Errata zu M. Kaplan: Computeralgebra

- S.11 Z.25 und statt ˜und˜ .
- S.17 Z.24 und statt ˜˜und˜˜ .
- S.23 Z.4 wenn doppelt.
- S.23 Z.21 Sind $a, b \in R \setminus \{0\}$ mit $\delta(b) \leq \delta(a)$, so...
  statt $\delta(b) < \delta(a)$
- S.24 vor `Gcdex` Vektor statt Vekotr.
- S.25 letzte Z. . statt ..
- S.30 Z.10

$$M(f,g) = \begin{pmatrix} f_m & f_{m-1} & \cdots & f_1 & f_0 & & & \\ & f_m & f_{m-1} & \cdots & f_1 & f_0 & & \mathbf{0} \\ & & \ddots & & & & \ddots & \\ & \mathbf{0} & & \ddots & & & & \ddots \\ & & & & f_m & f_{m-1} & \cdots & \cdots & f_0 \\ g_n & g_{n-1} & \cdots & \cdots & g_1 & g_0 & & & \\ & g_n & g_{n-1} & \cdots & \cdots & g_1 & g_0 & & \mathbf{0} \\ & & \ddots & & & & & \ddots & \\ & \mathbf{0} & & \ddots & & & & & \ddots \\ & & & & g_n & g_{n-1} & \cdots & \cdots & g_1 & g_0 \end{pmatrix}$$

statt

$$M(f,g) = \begin{pmatrix} f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 & & & & \\ & f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 & & & \\ & & \ddots & & & & & \ddots & & \\ & & & \ddots & & & & & \ddots & \\ & & & & f_m & f_{m-1} & f_{m-2} & \cdots & f_1 & f_0 \\ g_n & g_{n-1} & \cdots & g_0 & & & & & & \\ & g_n & g_{n-1} & \cdots & g_0 & & & & & \\ & & \ddots & & & \ddots & & & & \\ & & & \ddots & & & \ddots & & & \\ & & & & \ddots & & & \ddots & & \\ & & & & & \ddots & & & \ddots & \\ & & & & & & g_n & g_{n-1} & \cdots & g_0 \end{pmatrix}$$

Kommentar: Die Schreibweise von $M(f,g)$ in der Definition war eher systematisch zu verstehen. Genau genommen steht das g_1 von der ersten g-Zeile genau unter dem f_m der letzten f-Zeile, bzw. alle f_m und g_0 liegen auf der Hauptdiagonalen.

- S.51 Mitte In der 2. Zeile der Formel muss es jeweils statt $x_\ell + y_\ell$ nur x_ℓ heißen,also

$$(x_1^{n_1} \cdot \ldots \cdot x_r^{n_r}) + \left(\sum_{j=1}^{r} n_j \cdot (x_1^{n_1} \cdot \ldots \cdot x_j^{n_j-1} \cdot \ldots \cdot x_r^{n_r}) y_j \right) +$$

$$+ \sum_{j=1}^{r} \left(p_j y_j^2 \prod_{\substack{\ell=1 \\ \ell \neq j}}^{r} x_\ell^{n_\ell} + \sum_{\substack{k=1 \\ k \neq j}}^{r} n_j n_k y_j y_k x_j^{n_j-1} x_k^{n_k-1} \prod_{\substack{\ell=1 \\ \ell \neq j,k}}^{r} x_\ell^{n_\ell} \right)$$

statt

$$(x_1^{n_1} \cdot \ldots \cdot x_r^{n_r}) + \left(\sum_{j=1}^{r} n_j \cdot (x_1^{n_1} \cdot \ldots \cdot x_j^{n_j-1} \cdot \ldots \cdot x_r^{n_r}) y_j \right) +$$

$$+ \sum_{j=1}^{r} \left(p_j y_j^2 \prod_{\substack{\ell=1 \\ \ell \neq j}}^{r} (x_\ell + y_\ell)^{n_\ell} + \sum_{\substack{k=1 \\ k \neq j}}^{r} n_j n_k y_j y_k x_j^{n_j-1} x_k^{n_k-1} \prod_{\substack{\ell=1 \\ \ell \neq j,k}}^{r} (x_\ell + y_\ell)^{n_\ell} \right)$$

- S.58 Z.14 verbessern statt verbesseren.
- S.73 Z.9 sieht statt sieht sieht.
- S.115 Z.12 $\mathrm{LM}(p) := \mathrm{LK}(p) \cdot \mathrm{LT}(p) = a_m X^{I_m}$ statt $\mathrm{LM}(p) := \mathrm{LK}(p) \cdot \mathrm{LM}(p) = a_m X^{I_m}$.
- S.132 Z.10 v.u. so ergibt sich $\tilde{g}(\tilde{a}b\alpha\tilde{q} - a\tilde{b}\tilde{\alpha}q) = b(a\tilde{\alpha}r - \tilde{a}\alpha\tilde{r})$.
  statt
  so ergibt sich $\tilde{g}(\tilde{a}b\alpha\tilde{q} - a\tilde{b}\tilde{\alpha}q) = b(a\tilde{\alpha}r - u\tilde{a}\alpha\tilde{r})$.
- S.144 1.Textzeile nach dem Satz von Bézout zu statt nach dem Satz von Bézoutzu.
- S.174 in `ModPot` Statt $t \leftarrow t \cdot r^2 \bmod s$ in der **else**-Schleife muss es $t \leftarrow t^2 \cdot r \bmod s$ heißen.
- S.204 Z.8 v.u. $\prod_{j=1}^{n}(-1)^{i_j} Q_{i_j}$ statt $\prod_{k=1}^{n}(-1)^{i_j} Q_{i_j}$.
- S.216 Z.20 zu statt zu zu.
- S.233 in `SQF` Falscher Umbruch im Kommentar; richtig:
  # Ausgabe: quadratfreie Faktori-
  # sierung wie in *(6.2)*
- S.243 Beispiel: Die Zeile mit der Berlekamp-Matrix und der Kern-Berechnung ist doppelt.
- S.264 letzte Z. von Yun statt vonYun.
- S.268 `bezout21` **for** i **from** 1 **to** $t-1$ **do** statt **for** i **from** 1 **to** $p-1$ **do** .
- S.271 Z.3 $\max\{|q_j|\,,\, \deg q \leq \frac{n}{2}\}$ statt $\max\{|b_j|\,,\, \deg q \leq \frac{n}{2}\}$, wobei $q(x) = \sum_{i=0}^{m} q_i x^i$ ein Teiler von f sei.
- S.269 bis S.275 Durch einen Fehler des Textverarbeitungssystems stimmen auf diesen Seiten die Satz-, Beispiel- und Paragraphennummern nicht. Dies wirkt sich auch auf Seite XI im Inhaltsverzeichnis aus. Es muss dort richtig heißen
  6.4.2 Wie weit muss man liften?
  6.4.3 Swinnerton-Dyer Polynome
  mit jeweils angepasster Nummerierung in diesen Abschnitten.
- S.338 Z.28 Statt GPL lautet die Abkürzung für die „GNU Lesser General Public License“ richtig LGPL.
- S.341 Z.2 Der Satz endet ohne .
- S.342 Z.20/21 Es muss richtig heißen: das Paket `group` mit dem Befehl `with(group)` nachladen. und nicht jeweils `groups`.
- S.342 letzte Z. das gezeigte 22-seitige Beispiel.
- S.355 Z.3 v.u. Fortran statt fortran.
- S.357 Mitte Analog geht das in Java, VisualBasic, Fortran, Matlab etc. (statt In).
- S.367 Z.1 Proceedingsbände statt Prodeedingsbände

Für eventuelle weitere Hinweise per Email an **kaplan@ma.tum.de** bin ich dankbar.