Modul Computeralgebra mit Gröbnerbasen 14. April 2011
Sommersemester 2011
Schmale

Aufgabenblatt 2

(**4**) Überlegen Sie sich ein Verfahren zur modularen Multiplikation zweier Polynome f, g aus $\mathbb{Z}[x]$ analog zu Beispielen aus Kapitel I. Fortsetzung u.A. für Liebhaber(innen) von Laufzeitabschätzungen: Ex. 4.17. in [Sh] p. 86. (Link zum Text siehe VL-Seite)

(**5**) Beweisen Sie den Satz über die Resultante in Kap. I, § 4.

(**6**) Sei $f = g^r \cdot h^s$ in $\mathbb{Z}_p[x]$. Was liefert der Algorithmus zur quadratfreien Zerlegung in $\mathbb{Z}[x]$ aus Kap. II, § 5 in diesem Fall?
Wie könnte man den quadratfreien Teil von f gewinnen?
Mehr dazu oder Fortsetzung in Ex. 14.27 in [GaGe].