RUHR UNIVERSITÄT BOCHUM

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov, Elena Kirshanova

Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 12 / 17 July 2014

Exercise 1:
Let $I \subset k[x_1, \dots x_n]$ be a principal ideal (that is, I is generated by a single $f \in I$). Show that any finite subset of I containing a generator for I is a Groebner basis for I.

Exercise 2:
Let $f, g \in k[x_1, \dots x_n]$ be polynomials such that $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$ are relatively prime monomials and $\mathrm{LC}(f) = \mathrm{LC}(g) = 1$. Show that

$$S(f,g) = -(g - \mathrm{LT}(g))f + (f - \mathrm{LT}(f))g.$$

Exercise 3:
Consider an ideal I generated by $I = \langle xz-y, xy+2z^2, y-z\rangle$. Is this generating set a Groebner basis for I? If not, find a Groebner basis. What will be a minimal and the reduced Groebner basis for I?

Exercise 4:
Let G be a Groebner basis of an ideal I with the property that $\mathrm{LC}(g) = 1$ for all $g \in G$. Prove that G is a minimal Groebner basis if and only if no proper subset of G is a Groebner basis.

Exercise 5:
Let G and G' be Groebner bases for an ideal I with respect to the same monomial order in $k[x_1, \dots x_n]$. Show that $\bar{f}^G = \bar{f}^{G'}$ (here we write $\bar{f}^G$ for the remainder on division of f by a Groebner basis $G = \langle f_1, \dots f_s\rangle$). Hence, the remainder of division by a Groebner basis is independent of which Groebner basis we use, as long as we fix a monomial order.