RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Enrico Thomae

Hausübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 14 / 26. Januar 2011 / Abgabe bis spätestens 03. Februar 2011, 10 Uhr (vor der Übung)

AUFGABE 1 (8 Punkte)**:**
Bestimmen Sie $V(x^2 - y, y + x^2 - 4) \subseteq \mathbb{R}^2$. Gehen Sie dabei wie folgt vor.

1) Zeigen Sie, dass $G = \{x^2 - y, y + x^2 - 4\}$ keine Gröbnerbasis für $I = \langle G \rangle$ ist.

2) Formen Sie G mit Hilfe des Buchbergeralgorithmus zu einer Gröbnerbasis um.

3) Bilden Sie eine minimale Gröbnerbasis.

4) Bilden Sie die reduzierte Gröbnerbasis und lesen Sie $V(I)$ ab.

AUFGABE 2 (6 Punkte)**:**
Bestimmen Sie $V(xz-2, 2x^2-xy+2xz-y^2+yz+2z^2, -2x^2+xy+2xz+y^2-2yz-z^2+2) \subseteq \mathbb{Q}^3$. Bestimmen Sie dazu zunächst die reduzierte Gröbnerbasis.

AUFGABE 3 (4 Punkte)**:**
Sei G eine Gröbnerbasis des Ideals I mit $\mathrm{LC}(g) = 1$ für alle $g \in G$. Beweisen Sie, dass G genau dann eine minimale Gröbnerbasis ist, wenn keine echte Teilmenge von G existiert, die auch eine Gröbnerbasis für I bildet.

AUFGABE 4 (4 Punkte)**:**
Seien G und $\widetilde{G}$ zwei minimale Gröbnerbasen des Ideals I für eine beliebige fest gewählte Ordnung. Beweisen Sie, dass G und $\widetilde{G}$ die gleiche Anzahl an Elementen besitzen.