RUHR
UNIVERSITÄT
BOCHUM

RUB

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

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 12 / 12. Januar 2011

AUFGABE 1:
Bestimmen Sie in $\mathbb{R}^2$ alle Punkte der Varietät

$$V(x^2 + y^2 - 4) \cap V(xy - 1) = V(x^2 + y^2 - 4, xy - 1).$$

Skizzieren Sie $V(x^2 + y^2 - 4)$ und $V(xy - 1)$ in einem Diagramm.

AUFGABE 2:
Beiweisen 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 und wenden Sie dann den Satz über die Abgeschlossenheit unter Vereinigung und Schnitt aus der Vorlesung an.

AUFGABE 3:
Sei $I \subset \mathbb{F}[x_1, \ldots, x_n]$ ein Ideal. Zeigen Sie die Äquivalenz folgender Aussagen

i) $f_1, \ldots, f_s \in I$

ii) $\langle f_1, \ldots, f_s \rangle \subseteq I$.

Nutzen Sie diese Äquivalenz um zu zeigen, dass die von den Basen $B_1 = \{2x^2 + 3y^2 - 11, x^2 - y^2 - 3\}$ und $B_2 = \{x^2 - 4, y^2 - 1\}$ erzeugten Ideale gleich sind. Nutzen Sie dies um $V(B_1)$ zu bestimmen.

AUFGABE 4:
Zeigen Sie, dass $I(V(x^n, y^m)) = \langle x, y \rangle$ für alle $m, n \in \mathbb{N}_{>0}$ gilt.