Dr. Markus Junker — Mathematik II für Informatiker — Sommer 2012
Übungsblatt 10

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

1. **Euklidischer Algorithmus für Polynome.** Berechnen Sie mit dem Euklidischen Algorithmus den g.g.T. (eindeutig bis auf eine Konstante) der folgenden Polynome

$$p := X^4 + X^2 + X + 1 \text{ und } q := X^4 + X^3 + X + 1$$

   (a) in $\mathbb{R}[X]$,
   (b) in $\mathbb{F}_2[X]$,

   und finden Sie die zugehörige Darstellung

$$\mathrm{ggT}(p, q) = a \cdot p + b \cdot q.$$

   Hinweis: In (b) bezeichnet $\mathbb{F}_2[X]$ den Ring der Polynome $a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ mit Koeffizienten $a_i \in \mathbb{F}_2 = \{\overline{0}, \overline{1}\}$. Multipliziert werden diese Polynome durch ausmultiplizieren, z.B. $(X + \overline{1})^2 = X^2 + \overline{2}X + \overline{1} = X^2 + \overline{1}$.

2. **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).

3. **Endliche Körper von Primzahlpotenzordnung, Beispiel $\mathbb{F}_4$.**

   (a) Beweisen Sie, dass das Polynom $p := X^2 + X + \overline{1}$ in $\mathbb{F}_2[X]$ irreduzibel ist, mit anderen Worten, es gibt **keine** $a, b \in \mathbb{F}_2$ so, dass

$$X^2 + X + \overline{1} = (X + a)(X + b).$$

   Es gilt nun allgemein für einen Körper k und ein Polynom $p \in k[X]$:

$$k[X]/p \cdot k[X] \text{ ist genau dann ein Körper, wenn } p \text{ irreduzibel ist.}$$

   (b) $\mathbb{F}_2[X]/p \cdot \mathbb{F}_2[X]$ ist also ein Körper! Stellen Sie seine Additions- und Multiplikationstafel auf.

Bitte wenden!

Zusatzaufgabe (4 Punkte): Beweisen Sie die allgemeine Tatsache aus (a): $k[X]/p \cdot k[X]$ ist genau dann ein Körper, wenn p irreduzibel ist.

Hinweis: Nutzen Sie die Tatsache, dass für einen linearen Endomorphismus zwischen endlich-dimensionalen Vektörräumen über k, injektiv und surjektiv gleichbedeutend sind (folgt z.B. aus der Dimensionsformel). Wenden Sie dies auf den endlich-dimensionalen k-Vektorraum $k[X]/p \cdot k[X]$ und den Endomorphismus $x \mapsto x \cdot q$ an (diese Abbildung ist offensichtlich genau dann bijektiv, wenn q invertierbar ist).

4. **Zyklische Gruppen.** Seien $M > 0$ und $N > 0$ zwei teilerfremde natürliche Zahlen, also so dass $\mathrm{ggT}(M, N) = 1$. Konstruieren Sie einen Gruppenisomorphismus (mit Begründung!):

$$(\mathbb{Z}/(MN)\mathbb{Z}) \to (\mathbb{Z}/M\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z}).$$

Zur Erinnerung: Für zwei Gruppen G und H bezeichnet $G \times H$ die Menge der Paare (g, h), wobei $g \in G$ und $h \in H$, mit der Verknüpfung:

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 \circ g_2, h_1 \circ h_2).$$

In dieser Aufgabe ist die Verknüpfung auf der rechten Seite natürlich die Operation „+“.

Abgabe am 9.7.2012 im Hörsaal vor Beginn der Vorlesung