Dr. Markus Junker — Mathematik II für Informatiker — Sommer 2012
Übungsblatt 9

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

1. **Das Zentrum der GL_N.** Sei k ein Körper und $\mathrm{GL}_N(k)$ die Gruppe der invertierbaren $N \times N$-Matrizen über k. Beweisen Sie:

$$Z(\mathrm{GL}_N(k)) = \left\{ \left. \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \lambda & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda \end{pmatrix} \right| \lambda \in k^* \right\}.$$

Hinweis: Untersuchen Sie die Vertauschungsbedingung für die Vertauschung mit geeigneten Elementarmatrizen explizit.

2. **Die Einheitengruppe der Restklassen.** Erinneren Sie die Definition der Restklassen modulo N, die wir mit $\mathbb{Z}/N\mathbb{Z}$ bezeichnet hatten.

Definiere
$$(\mathbb{Z}/N\mathbb{Z})^* := \{\overline{x} \in \mathbb{Z}/N\mathbb{Z} \mid \mathrm{ggT}(x, N) = 1\}.$$

(a) Zeigen Sie, dass dies eine sinnvolle Definition ist, d.h. dass die Bedingung $\mathrm{ggT}(x, N) = 1$ nicht von der Wahl des Vertreters x abhängt.

(b) Beweisen Sie, dass die Menge $(\mathbb{Z}/N\mathbb{Z})^*$ bzgl. der Operation „$\cdot$" eine Gruppe bildet.
Sie dürfen sich hier darauf beschränken, die Existenz des Inversen zu zeigen. Die anderen Axiome kann man mit einigem Geschick formal aus der Gültigkeit für ganze Zahlen folgern, was nicht so interessant ist.

(c) Bestimmen Sie für die Gruppen $(\mathbb{Z}/5\mathbb{Z})^*$ und $(\mathbb{Z}/8\mathbb{Z})^*$ die Gruppentafel. Welche Ordnung haben diese beiden Gruppen? Welche der beiden Gruppen sind zyklisch?

3. **Der euklidische Algorithmus** (2 Punkte). Wenden Sie den euklidischen Algorithmus auf die Zahlen 26 und 42 an, und finden Sie eine Darstellung

$$x \cdot 26 + y \cdot 42 = \mathrm{ggT}(26, 42).$$

mit ganzen Zahlen x und y. Geben Sie alle Zwischenschritte an.

Bitte wenden!

*4. **Kern und Bild** (6 Punkte). Betrachten Sie die Drehgruppe G des Würfels mit 24 Elementen. G permutiert die 4 Diagonalen des Würfels und die 3 Koordinatenachsen. Durch Nummerierung der 4 Diagonalen erhalten wir daher einen Homomorphismus (Warum?)

$$\rho : G \to S_4,$$

sowie durch Nummerierung der 3 Koordinatenachsen einen Homomorphismus

$$\mu : G \to S_3.$$

(a) Zeigen Sie, dass $\ker(\rho) = \{\mathrm{id}\}$ ist. Es folgt, dass ρ sogar bijektiv, also ein Isomorphismus ist, da beide Gruppen 24 Elemente haben.

(b) Schliessen Sie, dass es einen nicht-trivialen Homomorphismus

$$\mu \circ \rho^{-1} : S_4 \to S_3$$

gibt, und bestimmen Sie dessen Kern und Bild.

Hinweis für (b): Überlegen Sie sich, dass die Bestimmung des Kerns darauf hinausläuft, erstens alle Drehungen des Würfels zu identifizieren, die sämtliche 3 Koordinatenachsen festhalten (also höchstens deren Richtung umkehren), und zweitens zu bestimmen, wie die entsprechenden Drehungen auf den 4 Diagonalen operieren.

Motivation: Man kann zeigen, dass dies der einzige *nicht-triviale surjektive Homomorphismus zwischen symmetrischen Gruppen*

$$S_n \to S_m$$

für $n > m \geq 3$ ist.

Abgabe am 2.7.2012 im Hörsaal vor Beginn der Vorlesung