Übung zur Algebra 1 vom 15.01.2014

ÜBUNGSMITSCHRIFT

Jesko Hüttenhain

13. Februar 2014

Kleine Wiederholung: Für einen Körper $\Bbbk$ bezeichnen wir einen Ring A als $\Bbbk$-Algebra, wenn A den Körper $\Bbbk$ als Unterring enthält und somit zu einem $\Bbbk$-Vektorraum ist.

Beispiel 0.1. Die Ringe $A = \Bbbk[X]$, $A = \Bbbk[X_1, \dots, X_n]$ und $A = \Bbbk[X]/(f)$ sind $\Bbbk$-Algebren.

Lemma 0.2. *Es sei $\Bbbk$ ein Körper und $f \in \Bbbk[X]$ mit $\deg f = 1$. Weiter sei $\pi\colon \Bbbk[X] \to \Bbbk[X]/(f)$ die kanonische Projektion und $\overline{X} := \pi(X)$. Dann ist $\{1, \overline{X}, \dots, \overline{X}^{n-1}\}$ eine Basis von $\Bbbk[X]/(f)$ als $\Bbbk$-Vektorraum.*

Beweis. Zunächst zeigen wir, dass $\{1, \overline{X}, \dots, \overline{X}^{n-1}\}$ ein Erzeugendensystem ist. Dies ist äquivalent dazu, dass für alle $g \in \Bbbk[X]$ ein $\tilde{g} \in \Bbbk[X]$ mit $\deg(\tilde{g}) < n$ und $\pi(g) = \pi(\tilde{g})$ existiert. Sei also $g \in \Bbbk[X]$ und schreibe

$$g = qf + \tilde{g}$$

mit $\deg(\tilde{g}) < \deg f = n$. Dann ist $\pi(g) = \pi(qf + \tilde{g}) = \pi(q)\pi(f) + \pi(\tilde{g}) = \pi(\tilde{g})$.
Zu zeigen bleibt die lineare Unabhängigkeit von $\{1, \dots, \overline{X}^{n-1}\}$. Dazu seien $a_0, \dots, a_{n-1} \in \Bbbk$ mit

$$\sum_{i=0}^{n-1} a_i \overline{X}^i = 0\,.$$

Dies bedeutet

$$\sum_{i=0}^{n-1} a_i X^i \in \ker \pi = (f)$$

und für alle von Null verschiedenen $g \in (f)$ ist $\deg g \geq n$. Demnach muss $\sum_i a_i X^i = 0$ sein, also sind alle a_i Null. □

Bevor wir zum Berlekamp-Algorithmus kommen, legen wir folgende Notation fest: Es ist $\mathbb{F}_p := \mathbb{Z}/(p)$ und $f \in \mathbb{F}_p[X]$ sei ein normiertes und quadratfreies Polynom mit Primfaktorzerlegung

$$f = p_1 \cdots p_t\,.$$

Weiter setzen wir $A := \mathbb{F}_p[X]/(f) \cong \mathbb{F}_p[X]/(p_1) \times \cdots \times \mathbb{F}_p[X]/(p_t)$. Die lineare Frobenius-Abbildung $\Phi\colon A \to A$ ist durch $\overline{g} \mapsto \overline{g}^p$ definiert. Letztlich sei $B := \{\overline{g} \in A : \Phi(\overline{g}) = \overline{g}\} = \ker(\Phi - \mathrm{id})$. Es ist also A ein $\mathbb{F}_p$-Vektorraum.

$$\begin{array}{ccccc} a & & \mathbb{F}_p & \longrightarrow & A \\ \downarrow & & \downarrow \cong & & \downarrow \\ \begin{pmatrix} a \\ 0 \\ \vdots \\ 0 \end{pmatrix} & & \mathbb{F}_p \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} & \longrightarrow & \mathbb{F}_p^n \end{array} \qquad \begin{array}{c} \sum_{i=0}^{n-1} a_i \overline{X}^i \\ \downarrow \\ (a_0, \dots, a_{n-1}) \end{array}$$

Lemma 0.3. *Es sei $a \in B \setminus \mathbb{F}_p$. Dann existiert $s \in \mathbb{F}_p$, so dass $a - s$ ein Nullteiler in A ist.*

Dass $\overline{g} \in \mathbb{F}_p[X]/(f)$ ein Nullteiler ist, bedeutet die Existenz eines $\overline{h} \in \mathbb{F}_p[X]/(f)$ mit $\overline{g}\overline{h} = 0 = \overline{f}$, d. h. $\mathrm{ggT}(f, g) \neq 1$.

Wir erklären nun Berlekamps Algorithmus:

Input: Ein normiertes quadratfreies Polynom $\mathbb{F}_p[X]$.

Output: Die Anzahl t der Primfaktoren von f und, falls $t \neq 1$, zwei Polynome $\mathbb{F}_p[X] \setminus \mathbb{F}_p$ mit $gh = f$.

1. Für $j = 1, \ldots, n$ sei $X^{jp} = qf + r$ nach Division durch Rest. Wir schreiben $r = \sum_{i=0}^{n-1} \beta_{ij} X^i$.
2. Setze $B := \ker\big((\beta_{ij} - \delta_{ij})_{ij}\big)$.
3. Setze $t := \dim_{\mathbb{F}_p}(B)$.
4. Ist $t > 1$, so wähle ein $a \in B$, für welches es ein $i > 0$ mit $a_i \neq 0$ (nicht die Restklasse eines konstanten Polynoms).
5. Für $s = 0, \ldots, p-1$ setze $g := \mathrm{ggT}(a - s, f)$. Sobald $g \neq 1$ ist, setze $h := \frac{f}{g}$ und gib dies aus.