RUHR
UNIVERSITÄT
BOCHUM

RUB

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

**Hausübungen zur Vorlesung**

# Kryptanalyse

**WS 2011/2012**

Blatt 11 / 11. Januar 2012 / Abgabe bis spätestens 18. Januar 2012, 10 Uhr in dem Kasten auf NA 02

**AUFGABE 1** (5 Punkte)**:**
Zeigen Sie

$$\mathbf{V}(x + xy, y + xy, x^2, y^2) = \mathbf{V}(x, y)$$

über $\mathbb{Q}$.

**AUFGABE 2** (5 Punkte)**:**
Sei $\mathbb{F}$ ein Körper. Beweisen Sie, dass jede endliche Teilmenge des $\mathbb{F}^n$ eine affine Varietät ist.

*Hinweis:* Zeigen Sie zunächst, dass jeder Punkt $(a_1, \ldots, a_n) \in \mathbb{F}^n$ eine affine Varietät ist.

**AUFGABE 3** (5 Punkte)**:**

a) Zeigen Sie, dass die Menge

$$X := \{(x, x) : x \in \mathbb{R}, x \neq 1\} \subset \mathbb{R}^2$$

*keine* affine Varietät ist. Gehen Sie hierbei wie in Präsenzübung 11, Aufgabe 3 vor.

b) Seien $V, W$ affine Varietäten. Zeigen Sie, dass *im Allgemeinen* die Menge

$$V \setminus W := \{v \in V : v \notin W\}$$

*keine* affine Varietät ist. Geben Sie hierzu ein konkretes Gegenbeispiel an.

**AUFGABE 4** (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)?

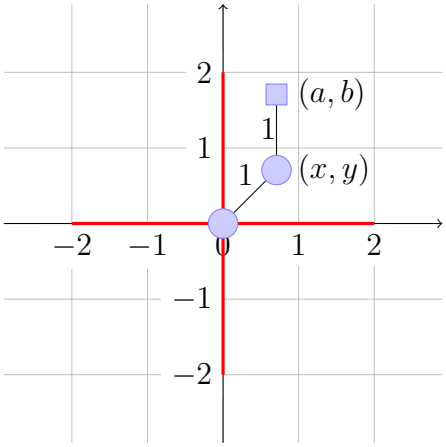


Abbildung 1: Roboter mit 2 Gelenken