Aufgabe (38).

(a) *Seien $R = K[x]$ Polynomring in einer Variablen über dem Körper K, $f_1, \ldots, f_s \in R$, $I = \langle f_1, \ldots, f_r \rangle_R$ und $g = \mathsf{ggT}(f_1, \ldots, f_s)$. Zeigen Sie:*

$\{g\}$ ist die einzige reduzierte Gröbnerbasis von I.

(b) *Seien $s, n \in \mathbb{N}_{\geq 1}$ und $R = K[x_1, \ldots, x_n]$ Polynomring in n Variablen über dem Körper K, $A \in K^{s \times n}$ eine obere Dreiecksmatrix mit 1-en in der Diagonalen,*

$$\begin{bmatrix} f_1 \\ \vdots \\ f_s \end{bmatrix} = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

und $I = \langle f_1, \ldots, f_s \rangle_R$. Zeigen Sie:

$\{f_1, \ldots, f_s\}$ ist bei geeigneter Anordnung der Variablen eine minimale $\leq_{\text{lex}}$-Gröbnerbasis für das Ideal I.

Wie muss A dann zusätzlich noch aussehen, damit eine reduzierte Gröbnerbasis ensteht?[1]

Zu (a). Nach §18 Beispiel 6 gibt es in Polynomringen mit einer Variablen nur genau eine Monomordnung. Wir werden im Folgenden also die Ordnung nicht weiter angeben. Zusätzlich werden wir annehmen, dass $I \neq \{0\}$ gilt.[2]

Sei $G := \{g\}$. Wir wissen aus Algebra I, dass

$$I = \langle f_1, \ldots, f_s \rangle_R = Rf_1 + \ldots + Rf_s = R\,\mathsf{ggT}(f_1, \ldots, f_s) = Rg = \langle g \rangle_R$$

gilt. Also erzeugt G das Ideal I. Weiterhin gelten $\mathsf{S}(g, g) = 0$ und somit auch $\overline{\mathsf{S}(g,g)}^G = 0$. Damit ist G nach dem Buchbergerkriterium (§21 Satz 2) eine Gröbnerbasis von $I = \langle g \rangle$. Da $\langle G \setminus \{g\} \rangle = \langle \varnothing \rangle = 0 \neq I$ gilt, ist G auch eine minimale Gröbnerbasis nach der Definition 11(a) in §20.

Nach einer Konvention dieser Vorlesung sind größte gemeinsame Teiler in R stets normiert. Es gilt also auch $\mathsf{LK}(g) = 1$. Schließlich ist

$$\overline{g}^{G \setminus \{g\}} = \overline{g}^{[\ ]} = g,$$

und folglich ist nach §20 Definition 11(b) G eine reduzierte Gröbnerbasis von I.[3]

Nach §20 Satz 13(b) besitzt jedes Ideal genau eine reduzierte Gröbnerbasis bezüglich einer gegebenen Monomordnung. Da im Falle einer Variablen überhaupt nur eine Monomordnung zur Verfügung steht, ist G also die einzige, eindeutig bestimmte reduzierte Gröbnerbasis von I.

Zu (b). Wir betrachten zunächst den Fall $s = n$. Zunächst haben wir zu beweisen, dass $F := [f_1, ..., f_s]$ eine Gröbnerbasis von I ist. Also Monomordnung wählen wir dabei die lexikographische Ordnung mit mit $x_1 > \ldots > x_n$. Nachfolgend werden zwei Beweisvarianten angeboten.

Variante A. Für ein f aus $I \setminus \{0\}$ mit erhält man mit dem Divisionsalgorithmus Polynome $a_1, \ldots, a_s$ und $r \in R$ mit

$$f = a_1 f_1 + \ldots + a_s f_s + r,$$

[1] Für die Bearbeitung der Aufgabe war es als Vereinfachung erlaubt, $n = s$ anzunehmen.

[2] Die einzige reduzierte Gröbnerbasis des Nullideals ist die leere Menge $\varnothing$.

[3] Hierbei bezeichnet $[\ ]$ die *leere Liste*.

die den Bedingungen aus §19 Satz 1 genügen. Es wird also kein Term von r durch einen Leitterm eines f_j geteilt. Da $\mathsf{LM}(f_i) = x_i$ ist, folgt somit $r \in K$.

Man sieht sofort, dass 0 eine gemeinsame Nullstelle von $f_1, \ldots, f_s$ ist. Damit muss wegen $f \in I$ auch $f(0) = 0$ gelten, und es folgt $r = 0$. Da dann $\mathsf{LM}(f) = \mathsf{LM}(a_i f_i) = \mathsf{LM}(a_i)x_i$ für ein i gelten muss, folgt $\mathsf{LM}(f) \in \langle x_1, \ldots, x_s \rangle$. Also gilt

$$\mathsf{in}_{\leq} I = \langle x_1, \ldots, x_s \rangle = \langle \mathsf{LM}(f_1), \ldots, \mathsf{LM}(f_s) \rangle.$$

Nach §20 Definition 6 ist F also eine Gröbnerbasis von I bezüglich der gewählten Ordnung.

Variante B. Wir wählen die Monomordnung wie in der vorigen Beweisvariante. Für $1 \leq i \leq s$ ist $\mathsf{LM}(f_i) = x_i$. Das von den Leitmonomen ausgespannte Ideal ist also $J := \langle x_1, ...x_s \rangle$.

Wegen $F \subseteq I$ gilt $J \subseteq \mathsf{in}_{\leq} I$. Nun ist J ein maximales Ideal.[4] Es folgt also $J = \mathsf{in}_{\leq} I$ oder $\mathsf{in}_{\leq} I = R$.

Wie man leicht sieht, ist $0 \in \mathscr{V}(f_1, \ldots, f_s) = \mathscr{V}(I)$. Es folgt insbesondere $1 \notin I$. Damit kann 1 aber auch kein Leitterm sein, also folgt $1 \notin \mathsf{in}_{\leq} I$. Somit ist $\mathsf{in}_{\leq} I \neq R$ und es folgt $\mathsf{in}_{\leq} I = J$. Nach §20 Definition 6 ist F folglich eine Gröbnerbasis von I bezüglich der gewählten Ordnung.

Variante C. Wie untem im allgemeinen Fall (zweiter Absatz) bewiesen wird, ist F genau dann eine Gröbnerbasis von I, wenn $X := [x_1, \ldots, x_s]$ es ist. Da $I = \langle x_1, \ldots, x_s \rangle$ ein Monomideal ist, folgt dies bereits mit §20 Beispiel 8(i).

Allgemeiner Fall. Wir nehmen nun an, dass $n \geq s$ gilt.[5] Das bedeutet, dass A die Gestalt

$$A = \begin{array}{c} \begin{bmatrix} 1 & & * & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * \\ & \ddots & & \ddots & & & & & & & & & & & \vdots \\ 0 & & \ddots & & \ddots & & & & & & & & & & \vdots \\ \vdots & & & \ddots & & \ddots & & & & & & & & & \vdots \\ \vdots & & & & \ddots & & \ddots & & & & & & & & \vdots \\ \vdots & & & & & \ddots & & \ddots & & & & & & & \vdots \\ \vdots & & & & & & \ddots & & \ddots & & & & & & \vdots \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & & 1 & & * & \cdot & \cdot & \cdot & \cdot & * \end{bmatrix} \\ \underbrace{\qquad\qquad\qquad\qquad}_{s \text{ Spalten}} \quad \underbrace{\qquad\qquad}_{n-s \text{ Spalten}} \end{array}$$

besitzt, wobei die $*$ für unspezifizierte Einträge (aus K) stehen. Wir wählen eine als Anordnung der Variablen $x_1 > x_2 > \ldots > x_n$.

Für jede invertierbare Matrix $M \in K^{s \times s}$ derart, dass MA eine obere Dreiecksmatrix ist, sind die Einträge von

$$\begin{bmatrix} g_1 \\ \vdots \\ g_s \end{bmatrix} := (MA) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

genau dann eine Gröbnerbasis, wenn $F = [f_1, \ldots, f_n]$ es ist: Wir setzen als Abkürzung $x := {}^t[x_1, \ldots, x_n]$ und $G := [g_1, \ldots, g_s]$. Die Zeilenumformungen ändern nicht den Aufspann von Ax, denn es gilt

$$R^{1 \times n} Ax = R^{1 \times n} M^{-1} MAx = R^{1 \times n}(MA)x.$$

Also ist $I = \langle F \rangle_R = \langle G \rangle_R$. Weiterhin sind die Leitmonome von F und diejenigen von G jeweils $x_1, \ldots, x_s$, denn sowohl A als auch MA sind obere Dreiecksmatrizen. Also erzeugen die Leitmonome von F genau dann das Anfangsideal, wenn diejenigen von G es tun.

[4] Das Ideal J ist maximal, da $R/J \cong K$ ein Körper ist. Eine andere Art dies einzusehen, ist es analog zu der ersten Variante den Divisionsalgorithmus zu betrachten, denn $x_1, \ldots, x_s$ ist eine Gröbnerbasis von J nach §20 Beispiel 8(i).

[5] Im Falle $n < s$ enthalten die unteren $n - s$ Zeilen von A nur Nullen, und die Polynome $f_{n+1}, \ldots, f_s$ wären ebenfalls Null. Das bedeutet aber, dass sie bei der Betrachtung der Gröbnerbasis-Eigenschaft ignoriert werden können. Weiterhin ist der Fall $n = s$ hier bereits enthalten.

Da es eine invertierbare Matrix M gibt, derart, dass MA die folgende Gestalt hat

$$\begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & * & \cdot & \cdot & \cdot & * \\ & \ddots & & & & & \vdots & \vdots & & & & \vdots \\ 0 & & \ddots & & & & \vdots & \vdots & & & & \vdots \\ \vdots & & & \ddots & & & \vdots & \vdots & & & & \vdots \\ \vdots & & & & \ddots & & \vdots & \vdots & & & & \vdots \\ \vdots & & & & & \ddots & 0 & \vdots & & & & \vdots \\ \vdots & & & & & & \ddots & \vdots & & & & \vdots \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & * & \cdot & \cdot & \cdot & * \end{bmatrix}, \tag{1}$$

können wir ab jetzt o.E. annehmen, dass bereits A die Gestalt (1) hat.

Wir betrachten nun die S-Polynome. Seien $1 \leq i < j \leq s$. Wegen der Gestalt von A sind dann $f_i = x_i + \tilde{f}_i$ und $f_j = x_j + \tilde{f}_j$, wobei $\tilde{f}_i$ und $\tilde{f}_j$ in $\langle x_{s+1}, \ldots, x_n \rangle_K$ sind. Damit ist

$$\mathsf{S}_{\leq}(f_i, f_j) = x_j \tilde{f}_i - x_i \tilde{f}_j,$$

denn alle Monome in $x_j \tilde{f}_i$ werden von x_j geteilt aber nicht von x_i und alle Monome in $x_i \tilde{f}_j$ werden von x_i aber nicht von x_j geteilt. Das Leitmonom ist aufgrund der gewählten Ordnung $x_i \cdot \mathsf{LM}(\tilde{f}_j)$.

Sei $\tilde{f}_j = \sum_{k=s+1}^{n} c_k x_k$, wobei wir ohne Einschränkung annehmen können, dass $c_{s+1} \neq 0$ gilt. Dann ist der Leitterm von $\mathsf{S}_{\leq}(f_i, f_j)$ also $-c_{s+1} x_i x_{s+1}$. Dies ist durch das Leitmonom x_i von f_i teilbar, aber duch kein Leitmonom eines f_k mit $k < i$. Also ist der erste Reduktionsschritt im Divisionsalgorithmus der Vorlesung

$$\mathsf{S}_{\leq}(f_i, f_j) = -\sum_{k=s+1}^{n} c_k x_i x_k \ + \ x_j \tilde{f}_i \text{ wird zu } -\sum_{k=s+2}^{n} c_k x_i x_k \ + \ c_{s+1} x_{s+1} \tilde{f}_i + x_j \tilde{f}_i.$$

Keiner der Terme von $c_{s+1} x_{s+1} \tilde{f}_i$ wird durch x_i geteilt, also ist der neue Leitterm $-c_{s+2} x_i x_{k+2}$. Dieses wird wieder durch das Leitmonom von f_i geteilt aber durch kein vorangegangenes.

Man sieht nun ein, dass der Divisionsalgorithmus genau so fortfährt, bis das Zwischenergebnis

$$\mathsf{S}_{\leq}(f_i, f_j) \text{ wird reduziert zu } \tilde{f}_j \tilde{f}_i + x_j \tilde{f}_i$$

erreicht ist. Hier ist das neue Leitmonom $x_j \cdot \mathsf{LM}(\tilde{f}_j)$. Vollkommen analog reduziert sich das S-Polynom also weiter zu

$$\mathsf{S}_{\leq}(f_i, f_j) \text{ wird zu } \tilde{f}_j \tilde{f}_i - \tilde{f}_j \tilde{f}_i = 0.$$

Ist $i = j$, so ist $\mathsf{S}(f_i, f_j) = 0$. Ist $i > j$, dann gilt $\mathsf{S}(f_i, f_j) = -\mathsf{S}(f_j, f_i) \xrightarrow{F}_{+} 0$ nach dem ersten Fall, da hier die Vorzeichen der Koeffizienten und des Restes bei der Multidivision durch F sich einfach jeweils umdrehen. Also gilt

$$\overline{\mathsf{S}_{\leq}(f_i, f_j)}^{F} = 0$$

für beliebige i und j. Nach dem Buchbergerkriterium (§21 Satz 2), ist F also eine Gröbnerbasis.

Wir beweisen nun, dass F eine minimale Gröbnerbasis ist. Sei dazu $1 \leq i \leq n$ Zu zeigen ist, dass $\langle F \setminus \{f_i\} \rangle \neq \langle F \rangle = I$ ist.

Analog zu dem obigen Beweis zeigt man, dass $F \setminus \{f_i\}$ eine Gröbner-Basis von $J := \langle F \setminus \{f_i\} \rangle$ ist. Hierbei wählen wir eine $\leq_{\text{lex}}$-Ordnung mit $x_1 > \ldots > x_{i-1} > x_{i+1} > \ldots > x_s > x_i > x_{s+1} > \ldots > x_n$. Man sieht nun, dass bei Anwendung des Divisionsalgorithmus auf die S-Polynome die obige Argumentation direkt übertragbar ist. Weiterhin ist (bezüglich dieser Ordnung) der Rest von f_i bei Division durch $F \setminus \{f_i\}$ nicht Null, da er zumindest den Term x_i enthält. Also ist $\langle F \setminus \{f_i\} \rangle \neq I$ für jedes i und F somit eine minimale Gröbnerbasis.

Alle Polynome in F sind normiert bezüglich der gewählten Ordnung. Nach §20 Bemerkung 12 ist F eine reduzierte Gröbnerbasis, wenn für alle i kein Term von f_i durch den Leitterm eines f_j mit

$j \neq i$ geteilt wird. Da die Leitterme von $F \setminus \{f_i\}$ gerade $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_s$ sind, bedeutet dies, dass keines dieser Monome in f_i vorkommen darf. Das wiederum ist gleichbedeutend damit, dass $a_{ij} = 0$ ist für $i \neq j$. Also ist F genau dann eine reduzierte Gröbnerbasis, wenn

$$A = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & * & \cdot & \cdot & \cdot & * \\ & \cdot & \cdot & & \cdot & & \cdot & \cdot & & & & \cdot \\ 0 & & \cdot & \cdot & & \cdot & \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & \cdot & \cdot & & \cdot & \cdot & & & & \cdot \\ \cdot & & \cdot & & \cdot & \cdot & \cdot & \cdot & & & & \cdot \\ \cdot & & & \cdot & & \cdot & 0 & \cdot & & & & \cdot \\ \cdot & & & & \cdot & & \cdot & \cdot & & & & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & * & \cdot & \cdot & \cdot & * \end{bmatrix}$$

gilt.