Vortragsliste Computeralgebraseminar Herbst 2018

1. ENES YAYCIOGLU, MERT CAN BESER: EUKLID**ische und faktorielle Ringe** *(6. Sept. 2018)*
   [P], *§2.1–3*

2. ERKUT DONAT, EMRE YÖNDEM: **Polynomringe** *(13. Sept. 2018)*
   [P], *§6.1–2*

3. SUSANNA GRAF, SHEELA SCHMID: **Die schnelle** FOURIER**-Transformation** *(20. Sept. 2018)*
   [AHU], *§7.1+2+4. Bei der Definition einer primitiven Einheitswurzel zu Beginn von §1 zeige man, daß Eigenschaft 3. äquivalent ist dazu, daß* $\omega^r \neq 1$ *für* $1 \leq r < n$.

4. ANDREA REHBERGER, PHILIPP BISCHOFF: **Polynomdivision** *(27. Sept. 2018)*
   [P], *§6.3,* **[DST]**, *§2.3.3*

5. REBECCA LEHMING: **Rechnen mit homomorphen Bildern** *(4. Okt. 2018)*
   [Ka], *Kap. 3*

6. SÜMEYYE-NUR AVCI, FURKAN ÖZDEMIR: **Nullstellen komplexer Polynome** *(11. Okt. 2018)*
   [M], *§4.1–2*

7. FATIH KESKIN, SARAH SWAIDAN: **Die Ungleichung von** LANDAU-MIGNOTTE *(18. Okt. 2018)*
   [M], *§4.3.1–3 und §4.4. Auf den Fall von Polynomen mehrerer Veränderlicher muß nicht eingegangen werden.*

8. EBRU SEMIR KEKLIK, EMRE HALICI: **Modulare Berechnung des ggT** *(25. Okt. 2018)*
   [DST], *§4.1.1.1–3*

9. ILONA SLUTSKER, BEN AMOR: **Resultanten** *(8. Nov. 2018)*
   [BK], *§4.2 ab Seite 222 unten,* **[vdW]**, *Kap. 5, §34+35,* **[XYZ]**
   Der Koeffizientenbereich sollte wie in **[BK]** *ein beliebiger faktorieller Ring sein.*

10. MARIE CHASSEIN, CHRISTINE VOCHTEL: **ggT in mehreren Veränderlichen und andere modulare Berechnungen** *(15. Nov. 2018)*
    [DST], *§4.1.2 und §4.1.3.2+3*

11. THERESA MERKT: **Quadratfreie Faktorisierung eines Polynoms** *(22. Nov. 2018)*
    [Ka], *§6.2 oder* **[M]**, *§6.3*

12. CATHRIN RÖHNISCH: **Faktorisierung von Polynomen über endlichen Körpern** *(29. Nov. 2018)*
    [Ka], *§6.3*

13. SIMON WINTER: **Faktorisierung von Polynomen über den ganzen Zahlen** *(6. Dez. 2018)*
    [Ka], *§6.4*

Literaturliste

[AHU] A.V. AHO, J.E. HOPCROFT, J.D. ULLMAN: Design and analysis of computer algorithms, *Addison-Wesley,* 1974 und zahlreiche Nachdrucke

[BK] EGBERT BRIESKORN, HORST KNÖRRER: Ebene Kurven, *Birkhäuser*, 1981

[DST] J.H. DAVENPORT, Y. SIRET, E. TOURNIER: Computer Algebra – Systems and algorithms for algebraic computation, *Academic Press,* 1988

[K] MICHAEL KAPLAN: Computeralgebra, *Springer,* 2004
(im Netz der Universität Mannheim auch elektronisch verfügbar)

[M] MAURICE MIGNOTTE: Algorithms for Coumputer Algebra, *Springer*, 1992

[P] ATTILA PETHÖ: Algebraische Algorithmen, *Vieweg,* 1999

[vdW] B.L. VAN DER WAERDEN: Algebra I, *Springer*, *zahlreiche Auflagen*

[XYZ] ZUSATZ: Im Vortrag über Resultanten sollte noch zusätzlich folgender Satz bewiesen werden:

Satz: Ist $\varphi\colon A \to B$ ein Homomorphismus von Ringen und $\widetilde{\varphi}\colon A[X] \to B[X]$ seine Fortsetzung auf die Polynomringe über A und B, so ist gilt für $f, g \in A[X]$

$$\mathrm{Res}_X\left(\widetilde{\varphi}(f), \widetilde{\varphi}(g)\right) = \varphi\Big(\mathrm{Res}_X(f,g)\Big)\,.$$

Daraus folgt dann

Korollar: Sind $f, g \in \mathbb{Z}[X]$, und ist h ihr ggT, so gibt es höchstens endlich viele Primzahlen p derart, daß der ggT von f mod p und g mod p einen größeren Grad als h hat.

Beweis: Sei $\bar{f} = f/h$ und $\bar{g} = g/h$. Wenn der ggT von f mod p und g mod p größeren Grad als h hat, müssen $\bar{f}$ mod p und $\bar{g}$ mod p einen gemeinsamen Teiler positiven Grades haben. d.h. ihre Resultante verschwindet.

Nun wende man den Satz an auf $\varphi\colon \mathbb{Z} \to \mathbb{Z}/p$ mit $\varphi(z) = z \bmod p$. Danach ist

$$0 = \mathrm{Res}_X(\bar{f} \bmod p, \bar{g} \bmod p) = \varphi\Big(\mathrm{Res}_X(\bar{f}, \bar{g})\Big) = \mathrm{Res}_X(\bar{f}, \bar{g}) \bmod p\,,$$

d.h. die Resultante von $\bar{f}$ und $\bar{g}$ muß durch p teilbar sein. Da eine ganze Zahl höchstens endlich viele Primteiler hat, folgt die Behauptung.