ETH Zürich, D-INFK
HS 2016, 21. November 2016

Prof. Ueli Maurer
Daniel Tschudi

# Diskrete Mathematik

# Übung 10

### 10.1 Eigenschaften kommutativer Ringe ($\star$)

Ziel dieser Aufgabe ist es, Lemma 5.18 (ii) und (iii) zu beweisen.

Sei $\langle R; +, -, 0, \cdot, 1\rangle$ ein kommutativer Ring und $a, b, c \in R$. Zeigen Sie:

**a)** Falls $a|b$ gilt $a|bc$ für alle $c$.

**b)** Falls $a|b$ und $a|c$ gilt $a|(b+c)$.

### 10.2 Nullteiler und Integritätsbereiche *(8 Punkte)*

**a)** ($\star\ \star$) Sei $R$ ein nicht-trivialer Ring (d.h. $0 \neq 1$) und sei $a(x) \in R[x]$ ein monisches Polynom. Zeigen Sie, dass $a(x)$ kein Nullteiler von $R[x]$ ist. *(3 Punkte)*

**b)** ($\star\star\star$) Beweisen Sie Theorem 5.25, d.h. zeigen Sie, dass jeder endliche Integritätsbereich ein Körper ist. *(5 Punkte)*

*Hinweis:* Verwenden Sie das Schubfachprinzip.

### 10.3 Lineares Gleichungssystem ($\star\ \star$)

Lösen sie folgendes Gleichungssystem über $\mathbb{Z}_{11}$.

$$\begin{aligned} 10 \odot x \ \oplus\ 2 \odot y \ \oplus\ 5 \odot z &= 1 \\ 7 \odot x \ \oplus\ 4 \odot y \ \oplus\ 6 \odot z &= 2 \\ 3 \odot x \ \oplus\ 6 \odot y \ \oplus\ 9 \odot z &= 4 \end{aligned}$$

### 10.4 Rechnen mit Polynomen

**a)** ($\star$) Dividieren Sie $x^5+6x^2+5$ durch $5x^2+2x+1$ über $\mathbb{Z}_7$ (es handelt sich um Division mit Rest).

**b)** ($\star\ \star$) Zählen Sie alle irreduziblen Polynome von Grad vier über $\mathrm{GF}(2)$ auf.

**c)** ($\star\ \star$) Sei $a(x)$ ein Polynom vom Grad $4$ in $\mathrm{GF}(7)[x]$, von dem Sie wissen, dass $a(x)$ eine doppelte Nullstelle an der Stelle $x = 2$ hat. Ferner kennen Sie $a(3) = 2$, $a(4) = 3$ und $a(6) = 5$. Bestimmen Sie $a(0)$.

### 10.5 Absicherung von Nuklearwaffen

Auf einer einsamen Insel lassen sich alle Nuklearwaffen durch einen geheimen Schlüssel $s \in \mathrm{GF}(q)$ für $q$ prim aktivieren. Dieser Schlüssel wird unter $n < q$ Generälen $G_1, \ldots, G_n$ aufgeteilt. Dazu werden geheime, uniform zufällige $a_1, \ldots, a_{t-1} \in \mathrm{GF}(q)$ gewählt, wobei

$$a(x) := a_{t-1}x^{t-1} + \cdots + a_1 x + s \in \mathrm{GF}(q)[x].$$

Jeder General $G_i$ bekommt einen geheimen 'Share' $s_i = a(\alpha_i)$, wobei $\alpha_1, \ldots, \alpha_n$ öffentlich bekannte, paarweise verschiedene Elemente aus $\mathrm{GF}(q) - \{0\}$ sind.

**a)** ($\star$ $\star$) Bei einem Angelausflug sterben alle bis auf $t$ Generäle. Zeigen Sie, dass der Schlüssel nicht verloren ist, da er sich aus $t$ Shares eindeutig bestimmen lässt.

**b)** ($\star$ $\star$) Ein irrer General will einen Nachbarschaftsstreit nuklear lösen. Um den Schlüssel $s$ zu bestimmen, hat er insgesamt (inkl. seinem eigenen) $t-1$ Shares gesammelt. Wie viele Werte in $\mathrm{GF}(q)$ kommen noch als Schlüssel in Frage, wenn $t-1$ Shares gegeben sind? Was bedeutet das für den General?

**Abgabe am 28./29. November 2016**
**Korrigiert wird Aufgabe 10.2**