RUHR UNIVERSITÄT BOCHUM

RUB

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

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 14 / 1. Februar 2012

AUFGABE 1:
Man kann für die Polynome

$$f_1 = x^{n+1} - yz^{n-1}w$$
$$f_2 = xy^{n-1} - z^n$$
$$f_3 = x^n z - y^n w$$

zeigen, dass die reduzierte Gröbnerbasis bzgl. $>_{grevlex}$ und $x > y > z > w$ das Polynom

$$z^{n^2+1} - y^{n^2} w$$

enthält[1]. Überprüfen Sie diese Aussage für $n = 2$.

Hinweis: Es ist hierbei nur selten nötig, den Divisionsalgorithmus tatsächlich durchzuführen: Man sieht entweder sofort, dass keiner der $\mathrm{LT}(f_i)$ den Leitterm von $S(f_j, f_k)$ teilt oder es reicht *ein einziges* Basispolynom aus, um $S(f_j, f_k)$ darzustellen.

AUFGABE 2:
Sei $I \subset k[x_1, \ldots, x_n]$ ein Ideal. Beweisen Sie, dass $I_\ell := I \cap k[x_{\ell+1}, \ldots, x_n]$ ein Ideal (in $k[x_{\ell+1}, \ldots, x_n]$) ist.

AUFGABE 3:
Berechnen Sie die Gröbnerbasen G_1 und G_2 für die Eliminationsideale I_1 und I_2 für das durch die Gleichungen

$$x^2 + y^2 + z^2 = 4$$
$$x^2 + 2y^2 = 5$$
$$xz = 1$$

definierte Ideal (d.h. benutzen Sie $>_{lex}$ und $x > y > z$). Bestimmen Sie alle reellen Lösungen (d.h. in $\mathbb{R}^3$).

Hinweis: Sie können direkt mit der Gröbnerbasis $G = \{1-3z^2+2z^4, -1+y^2-z^2, x-3z+2z^3\}$ rechnen. Als Vorbereitung auf die Klausur bietet sich eine manuelle Berechnung von G an.

[1] Einen Beweis findet man in „Gröbner-Bases, Gaussian elimination and resolution of systems of algebraic equations“ (Lazard, 1983). Das Resultat liefert ein Beispiel für eine relativ aufwändig zu berechnende Gröbnerbasis die Basispolynome mit hohem Grad enthält