Dr. Markus Junker — Diskrete Algebraische Strukturen — Sommer 2011
Übungsblatt 5

Verantwortlich für die Übungen:
Dr. Fritz Hörmann (fritz.hoermann@math.uni-freiburg.de)

Jede Aufgabe ergibt 4 Punkte. **16 Punkte zählen als 100%**.

1. **Zyklische Einheitengruppen, diskreter Logarithmus.** Bestimmen Sie alle Erzeuger der zyklischen Gruppe $(\mathbb{Z}/13\mathbb{Z})^*$.

   Geben Sie für einen dieser Erzeuger ξ explizit den Gruppenisomorphismus

   $$\mathbb{Z}/12\mathbb{Z} \to (\mathbb{Z}/13\mathbb{Z})^*,$$

   welcher $\overline{1}$ auf ξ abbildet als Tabelle an und auch sein Inverses (diskreter Logarithmus zur Basis ξ).

2. **Euklidischer Algorithmus für Polynome.** Zur Erinnerung: Für Polynome funktioniert der Algorithmus „Division mit Rest“ wie für ganze Zahlen. D.h. falls Polynome

   $$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in \mathbb{R}[X] \qquad a_n \neq 0$$

   und

   $$g = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0 \in \mathbb{R}[X] \qquad b_m \neq 0$$

   gegeben sind, so findet man — mittels des Schulschemas für Division — Polynome q (Quotient) und r (Rest), so dass

   $$f = q \cdot g + r,$$

   wobei der Grad von r echt kleiner als der Grad m von g ist.

   Mit dem euklidischen Algorithmus kann man deshalb auch den g.g.T. zweier Polynome f und g berechnen und eine Darstellung

   $$\mathrm{ggT}(f, g) = m \cdot f + n \cdot g$$

   finden (hier sind auch m und n Polynome!). Der g.g.T. ist eindeutig bis auf Multiplikation mit einer reellen Zahl ($\neq 0$).

   Berechnen Sie den g.g.T. der Polynome $f = X^3 - X^2 + 2X + 1$ und $g = X^2 + 2$ und finden Sie die zugehörige Darstellung $\mathrm{ggT}(f, g) = m \cdot f + n \cdot g$.

Bitte wenden!

3. **Der Körper mit 4 Elementen.** Die kommutative Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ wird durch eine geeignete Multiplikation zu einem Körper $\mathbb{F}_4$. Finden Sie die dazugehörige Multiplikationstafel.

   Hinweis: Bezeichnen wir die Elemente von $\mathbb{F}_4$ wie folgt:

$$0 := (\overline{0}, \overline{0}), \quad 1 := (\overline{1}, \overline{0}), \quad a := (\overline{0}, \overline{1}), \quad b := (\overline{1}, \overline{1}).$$

   Dabei ist 0 das Nullelement der Addition und 1 soll das Einselement der zu konstruierenden Multiplikation werden. (Sie können sich überlegen, dass alle Elemente ausser 0 hier a priori gleichberechtigt sind.).

   Dann ergibt sich die folgende Additionstafel:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

   Für die Multiplikation wissen wir schon einmal, dass $0 \cdot x = 0$ für alle $x \in \mathbb{F}_4$ und $1 \cdot x = x$ für alle $x \in \mathbb{F}_4$, d.h. wir bekommen die folgende Multiplikationstafel:

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	$\square$	$\square$
b	0	b	$\square$	$\square$

   Füllen Sie die restlichen Felder, und begründen Sie, warum es nur eine Wahl gibt. Sie müssen nicht beweisen, dass es ein tatsächlich ein Körper ist.

4. **Erzeuger von Einheitengruppen.** Sei $N \in \mathbb{N}_{>0}$ so gewählt, dass $(\mathbb{Z}/N\mathbb{Z})^*$ zyklisch ist[1], und sei g ein Erzeuger dieser Gruppe. Zeigen Sie: g^k ist genau dann ebenfalls ein Erzeuger, wenn $\mathrm{ggT}(k, \varphi(N)) = 1$ ist. Hier bezeichnet φ die Eulersche φ-Funktion.

*5. **Der Körper mit 4 Elementen II.** Geben Sie einen Ringisomorphismus des Körpers $\mathbb{F}_4$ aus Aufgabe 3 mit dem Restklassenring $\mathbb{F}_2[X]/(X^2 + X + 1)\mathbb{F}_2[X]$ an. Hierbei ist $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ der Körper mit 2 Elementen.

Abgabe am 6.6.2011 im Hörsaal vor Beginn der Vorlesung

[1] Man kann zeigen, dass dies bedeutet: $N = p^n$ oder $N = 2p^n$ für eine ungerade Primzahl p und natürliche Zahl n, oder $N = 2$, oder $N = 4$.