Dr. Markus Junker — Mathematik II für Informatiker — Sommer 2013
Übungsblatt 10

Verantwortlich für die Übungen:
Dr. Blaž Mramor (blaz.mramor@math.uni-freiburg.de)

1. **Kern und Bild**. Betrachten Sie einen 3-dimensionalen Würfel und bezeichnen Sie die vier Diagonalen des Würfels mit a, b, c, d und die drei Mittelsenkrechten mit α, β, γ.

   Die Drehgruppe G des Würfels permutiert die 4 Diagonalen des Würfels und die 3 Mittelsenkrechten. Man bekommt also einen Homomorphismus

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

   und kann sich überlegen, dass dies ein Isomorphismus ist. (Beweis ist auf der Webseite zu finden.)

   Außerdem permutiert G die drei Mittelsenkrechten, also bekommt man einen Homomorphismus

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

   (a) Geben Sie zu jedem Element $\sigma \in S_4$ das Bild $\mu(\sigma) \in S_3$ an und bestimmen Sie den Kern von μ.

   (b) Zu welcher aus der Vorlesung bekannten Gruppe ist der Kern isomorph?

   Hinweis: Überlegen Sie sich, dass die Bestimmung des Kerns darauf hinausläuft, erstens alle Drehungen des Würfels zu identifizieren, die sämtliche 3 Mittelsenkrechten als Menge 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.

2. **Zyklische Einheitengruppen, diskreter Logarithmus.** Bestimmen Sie für alle Elemente von $(\mathbb{Z}/13\mathbb{Z})^*$ die Ordnung. Sie werden feststellen, dass $(\mathbb{Z}/13\mathbb{Z})^*$ zyklisch ist.

   Wählen Sie sich einen der Erzeuger ξ und geben Sie explizit den Gruppenisomorphismus

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

   welcher ξ auf $\overline{1} = 1 + 12\mathbb{Z}$ abbildet, als Wertetabelle an. (Es gilt also $\overline{x} = \alpha_\xi(\xi^{\overline{x}})$, deshalb heißt α_ξ auch diskreter Logarithmus.)

Bitte wenden!

3. **Euklidischer Algorithmus für Polynome.**

   Division mit Rest für Polynome: Sei k ein Körper und $q, p \in k[X]$ zwei Polynome, wobei $\operatorname{Grad} q \geq \operatorname{Grad} p$. Wenn man q durch p teilt, sucht man zwei Polynome $k, r \in k[X]$, so dass $q = k \cdot p + r$, wobei der Grad von r minimal sein soll (mindestens kleiner als der Grad von p).

   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 $a_i \in \mathbb{F}_2 = \{0, 1\}$. Multipliziert werden diese Polynome durch Ausmultiplizieren, z.B. $(X + 1)^2 = X^2 + 2X + 1 = X^2 + 1$.

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

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

   $$X^2 + X + 1 = (X + a)(X + b).$$

   (b) Ohne Beweis verwenden wir: Für einen Körper k und ein Polynom $p \in k[X]$ gilt:

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

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

   Hinweis: Finden Sie Polynome von Grad ≤ 1 als Repräsentanten der Nebenklassen.

Abgabe am 1.7.2013 im Hörsaal vor Beginn der Vorlesung