TECHNISCHE UNIVERSITÄT DRESDEN

Bereich Mathematik und Naturwissenschaften Fakultät Mathematik, Institut für Algebra

Jun.-Prof. Martin Schneider, Dr. C. Zschalig

Algebra und Zahlentheorie für Lehramt (Modul ALGZTH), Sommersemester 2019

14. Übungsblatt für die Übungen vom 8.7.-12.7.2019

Wiederholung, Anwendung

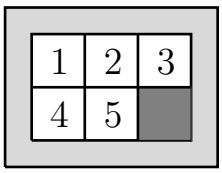
N14.1 **Hausaufgabe (Nachbereitung) Abgabe vor Übungsbeginn**
Verschlüsseln Sie Ihren Nachnamen mit dem RSA-Verfahren mit dem öffentlichen Schlüssel $(n, e) = (33, 13)$. Führen Sie dazu folgende Schritte aus:

(i) Codieren Sie die Buchstaben $A_1, \ldots, A_n$ Ihres Nachnamens durch $m_1, \ldots, m_n \in \mathbb{Z}_{33}$ durch die Zuordnung $\mathrm{A} \to 2, \mathrm{B} \to 3, \ldots, \mathrm{Z} \to 27, \ddot{\mathrm{A}} \to 28, \ddot{\mathrm{O}} \to 29, \ddot{\mathrm{U}} \to 30, \ß \to 31$.

(ii) Bestimmen Sie zu jedem Klartextbuchstaben m_i den Geheimtextbuchstaben c_i.
Bewertet wird die sorgfältige Formulierung des Lösungsweges, nicht nur das Ergebnis.

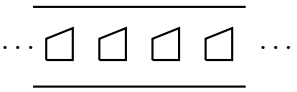
Bestimmen Sie den privaten Schlüssel d mit Hilfe des erweiterten Euklidischen Algorithmus und entschlüsseln Sie den entstandenen Geheimtext.

Ü14.2 Ein Schiebepuzzle besteht aus 15 Schiebeplättchen in einem 4×4-Raster, die von 1 bis 15 nummeriert sind und in die richtige Reihenfolge gebracht werden müssen. Das letzte Feld bleibt leer, um Plättchen verschieben zu können. Wir betrachten hier eine verkleinerte Version eines 2×3-Rasters, um die bekannte Tatsache zu begründen, dass keine zwei benachbarten Plättchen regelgerecht vertauscht werden können, ohne dass andere Plättchen ihren Platz verändern.
Modellieren Sie die Situation mit Hilfe von Permutationen, insbesondere Transpositionen!

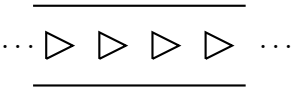


Ü14.3 Eine *Friesgruppe* ist die Symmetriegruppe einer ins Unendliche verlängerten bandartigen Struktur. Kennzeichen einer Friesgruppe ist, dass die Untergruppe der Translationen zyklisch ist. In dieser Aufgabe sollen einige Friesgruppen gefunden werden:

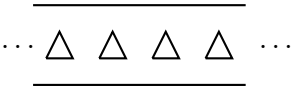
(a) Bestimmen Sie alle Symmetrieabbildungen F_1, des rechtsstehenden (ins unendlich verlängerten) Frieses. Zu welcher bekannten Gruppe ist die Menge der Symmetrieabbildungen F_1 zusammen mit der Hintereinanderausführung $\circ$ isomorph?



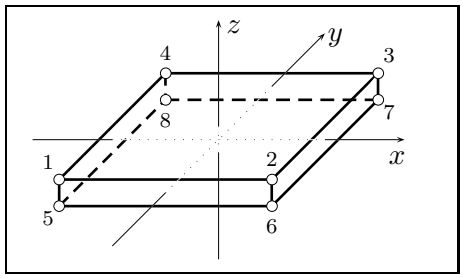
(b) Zeigen Sie, dass die Symmetriegruppe des rechts stehenden Frieses isomorph zu $\underline{\mathbb{Z}} \times \underline{\mathbb{Z}_2}$ ist.



(c) Beschreiben Sie die Symmetriegruppe des rechts stehenden Frieses. Ist sie isomorph zu $\underline{\mathbb{Z}} \times \underline{\mathbb{Z}_2}$?



Ü14.4 Ein Quader mit quadratischer Grundfläche (Seitenlänge a und Höhe $b \neq a$) besitzt u.a. offenbar folgende Symmetrieabbildungen: Drehung d entlang der senkrechten Drehachse z (um 90° im math. positiven Drehsinn) und die Spiegelung h an der x-y-Ebene.
Hinweis: Weitere Symmetrieabbildungen des Quaders spielen in der Aufgabe keine Rolle.



(a) Beschreiben Sie d und h als Permutationen der Eckenmenge $\{1, \ldots, 8\}$.

(b) Beweisen Sie mit Hilfe der Permutationsdarstellungen aus (a), dass $d \circ h = h \circ d$ gilt.

(c) Beweisen Sie mit Hilfe der Permutationsdarstellungen aus (a), dass sich die „Punktspiegelung am Ursprung“ $s = (17)(35)(46)(28)$ mit Hilfe von h und d darstellen lässt.

(d) Für die Menge $S = \langle\{d, h\}\rangle$ gilt $S = \{d^\alpha h^\beta \mid \alpha \in \{0,1,2,3\}, \beta \in \{0,1\}\}$ (das müssen Sie nicht beweisen). Zeigen Sie mit Hilfe von (b), dass $(S, \circ)$ abelsch ist.

(e) Zeigen Sie, dass $D = \{\mathrm{id}, d, d^2, d^3\}$ Normalteiler von S ist. Zu welcher bekannten Gruppe ist die Faktorgruppe S/D isomorph?

(f) Begründen Sie, dass $H := \langle h\rangle = \{\mathrm{id}, h\}$ ein Normalteiler ist. Zeigen Sie $d^2H = Hd^2$.

Die folgenden Selbststudiumsaufgaben dienen der Festigung und Vertiefung des Stoffes in der Nachbereitung der Lehrveranstaltung. Sie müssen nicht abgegeben werden.

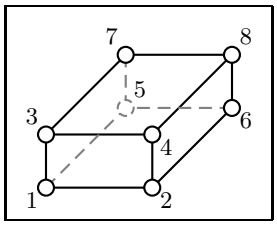
H14.5 Der $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ bildet bezüglich der Addition eine abelsche Gruppe $(\mathbb{R}^2, +)$. Es sei $u \in \mathbb{R}^2$ vom Nullvektor verschieden und U sei der von u erzeugte Untervektorraum.

(a) Begründen Sie, warum U eine Untergruppe von $(\mathbb{R}^2, +)$ ist. Ist U zyklisch?

(b) Da jede Untergruppe Normalteiler ist (warum?), lässt sich die Faktorgruppe $\mathbb{R}^2/U$ bilden. Wie kann man die Nebenklassen und die Addition in dieser Faktorgruppe geometrisch deuten?

(c) Gibt es einen surjektiven Homomorphismus $f : \mathbb{R}^2 \to \mathbb{R}$ auf die additive Gruppe $(\mathbb{R}, +)$, so dass $\mathrm{Ker}\, f = U$? (Wenn nein, Beweis; sonst Beispiel für f angeben.) Was besagt dann der Homomorphiesatz?

H14.6 Welche Bewegungen des Raums bilden einen Quader mit den Seitenlängen a, $2a$, $3a$ auf sich selbst ab? Beschreiben Sie sie durch Permutationen der Knotenmenge $\{1, 2, 3, 4, 5, 6, 7, 8\}$. Stellen Sie eine Gruppentafel auf. Bestimmen Sie zu jedem Element sein Inverses. Geben Sie eine Untergruppe der Ordnung 2 und eine Untergruppe der Ordnung 4 an.
Ist die Permutationsgruppe isomorph zu $(\mathbb{Z}_8, +)$?



H14.7* Eine *Parkettierung der Ebene* ist die Überdeckung von der Euklidischen Ebene $\mathbb{R}^2$ mit gleichförmigen Teilfiguren. Bestimmen Sie die Symmetriegruppe derjenigen Parkettierung, die entsteht, wenn übliches „Kästchenpapier“ ins Unendliche verlängert wird.