Prof. Dr. U. Görtz **Sommersemester 2011**
Dr. U. Terstiege
A. Herrmann

Lineare Algebra II

9. Übungsblatt

Abgabe: Mittwoch, 08. Juni 2011 vor der Vorlesung (Postfach 7 in T03 R03)

Aufgabe 1

Sei p eine Primzahl. Nutze den Satz von Euler-Lagrange, um den kleinen Satz von Fermat zu beweisen: Für jedes $a \in \mathbb{Z}$, das teilerfremd zu p ist, gilt $a^{p-1} \equiv 1 \mod p$. Folgere, daß $a^p \equiv a \mod p$ für jedes $a \in \mathbb{Z}$.

Aufgabe 2

Sei $n \in \mathbb{N}$ und $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$ ein Gruppenhomomorphismus.

a) Zeige, daß das Bild $\operatorname{im}\varphi$ eine Untergruppe von $\mathbb{Z}^n$ ist, und daß es einen eindeutig bestimmten Endomorphismus $\varphi_{\mathbb{Q}}$ des $\mathbb{Q}^n$ gibt, dessen Einschränkung auf $\mathbb{Z}^n$ die Abbildung φ ist.

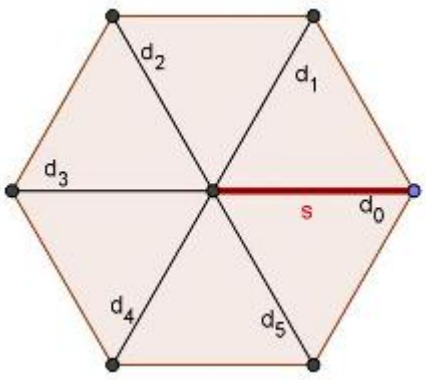
b) Zeige, daß φ genau dann injektiv ist, wenn der Quotient $\mathbb{Z}^n/\operatorname{im}\varphi$ eine endliche Gruppe ist. (*Hinweis:* Zeige zunächst, daß φ genau dann injektiv ist, wenn $\varphi_{\mathbb{Q}}$ injektiv ist. Überlege dann zunächst, wie man die Behauptung für $n = 1$ zeigen kann, und verallgemeinere dann auf beliebiges n.)

Aufgabe 3

Für die RSA-Verschlüsselung habe jemand folgende Zahlen gewählt (Notationen wie in der Vorlesung): $N = 901$ und $e = 123$. Bestimme eine geeignete Zahl d zur Dekodierung.

Aufgabe 4

Ein 6-Eck kann durch verschiedene Drehungen (entgegen dem Uhrzeigersinn) wieder in sich selbst überführt werden (d_0 := Drehung um 0°, d_1 := Drehung um 60°, ..., d_5 := Drehung um 300°). Diese Drehungen bilden zusammen mit der Hintereinanderausführung als Verknüpfung eine abelsche Gruppe $G = \{d_0, d_1, \ldots, d_5\}$. Ein Drehung lässt sich dabei durch die „Speichen“ des 6-Ecks veranschaulichen. Wir greifen uns eine feste Speiche s heraus und schauen wo sie nach der Drehung d_i zum Liegen kommt. Die Gruppe sieht damit so aus:



a) Bestimmen Sie die kleinste Untergruppe U von G, die d_2 enthält.
(*Hinweis: Überlegen Sie, welche weiteren Elemente in jedem Fall noch in der Untergruppe liegen müssen.*)
Skizzieren Sie die Untergruppe U anhand der Veranschaulichung mit „Speichen".

b) Aus welchen Elementen $(x + U)$ besteht der Quotient G/U? Skizzieren Sie die Elemente von G/U wie oben (möglichst farblich).

c) Zeigen Sie, dass G isomorph zu $\mathbb{Z}/6\mathbb{Z}$ ist ($6\mathbb{Z} = \{6 \cdot l \mid l \in \mathbb{Z}\}$). (*Anleitung:* Definieren Sie auf geeignete Weise Drehungen d_k für $k \in \mathbb{Z}$. Überlegen Sie, wann zwei Drehungen d_k und $d_{k'}$ gleich sind und begründen Sie so, dass die von Ihnen definierten d_k in der Gruppe G liegen. Finden Sie dann eine surjektive Abbildung $\varphi : \mathbb{Z} \to G$ mit $\ker \varphi = 6\mathbb{Z}$. Wenden Sie schließlich den Homomorphiesatz für Gruppen - Satz 4.6 in den Vorlesungsnotizen - auf φ an.)

Präsenzaufgabe

Sei $p = 3, q = 7$ und $e = 5$. Verschlüssele mit der RSA-Methode die Zahl 3. Finde ein geeignetes d zur Dekodierung und entschlüssele das Ergebnis zur Probe wieder.