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 12 / 12. Januar 2011 / Abgabe bis spätestens 19. Januar 2011, 10 Uhr (vor der Übung)

AUFGABE 1 (4 Punkte)**:**
Sei $R = \{(x, y) \in \mathbb{R}^2 \mid y > 0\}$. Zeigen Sie, dass R **keine** affine Varietät ist.

Hinweis: Betrachten Sie f(x,x) und zeigen Sie, dass f(0,0)=0.

AUFGABE 2 (5 Punkte)**:**
Beschreiben Sie alle möglichen Stellungen des in Abbildung 1 dargestellten Roboters durch ein System von Polynomgleichungen. Dabei seien die Punkte $(0, 0)$ und (x, y) um 360° drehbare Gelenke und (a, b) der Schreibkopf. Die Länge der Gelenke ist jeweils 1. Zeigen Sie formal, dass der Schreibkopf in der Lage ist alle Punkte auf dem Kreuz $\{(0, y) \mid y \in [-2, 2]\} \cup \{(x, 0) \mid x \in [-2, 2]\}$ zu erreichen. Wie sieht die affine Varietät des Polynomssystems geometrisch aus, d.h. welche Punkte kann der Schreibkopf erreichen (dies muss nicht formal bewiesen werden)?

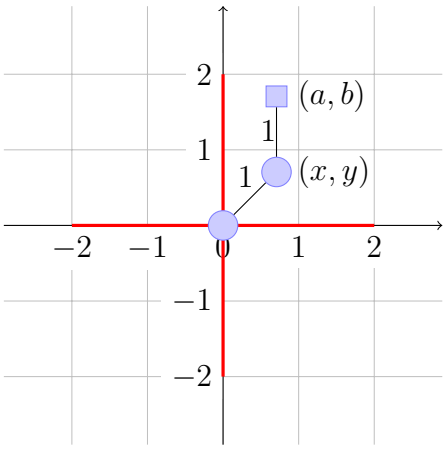

Abbildung 1: Roboter mit 2 Gelenken

AUFGABE 3 (5 Punkte)**:**
Prüfen Sie folgende Aussage über $\mathbb{R}$

$$x^3 - x \in \left\langle x^3 - x^2 - x + 1, x^4 + x^3 - x^2 - x \right\rangle .$$

Bilden Sie dazu zunächst das Hauptideal.