# 1. Übungsblatt zu Computeralgebra II, SS 1996

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Do, 2. 5. 1996 in der Vorlesung

**Aufgabe 1 (Inhalt und primitiver Teil)** *(6 Punkte)*

*Wir betrachten den Ring* $R = \mathbb{Z}[\frac{1}{2}] = \{\frac{z}{2^n} : z \in \mathbb{Z}, n \in \mathbb{N}\}$.

*i.* *Zeige, daß* $R$ *der kleinste Unterring von* $\mathbb{Q}$ *ist, der* $\mathbb{Z}$ *und* $\frac{1}{2}$ *enthält.*

*ii.* *Welches sind die Einheiten von* $R$ *(Beweis)?*

*iii.* $R$ *ist ein faktorieller Ring, und damit haben auch je zwei Elemente* $a, b \in R$ *einen ggT (das braucht nicht gezeigt werden). Dieser ist jedoch nur bis auf Einheiten bestimmt. Wähle aus allen möglichen ggTs von* $a$ *und* $b$ *einen "kanonischen" Vertreter aus. Dieser sei im Folgenden mit* $\mathrm{ggT}(a,b)$ *bezeichnet. Dabei sollte* $\mathrm{ggT}(a,b) = 1$ *gelten, wenn alle ggTs von* $a$ *und* $b$ *Einheiten sind. Analog zur Vorlesung wird der Inhalt eines Polynoms* $f = \sum_{0 \leq i \leq n} f_i x^i \in R[x]$ *als* $\mathrm{cont}(f) = \mathrm{ggT}(f_0, f_1, \ldots, f_n)$ *definiert, und der primitive Teil durch* $\mathrm{cont}(f) \cdot \mathrm{pp}(f) = f$. $f$ *heißt primitiv, falls* $\mathrm{cont}(f) = 1$ *gilt.*

*iv.* *Bestimme Inhalt und primitiven Teil des Polynoms* $f = 2x^2 + 6x - 4$ *bezüglich* $\mathbb{Z}$, $R$ *und* $\mathbb{Q}$. *Ist* $f$ *primitiv bzgl.* $R$*?*

**Aufgabe 2 (Division mit Rest durch normierte Polynome)** *(4 Punkte)*

*Sei* $R$ *ein Ring. Zeige:*

*i.* *Für Polynome* $f, g \in R[x]$ *mit* $g \neq 0$ *und* $g$ *normiert gibt es Polynome* $q, r \in R[x]$ *mit* $f = qg + r$ *und* $\deg r < \deg g$. *Hinweis: Induktion über* $\deg f - \deg g$.

*ii.* *Der Quotient* $q$ *und der Rest* $r$ *aus Teilaufgabe i. sind eindeutig bestimmt.*

*iii.* *Sind* $f, g, q, r$ *wie in i. und* $m \in R$ *mit* $m \mid f$, *so gilt* $m \mid q$ *und* $m \mid r$. *Hinweis: Induktion über* $\deg f - \deg g$.

**Aufgabe 3 (Hensel Lifting in $\mathbb{Z}[x]$)** *(7 Punkte)*

*Sei* $f = 14x^4 + 15x^3 + 42x^2 + 3x + 1 \in \mathbb{Z}[x]$.

i. *Finde eine geeignete Primzahl* $p$*, so daß* $f$ *modulo* $p$ *quadratfrei ist und denselben Grad wie* $f$ *hat.*

ii. *Berechne die Zerlegung von* $f$ *modulo* $p$ *in irreduzible Faktoren. Wähle daraus eine Faktorisierung* $f \equiv g_1 h_1 \bmod p$ *mit modulo* $p$ *teilerfremden Polynomen* $g_1, h_1 \in \mathbb{Z}[x]$, $h_1$ *normiert und irreduzibel modulo* $p$*. Bestimme* $s, t \in \mathbb{Z}[x]$ *mit* $sg_1 + th_1 \equiv 1 \bmod p$.

iii. *Führe die ersten zwei Schritte des Hensel-Lifting aus, d.h. berechne* $g_i, h_i \in \mathbb{Z}[x]$ *mit* $f \equiv g_i h_i \bmod p^i$ *für* $i = 2, 3$ *mit Hilfe der Regel*

$$\begin{aligned} e_{i-1} &\equiv f - g_{i-1}h_{i-1} \bmod p^i, \\ g_i &\equiv g_{i-1} + te_{i-1} \bmod p^i, \\ h_i &\equiv h_{i-1} + se_{i-1} \bmod p^i. \end{aligned}$$

*Was fällt auf?*

iv. *Führe die ersten drei Schritte des Hensel-Lifting mit der verbesserten Regel*

$$\begin{aligned} e_{i-1} &\equiv f - g_{i-1}h_{i-1} \bmod p^i, \\ q_{i-1} &\equiv se_{i-1} \text{ quo } h_{i-1} \bmod p^i, \\ g_i &\equiv g_{i-1} + te_{i-1} + g_{i-1}q_{i-1} \bmod p^i, \\ h_i &\equiv h_{i-1} + se_{i-1} - h_{i-1}q_{i-1} \bmod p^i \end{aligned}$$

*durch (dabei bezeichnet "quo" den Quotienten bei Division mit Rest). Läßt sich daraus eine Faktorisierung von* $f$ *über* $\mathbb{Z}$ *ableiten?*

*Für die Zwischenrechnungen darf ein Computeralgebrasystem verwendet werden.*

Hinweis: Bei der Verwendung von Computeralgebrasystemen bitte immer den Quelltext oder ein Ablaufprotokoll (z.B. Maple-„worksheet“) mit abgeben.

# 2. Übungsblatt zu Computeralgebra II, SS 1996

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Do, 9. 5. 1996 in der Vorlesung

**Aufgabe 4 (Gram-Schmidt Orthogonalisierung)** *(3 Punkte)*

*Die Gram-Schmidt-Orthogonalbasis (GSO) $b_1^*, \ldots, b_n^* \in \mathbb{R}^n$ zu einer gegebenen Basis $b_1, \ldots, b_n \in \mathbb{R}^n$ ist – wie in der Vorlesung – durch*

$$\begin{aligned} b_i^* &= b_i - \sum_{1 \le i < j} \mu_{i,j} b_j^* \text{ für } 1 \le i \le n, \\ \mu_{i,j} &= \frac{< f_i, f_j^* >}{< f_j^*, f_j^* >} \text{ für } 1 \le j < i \le n \end{aligned}$$

*definiert.*

i. *Zeige, daß $b_1^*, \ldots, b_n^*$ tatsächlich eine Orthogonalbasis ist, d.h. $< b_i^*, b_j^* > = 0$ für $1 \le j < i \le n$.*

ii. *Berechne die GSO von*

$$(22, 11, 5),\ (13, 6, 3),\ (-5, -2, -1) \in \mathbb{R}^3.$$

**Aufgabe 5 (Kurze Vektoren in $\mathbb{Z}^3$)** *(4 Punkte)*

*Berechne mit dem Algorithmus aus der Vorlesung eine reduzierte Basis des von*

$$(22, 11, 5),\ (13, 6, 3),\ (-5, -2, -1)$$

*erzeugten Gitters in $\mathbb{Z}^3$. Zwischenrechnungen dürfen mit einem Computeralgebrasystem durchgeführt werden.*

**Aufgabe 6 (Gitter in $\mathbb{R}^n$)** *(3 Punkte)*

*Seien $g_1, \ldots, g_n \in \mathbb{R}^n$ linear unabhängig und $M = \sum_{1 \le i \le n} \mathbb{Z} g_i$ das erzeugte Gitter. Beweise die folgende Aussage:*

*Zu jedem Vektor $x \in \mathbb{R}^n$ gibt es ein $g \in M$ mit*

$$\|x - g\|^2 \le \frac{1}{4}(\|g_1\|^2 + \cdots + \|g_n\|^2).$$

*Hinweis: Induktion über $n$. Für den Induktionsschritt bestimme $\lambda \in \mathbb{Z}$ geeignet, so daß der Vektor $x - \lambda g_n$ minimalen Abstand zu der von $g_1, \ldots, g_{n-1}$ aufgespannten Hyperebene hat.*

<u>Hinweis:</u> Bei der Verwendung von Computeralgebrasystemen bitte immer den Quelltext oder ein Ablaufprotokoll (z.B. Maple-„worksheet“) mit abgeben.

# 3. Übungsblatt zu Computeralgebra II, SS 1996

JOACHIM VON ZUR GATHEN, JÜRGEN GERHARD

Abgabe: Di, 21. 5. 1996 in der Vorlesung

**Aufgabe 7 (Gram-Schmidt-Orthogonalbasen)** *(3 Punkte)*

*Seien $g_1, \ldots, g_n \in \mathbb{R}^n$ linear unabhängig und $g_1^*, \ldots, g_n^*$ die zugehörige Gram-Schmidt-Orthogonalbasis mit*

$$g_i^* = g_i - \sum_{1 \le j < i} \mu_{ij} g_j^* \text{ für } 1 \le i \le n.$$

*Definiere $h_1, \ldots, h_n \in \mathbb{R}^n$ durch*

$$\begin{aligned} h_k &= g_k \text{ für } 1 \le k < n-1, \\ h_{n-1} &= g_n, \\ h_n &= g_{n-1}, \end{aligned}$$

*und sei $h_1^*, \ldots, h_n^* \in \mathbb{R}^n$ die zugehörige Gram-Schmidt-Orthogonalbasis. Zeige, daß*

$$h_n^* = \frac{|g_n^*|^2 g_{n-1}^* - \mu_{n,n-1} |g_{n-1}^*|^2 g_n^*}{|g_n^*|^2 + \mu_{n,n-1}^2 |g_{n-1}^*|^2}$$

*gilt. Die bereits bewiesenen Aussagen aus der Vorlesung dürfen dabei verwendet werden. Hinweis: $h_n^*$ ist die Projektion von $h_n$ auf $\operatorname{span}\{h_1, \ldots, h_{n-1}\}^\perp$.*

**Aufgabe 8 (Swinnerton-Dyer-Polynome)** *(6 Punkte)*

*Berechne (ohne Verwendung eines Computeralgebrasystems) die Koeffizienten des Swinnerton-Dyer-Polynoms*

$$f = (x + \sqrt{-1} + \sqrt{2})(x + \sqrt{-1} - \sqrt{2})(x - \sqrt{-1} + \sqrt{2})(x - \sqrt{-1} - \sqrt{2}) \in \mathbb{Z}[x]$$

*und die Faktorisierungen von $f \bmod p$ in irreduzible Faktoren für $p = 2, 3, 5$. Beweise, daß $f$ irreduzibel ist.*

**Aufgabe 9 (Knapsack-Kryptosystem)** *(6 Punkte)*

*Wir betrachten das folgende public-key Kryptosystem.*

1. *Geheimer Schlüssel:* $c_1, \ldots, c_6, m, w \in \mathbb{N}$ *mit* $c_{i+1} \geq 2c_i$ *für* $1 \leq i \leq 5$, $m > \sum_{1 \leq i \leq 6} c_i$ *und* $\mathrm{ggT}(w, m) = 1$.

2. *Öffentlicher Schlüssel:* $a_i = (wc_i \text{ rem } m) \in \mathbb{N}$ *für* $i = 1, \ldots, 6$.

3. *Verschlüsseln: Eine Nachricht* $x = (x_1, \ldots, x_6) \in \{0,1\}^6$ *wird in den Chiffretext* $s = \sum_{1 \leq i \leq 6} x_i a_i \in \mathbb{N}$ *überführt.*

4. *Entschlüsseln: Berechne* $t \in \mathbb{N}$ *mit* $t \equiv w^{-1} s \bmod m$ *und* $0 \leq t < m$. *Dann ist* $t = \sum_{1 \leq i \leq 6} x_i c_i \in \mathbb{N}$. *Rekonstruiere daraus* $x_1, \ldots, x_6$.

i. *Führe eine Ver- und Entschlüsselung mit den Daten* $c_1 = 3$, $c_{i+1} = 2c_i + 1$ *für* $1 \leq i \leq 5$, $m = 257$, $w = 217$ *und* $x = (1, 0, 0, 1, 0, 1)$ *durch.*

ii. *Beweise, daß in Schritt 4 tatsächlich* $t = \sum_{1 \leq i \leq 6} x_i c_i$ *gilt.*

iii. *Jetzt bist Du ein/e Einbrecher/in und kennst nur den öffentlichen Schlüssel und den Chiffretext. Versuche, daraus mit Hilfe von Gitterbasisreduktion für die folgenden drei Beispiele die jeweiligen Originalnachrichten herauszubekommen (das muß nicht immer klappen):*

| $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ | $a_6$ | $s$ |
|---|---|---|---|---|---|---|
| 3810 | 3774 | 3702 | 3558 | 3270 | 2694 | 10746 |
| 3810 | 3774 | 3702 | 3558 | 3270 | 2694 | 11070 |
| 3810 | 3774 | 3702 | 3558 | 3270 | 2694 | 17034 |

*Für die Lösung darf ein Computeralgebrasystem zu Hilfe genommen werden.*

Hinweis: Bei der Verwendung von Computeralgebrasystemen bitte immer den Quelltext oder ein Ablaufprotokoll (z.B. Maple-„worksheet“) mit abgeben.

# 4. Übungsblatt zu Computeralgebra II, SS 1996

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Di, 4. 6. 1996 in der Vorlesung

**Aufgabe 10 (Kosten des Faktorisierungsalgorithmus)** *(2 Punkte)*

*Zeige, daß Schritt 5 des Algorithmus aus der Vorlesung zum Faktorisieren eines primitiven quadratfreien Polynoms $n$-ten Grades $f \in \mathbb{Z}[x]$ mit $O^{\sim}(n^{12} + n^{10} \log^2 |f|)$ Bitoperationen durchgeführt werden kann. Verwende dazu folgende Abschätzung: Ein „kurzer" Vektor $u$ in dem von $f_1, \ldots, f_n \in \mathbb{Z}^n$ erzeugten Gitter $L \subseteq \mathbb{Z}^n$ mit $|u| \leq 2^{(n-1)/2} \min\{|v| : 0 \neq v \in L\}$ kann mit $O^{\sim}(n^8 \log^2 A_0)$ Bitoperationen berechnet werden, wobei $A_0 = \max\{|f_i| : 1 \leq i \leq n\}$ ist.*

**Aufgabe 11 (Nichtpotenzen)** *(4 Punkte)*

*Betrachte den folgenden Algorithmus zum Wurzelziehen.*

**Algorithmus** *Ganzzahlige Wurzeln.*
*Eingabe: $k, N \in \mathbb{N}$ mit $3 \leq k < N$ und $k, N$ ungerade.*
*Ausgabe: Eine $k$-te Wurzel von $N$ in $\mathbb{N}$, falls eine solche existiert, andernfalls „FAIL".*

1. *Setze $h_0 = 1$ und $l = \lceil \log_2 \log_2 N \rceil$.*
2. *Wiederhole Schritt 3 für $i = 1, \ldots, l$.*
3. *Berechne $h_i \in \{0, \ldots, 2^{2^i} - 1\}$ mit*
$$h_i \equiv h_{i-1} - (h_{i-1}^k - N)(k h_{i-1}^{k-1})^{-1} \bmod 2^{2^i}.$$
4. *Falls $h_l^k = N$, gib $h_l$ aus, andernfalls „FAIL".*

i. *Zeige, daß der Algorithmus mit $O(\mathsf{M}(n) \log k)$ Bitoperationen auskommt, wenn $n$ die Bitlänge von $N$ ist. Verwende dabei, daß Multiplikationen modulo $2^t$ mit $\mathsf{M}(t) \in O(t \log t \operatorname{loglog} t)$ Bitoperationen und Inversionen modulo $2^t$ mit $O(\mathsf{M}(t))$ Bitoperationen durchgeführt werden können.*

ii. *Eine Zahl $N \in \mathbb{N}_{\geq 2}$ heiße* Nichtpotenz, *wenn sie sich nicht in der Form $N = M^k$ mit $k, M \in \mathbb{N}$ und $k \geq 2$ schreiben läßt. Entwirf auf Basis der obigen Prozedur ein Verfahren, das den Nichtpotenz-Anteil einer ungeraden Zahl $N \in \mathbb{N}_{\geq 3}$, die keine Quadratzahl ist, berechnet, d.h. eine Nichtpotenz $M \in \mathbb{N}$ und eine ungerade Zahl $k \in \mathbb{N}$ mit $N = M^k$. Dein Algorithmus sollte höchstens $O(n \cdot \mathsf{M}(n) \log n)$ Bitoperationen benötigen (wobei $n$ wieder die Bitlänge von $N$ ist); zeige dies.*

*Freiwillige Zusatzaufgabe: Was macht man im Fall einer Quadratzahl?*

# 5. Übungsblatt zu Computeralgebra II, SS 1996

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Do, 13. 6. 1996 in der Vorlesung

**Aufgabe 12 (Pollards $\rho$-Methode)** *(3 Punkte)*

*Faktorisiere die Zahl $N = 297705193373077561$ mit Pollards $\rho$-Methode. Für die Zwischenrechnungen darf ein Computeralgebrasystem verwendet werden.*

**Aufgabe 13 (Quadratisches Sieb)** *(4 Punkte)*

*Faktorisiere die Zahl $N = 276121$ mit dem Quadratischen Sieb. Verwende dazu die Faktorbasis $B = \{3, 5, 7, 11\}$. Für Zwischenrechnungen darf ein Computeralgebrasystem verwendet werden.*

**Aufgabe 14 (Monomordnungen)** *(4 Punkte)*

i. *Zeige, daß $\prec = \prec_{\mathrm{grlex}}$ eine Monomordnung ist, d.h.*

   - $\alpha \prec \beta$ *und* $\beta \prec \gamma \Longrightarrow \alpha \prec \gamma$ *($\prec$ ist transitiv),*
   - $(\alpha \prec \beta) \vee (\beta \prec \alpha)$ *falls* $\alpha \neq \beta$ *($\prec$ ist total),*
   - $\alpha \prec \beta \Longrightarrow \alpha + \gamma \prec \beta + \gamma$

   *gilt für alle $\alpha, \beta, \gamma \in \mathbb{N}^n$, und*

   - *jede nichtleere Teilmenge von $\mathbb{N}^n$ besitzt ein bzgl. $\prec$ kleinstes Element (Wohlordnungseigenschaft).*

   *Dabei darf verwendet werden, daß $\prec_{\mathrm{lex}}$ eine Monomordnung ist.*

ii. *Beweise oder widerlege: Die Relation $\prec_{\mathrm{invlex}}$, die durch $\alpha \prec_{\mathrm{invlex}} \beta \Longleftrightarrow \beta \prec_{\mathrm{lex}} \alpha$ definiert wird, ist eine Monomordnung.*

<u>Hinweis:</u> Bei der Verwendung von Computeralgebrasystemen bitte immer den Quelltext oder ein Ablaufprotokoll (z.B. Maple-„worksheet“) mit abgeben.

# 6. Übungsblatt zu Computeralgebra II, SS 1996

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Do, 20. 6. 1996 in der Vorlesung

**Aufgabe 15 (Eigenschaften des Multigrads)** *(3 Punkte)*

*Seien $F$ ein Körper, $f, g \in R = F[x_1, \ldots, x_n]$ von 0 verschiedene Polynome und $\prec$ eine Monomordnung auf $R$. Beweise die folgenden Aussagen aus der Vorlesung.*

*i.* $\mathrm{mdeg}(fg) = \mathrm{mdeg}(f) + \mathrm{mdeg}(g)$.

*ii. Für $f \neq -g$ gilt:* $\mathrm{mdeg}(f+g) \preceq \max_{\prec}\{\mathrm{mdeg}(f), \mathrm{mdeg}(g)\}$. *Es gilt sogar die Gleichheit, wenn* $\mathrm{mdeg}(f) \neq \mathrm{mdeg}(g)$ *ist.*

**Aufgabe 16 (Kurven in $\mathbb{R}^2$)** *(5 Punkte)*

*Neben den üblichen kartesischen Koordinaten $(x, y)$ mit $x, y \in \mathbb{R}$ stellen wir die Punkte des $\mathbb{R}^2$ in Polarkoordinaten $(r, \varphi)$ mit $r \in \mathbb{R}$ und $0 \leq \varphi < 2\pi$ dar (auch negative $r$ sind zugelassen, d.h. die Darstellung ist nicht eindeutig; z.B. für $\varphi < \pi$ sind $(r, \varphi)$ und $(-r, \varphi + \pi)$ derselbe Punkt), mit der Umrechnung*

$$x = r\cos\varphi, \quad y = r\sin\varphi$$

*von Polarkoordinaten in kartesische Koordinaten.*

*Betrachte nun die Kurve $C = \{(r, \varphi) : 0 \leq \varphi < 2\pi \text{ und } r = \sin 2\varphi\} \subseteq \mathbb{R}^2$. Sei $I = ((x^2+y^2)^3 - 4x^2y^2) \subseteq \mathbb{R}[x, y]$ das von $(x^2+y^2)^3 - 4x^2y^2$ erzeugte Ideal und $\mathsf{V}(I) \subseteq \mathbb{R}^2$ seine Nullstellenmenge.*

*i. Stelle $C$ graphisch dar.*

*ii. Zeige, daß $C \subseteq \mathsf{V}(I)$ gilt. Hinweis: Additionstheoreme für* sin *und* cos.

*iii. Zeige, daß auch $\mathsf{V}(I) \subseteq C$ gilt (Vorsicht mit den Vorzeichen).*

**Aufgabe 17 (Polynomideale I)** *(2 Punkte)*

*Sei $F$ ein Körper. Zeige: Die Ideale $I = (x + xy, y + xy, x^2, y^2) \subseteq F[x, y]$ und $J = (x, y) \subseteq F[x, y]$ stimmen überein. Der Beweis sollte für* jeden *Körper (insbesondere auch für* $\mathrm{char} F = 2$*) gelten. Hinweis: Es genügt zu zeigen, daß die Erzeuger eines Ideals in dem jeweils anderen Ideal liegen.*

Bonusaufgabe:

**Aufgabe 18 (Polynomideale II)** *(8 Punkte)*

*Seien $F$ ein Körper und $n \in \mathbb{N}$. Für eine Teilmenge $M \subseteq F^n$ definieren wir*

$$\mathsf{I}(M) = \{f \in F[x_1, \ldots, x_n] : f(a) = 0 \text{ für alle } a \in M\}.$$

*i.* *Zeige:* $\mathsf{I}(M)$ *ist ein Ideal.*

*ii.* *Zeige:* $N \subseteq M \Longrightarrow \mathsf{I}(N) \supseteq \mathsf{I}(M)$ *und* $\mathsf{V}(\mathsf{I}(M)) \supseteq M$.

*iii.* *Ein Ideal* $I \subseteq F[x_1, \ldots, x_n]$ *heißt* Radikalideal, *wenn für alle* $m \in \mathbb{N}$ *und* $f \in F[x_1, \ldots, x_n]$ *aus* $f^m \in I$ *bereits* $f \in I$ *folgt. Zeige:* $\mathsf{I}(M)$ *ist ein Radikalideal.*

*iv.* *Bestimme Polynome* $f_1, f_2 \in F[x, y]$ *mit* $\mathsf{I}(\{P\}) = (f_1, f_2)$ *für einen beliebigen Punkt* $P = (a, b) \in F^2$. *Gib eine Menge* $M \subseteq F^2$ *mit* $\mathsf{I}(M) = J$ *aus Aufgabe 17 an.*

*v.* *Bestimme* $\mathsf{I}(\varnothing)$ *und* $\mathsf{I}(F^n)$. *Überlege Dir letzteres zuerst für den Fall* $n = 1$.

*vi.* *Bestimme ein Polynom* $f \in \mathbb{R}[x, y]$ *mit* $\mathsf{I}(M) = (f)$ *für* $M = \{(a, 0) \in \mathbb{R}^2 : 0 \leq a \leq 1\} \subseteq \mathbb{R}^2$.

# 7. Übungsblatt zu Computeralgebra II, SS 1996

JOACHIM VON ZUR GATHEN, JÜRGEN GERHARD

Abgabe: Do, 27. 6. 1996 in der Vorlesung

**Aufgabe 19 (Polynomiale Gleichungssysteme)** *(6 Punkte)*

*Es soll die folgende Optimierungsaufgabe gelöst werden: Zu bestimmen sind sämtliche Maximal- und Minimalstellen der Funktion* $f(x,y) = x^2y - 2xy + y + 1$ *auf dem Einheitskreis* $S = \{(a,b) \in \mathbb{R}^2 : g(a,b) = 0\}$*, wobei* $g(x,y) = x^2 + y^2 - 1$*, einschließlich der Funktionswerte an den Extremstellen. In der Analysis löst man das Problem mit Hilfe der* Lagrange-Multiplikatorenregel*, welche besagt, daß an einer Extremalstelle* $(a,b) \in S$ *die Gleichung* $\nabla f(a,b) = \lambda \nabla g(a,b)$ *für einen „Lagrange-Multiplikator“* $\lambda \in \mathbb{R} \setminus \{0\}$ *erfüllt ist. Dabei ist* $\nabla f = (\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})$ *der Gradient von* $f$ *und analog* $\nabla g$ *der Gradient von* $g$.

i. *Stelle gemäß der Lagrange-Multiplikatorenregel das Gleichungssystem*

$$g = 0 \text{ und } \nabla f = z \nabla g \tag{1}$$

*auf. Gib eine Basis eines Ideals* $I \subseteq \mathbb{R}[x,y,z]$ *an, so daß für die Menge* $L \subseteq \mathbb{R}^3$ *aller Lösungen des Gleichungssystems (1) gilt* $L = V(I) = \{(a,b,\lambda) \in \mathbb{R}^3 : h(a,b,\lambda) = 0 \text{ für alle } h \in I\}$.

ii. *Berechne eine Gröbnerbasis* $G$ *von* $I$ *bzgl. lexicographischer Ordnung mit* $z \succ x \succ y$.

iii. *Löse das zu* $G$ *gehörige (zu (1) äquivalente) polynomiale Gleichungssystem durch Rückwärtssubstitution. Überprüfe, daß alle gefundenen Lösungen tatsächlich Lösungen von (1) sind. Welches sind demnach die* absoluten *Maxima und Minima von* $f$ *auf* $S$*?*

*Zur Lösung der Aufgabe darf (soll) ein Computeralgebrasystem verwendet werden (bitte Quelltext oder „worksheet“ mit abgeben).*

**Aufgabe 20 (Minimale Gröbnerbasen)** *(5 Punkte)*

i. *Ist* $G$ *eine endliche Teilmenge eines Ideals* $I \subseteq R = F[x_1, \ldots, x_n]$ *mit* $\langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(I) \rangle$*, dann gilt* $\langle G \rangle = I$ *(d.h. jede Gröbnerbasis ist tatsächlich auch eine Idealbasis). Hinweis: Zeige per Induktion über* $\mathrm{mdeg}(f)$*, daß für alle* $f \in I$ *gilt* $f \in \langle G \rangle$.

ii. *Beweise: Ist* $G$ *eine Gröbnerbasis für das Ideal* $I \subseteq R = F[x_1, \ldots, x_n]$ *und* $g \in G$ *ein Polynom mit* $\mathrm{lt}(g) \in \langle \mathrm{lt}(G \setminus \{g\}) \rangle$*, dann ist auch* $G \setminus \{g\}$ *eine Gröbnerbasis von* $I$.

iii. *Eine Gröbnerbasis $G$ des Ideals $I \subseteq R$ heißt* minimal, *wenn für alle $g \in G$ gilt: $\mathrm{lc}(g) = 1$ und $\mathrm{lt}(g) \notin \langle \mathrm{lt}(G \setminus \{g\}) \rangle$. Zeige: Sind $G$ und $G'$ zwei minimale Gröbnerbasen desselben Ideals $I \subseteq R$, dann gilt $\mathrm{lt}(G) = \mathrm{lt}(G')$.*

**Aufgabe 21 (Gröbnerbasen I)** *(5 Punkte)*

i. *Berechne mit dem Algorithmus von Buchberger eine Gröbnerbasis für das Ideal $I = \left\langle x^2 + y - 1,\, xy - x \right\rangle \subseteq \mathbb{R}[x, y]$ bzgl. lexicographischer Ordnung mit $x \succ y$. Ist die berechnete Basis minimal? Falls nicht, berechne unter Verwendung von Aufgabe 20 ii. eine minimale Gröbnerbasis.*

ii. *Welche der folgenden Polynome sind in $I$ enthalten: $f_1 = x^2 + y^2 - y$, $f_2 = 3xy^2 - 4xy + x + 1$?*

**Aufgabe 22 (Gröbnerbasen II)** *(6 Punkte)*

*Welche der folgenden Teilmengen von $\mathbb{R}[x, y, z]$ sind Gröbnerbasen bzgl. der lexicographischen Ordnung? Welche sind sogar minimal?*

i. $\{x + y,\, y^2 - 1\}$ *für* $x \succ y$,

ii. $\{y + x,\, y^2 - 1\}$ *für* $y \succ x$,

iii. $\{x^2 + y^2 - 1,\, xy - 1,\, x + y^3 - y\}$ *für* $x \succ y$,

iv. $\{xyz - 1,\, x - y,\, y^2 z - 1\}$ *für* $x \succ y \succ z$.

# 8. Übungsblatt zu Computeralgebra II, SS 1996

Joachim von zur Gathen, Jürgen Gerhard

Abgabe: Do, 11. 6. 1996 in der Vorlesung

**Aufgabe 23 (Differenzenoperator)** *(5 Punkte)*

*Wir bezeichnen mit $E$ den Verschiebungsoperator $(Ef)(k) = f(k+1)$. Dann gilt die Operatoridentität $\Delta = E - I$, wobei $I$ der identische Operator ist. Für $m \in \mathbb{Z}$ ist $E^m$ die $m$-fache Komposition von $E$ mit sich selbst, d.h. $(E^m f)(k) = f(k+m)$.*

i. *Die Produktregel für $\Delta$ läßt sich auch als*

$$\Delta(f \cdot g) = f \cdot \Delta g + Eg \cdot \Delta f = Ef \cdot \Delta g + g \cdot \Delta f$$

*schreiben. Finde und beweise eine Quotientenregel für $\Delta$, in der $\Delta(f/g)$ durch $f, \Delta f, g, \Delta g$ und $Eg$ ausgedrückt wird.*

ii. *Für $m \in \mathbb{Z}$ definieren wir $f^{\underline{m}}$ durch*

$$f^{\underline{m}}(k) = \begin{cases} f(k)f(k-1)\cdots f(k-m+1) & \text{falls } m \geq 1, \\ 1 & \text{falls } m = 0, \\ \dfrac{1}{f(k+1)\cdots f(k-m)} & \text{falls } m \leq -1. \end{cases}$$

*Für $f(k) = k$ sind dies genau die fallenden Potenzen aus der Vorlesung. Beweise die Identität $\Delta f^{\underline{m}} = (Ef - E^{1-m} f) \cdot f^{\underline{m-1}}$.*

iii. *Zeige, daß für alle $m \in \mathbb{N}$ für die $m$-fache Anwendung des Differenzenoperators gilt: $(\Delta^m f)(k) = \sum_{0 \leq i \leq m} (-1)^{m-i} \binom{m}{i} f(k+i)$.*

**Aufgabe 24 (Einige Summen)** *(6 Punkte)*

*Stelle die folgenden Summen in geschlossener Form dar und überprüfe Deine Ergebnisse für $n = 1, 2$.*

i. $\displaystyle\sum_{0 \leq k < n} (k^3 - 3k^2 + 2k + 5)$.

ii. $\displaystyle\sum_{0 \leq k < n} \frac{k+4}{k^3 + 6k^2 + 11k + 6}$ *(Hinweis: schreibe den Summanden als $ak^{\underline{-3}} + bk^{\underline{-2}} + ck^{\underline{-1}}$ mit $a, b, c \in \mathbb{Q}$).*

iii. $\displaystyle\sum_{0 \leq k < n} k2^k$ *(denke dabei an partielle Integration).*

**Aufgabe 25 (Stirling-Zahlen)** *(4 Punkte)*

*Für* $n, k \in \mathbb{N}$ *bezeichnet* $\left\{ {n \atop k} \right\}$ *die Anzahl Partitionen von* $\{1, \ldots, n\}$ *in* $k$ *nicht-leere Teilmengen (Blöcke). Diese Zahlen heißen auch* Stirling-Zahlen zweiter Art. *Für* $k = 0$ *wird* $\left\{ {n \atop 0} \right\} = \delta_{n,0}$ *(Kronecker-Symbol) vereinbart, und natürlich ist* $\left\{ {n \atop k} \right\} = 0$ *falls* $k > n$.

1. *Gib für* $1 \leq k \leq n \leq 4$ *alle Möglichkeiten an,* $\{1, \ldots, n\}$ *in* $k$ *Blöcke zu zerlegen.*

2. *Finde und beweise eine Rekursionsformel für* $\left\{ {n \atop k} \right\}$*, die für* $1 \leq k \leq n$ *richtig ist. Hinweis: unterscheide zwei Fälle danach, ob* $n$ *das einzige Element in seinem Block ist oder nicht.*

3. *Beweise die Identität* $k^m = \sum_{0 \leq i \leq m} \left\{ {m \atop i} \right\} k^{\underline{i}}$ *für* $m \in \mathbb{N}$.