^5f_2 = 3Y^2 + Y^5 \quad \text{und} \quad a_2 \leftarrow Y^5\,.$$

Führender Term ist $Y^5 = Y^2 \cdot Y^3$, also

$$p \leftarrow p - Y^2f_2 = 4Y^2 \quad \text{und} \quad a_2 \leftarrow a_2 + Y^2 = Y^5 + Y^2\,.$$

$4Y^2$ ist weder durch XY noch durch Y^3 teilbar, wandert also in den Rest. Dadurch wird p zu Null, und r zu $-2X + 4Y^2$. Das Endergebnis ist also

$$f = a_1f_1 + a_2f_2 + r = (X^2Y + XY^3 + 2X + 2Y^2)f_1 + (Y^5 + Y^2)f_2 + (-2X + 4Y^2)\,.$$

b) Wenden Sie den Divisionsalgorithmus an auf die Division von f durch f_2, f_1 bezüglich der graduiert lexikographischen Ordnung!

Lösung: Nun ist der führende Term von f das Monom mit dem höchsten Grad, also Y^8; an den führenden Termen von f_1 und f_2 ändert sich nichts. Wir dividieren durch f_2, f_1, testen also zunächst f_2, und $Y^8 = Y^5 \cdot Y^3$. Also wird

$$p \leftarrow f - Y^5 f_2 = X^2Y^4 + X^3Y^2 - Y^2 - 6X + Y^5 \quad \text{und} \quad a_2 \leftarrow Y^5 .$$

Der höchste vorkommende Grad ist sechs, und nur X^2Y^4 hat diesen Grad. Der Term ist sowohl durch Y^3 als auch durch XY teilbar; da wir durch f_2, f_1 teilen, verwenden wir f_2:

$$p \leftarrow p - X^2Yf_2 = X^3Y^2 - Y^2 - 6X + Y^5 + X^2Y \quad \text{und} \quad a_2 \leftarrow a_2 + X^2Y = Y^5 + X^2Y .$$

Jetzt haben X^3Y^2 und Y^5 beide den höchsten Grad fünf; da X^3Y^2 lexikographisch größer ist, ist das der führende Term. Er ist nicht durch Y^3 teilbar, aber durch XY, d.h.

$$p \leftarrow p - X^2Yf_1 = -Y^2 - 6X + Y^5 + 3X^2Y \quad \text{und} \quad a_1 \leftarrow X^2Y .$$

Jetzt hat nur noch Y^5 den Grad fünf, ist also führender Term und durch Y^3 teilbar:

$$p \leftarrow p - Y^2 f_2 = -6X + 3X^2Y \quad \text{und} \quad a_2 \leftarrow a_2 + Y^2 = Y^5 + X^2Y + Y^2 .$$

Der führende Term a$3X^2Y$ ist nicht durch Y^3 teilbar, aber durch XY; also subtrahieren wir $3Xf_1$:

$$p \leftarrow p - 3Xf_1 = 0 \quad \text{und} \quad a_1 \leftarrow a_1 + 3X = X^2Y + 3X .$$

Der Divisionsalgorithmus liefert hier also keinen Rest, sondern das Ergebnis

$$f = a_2 f_2 + a_1 f_1 = (Y^5 + X^2Y + Y^2) f_2 + (X^2Y + 3X) f_1 .$$

c) Liegt f im von f_1 und f_2 erzeugten Ideal von $\mathbb{Q}[X, Y]$?

Lösung: Wie *b)* zeigt, läßt sich f als Linearkombination von f_1 und f_2 darstellen, liegt also im Ideal (f_1, f_2).

Aufgabe 3: *(2 Punkte)*
Das Ideal I von $\mathbb{Q}[X_1, \dots, X_n]$ habe die Eigenschaft, daß es mit jedem $f \in I$ auch alle in f vorkommenden Monome enthält. Zeigen Sie: I ist ein monomiales Ideal!

Lösung: Offensichtlich erzeugt dann die Menge aller Monome, die in irgendeinem Polynom aus I vorkommen, das Ideal.

Aufgabe 4: *(3 Punkte)*

$\mathcal{M}$ sei eine nichtleere Menge von Idealen des Polynomrings $k[X_1, \dots, X_n]$ über einem Körper k. Zeigen Sie, daß es in $\mathcal{M}$ ein maximales Element I gibt, d.h. ein Ideal I, das in keinem Ideal $J \in \mathcal{M}$ echt enthalten ist!

Hinweis: Zeigen Sie, daß es sonst eine unendliche echt aufsteigende Folge von Idealen gäbe, und wenden Sie den HILBERT*schen Basissatz an auf die Vereinigung dieser Ideale.*

Lösung: Falls es kein maximales Element in M gibt, können wir zu jedem Ideal $I \in M$ ein Ideal $J \in M$ finden, in dem I echt enthalten ist. Somit gibt es eine unendliche aufsteigende Folge

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

von Idealen in M. Die Vereinigung alle I_ν ist ein Ideal von $k[X_1, \dots, X_n]$, das nach dem HILBERTschen Basissatz ein endliches Erzeugendensystem $f_1, \dots, f_r$ hat. Jedes f_r liegt in einem Ideal I_{ν_r}, und da I_ν in allen I_μ mit $\mu \geq \nu$ liegt, liegen somit für $\nu = \max\{\nu_1, \dots, \nu_r\}$ alle f_r in I_ν. Da I die Vereinigung aller I_μ ist, liegt dann *jedes* Ideal I_μ in I_ν, im Widerspruch zur Annahme, daß I_ν eine echte Teilmenge von $I_{\nu+1}$ ist. Somit muß M ein maximales Element enthalten.

Aufgabe 5: *(4 Punkte)*

Die Ordnungsrelation $<$ auf $\mathbb{N}_0^n$ erfülle die ersten beiden Bedingungen an eine Monomordnung und zusätzlich gelte, daß $(0, \dots, 0)$ das kleinste Element von $\mathbb{N}_0$ ist.

a) Zeigen Sie: Ist X^α ein Teiler von X^β, so ist $X^\alpha \leq X^\beta$ im Sinne dieser Ordnung.

Lösung: Ist X^α ein Teiler von X^β, so gibt es ein Monom X^γ, für das $X^\beta = X^\alpha \cdot X^\gamma$ ist. Aus $(0, \dots, 0) \leq \gamma$ folgt wegen der zweiten Eigenschaft einer Monomordnung, daß

$$\alpha = \alpha + (0, \dots, 0) \leq \alpha + \gamma = \beta$$

omit ist $X^\alpha \leq X^\beta$,

b) Folgern Sie aus dem Lemma von DICKSON, daß $<$ eine Monomordnung ist!

Lösung: Da die ersten beiden Bedingungen erfüllt sind, muß nur die dritte nachgewiesen werden, also daß jede nichtleere Menge M von Monomen ein kleinstes Element enthält. Dazu sei I das von den Monomen aus M erzeugte Ideal; nach dem Lemma von DICKSON hat es ein endliches Erzeugendensystem $\{u_1, \dots, u_r\}$, wobei alle u_i in M liegen. Somit ist jedes Monom aus M teilbar durch mindestens eines der u_i. Nach *a)* ist deshalb jedes Monom aus M größer oder gleich einem der u_i.

Die endliche Menge $\{u_1, \dots, u_r\}$ hat natürlich ein kleinstes Element; dieses sei u_j. Dann ist u_j kleiner oder gleich jedem Monom aus M, also das kleinste Element von M.