TECHNISCHE UNIVERSITÄT DRESDEN

Bereich Mathematik und Naturwissenschaften Fakultat Mathematik, Institut fur Algebra

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

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

6. Übungsblatt für die Übungen vom 6.5.-10.5.2019

Gruppen

N6.1 **Hausaufgabe (Nachbereitung) Abgabe vor Übungsbeginn**

(a) Bestimmen Sie mit square & multiply $7^x \pmod{17}$. Dabei ist x Ihre Matrikelnummer (als 7-stellige Zahl gelesen). Das Ergebnis sollte ein Element von $\mathbb{Z}_{17}$ sein.

(b) Finden Sie alle Paare (a, b) von Zahlen a, b aus $\mathbb{Z}_{12}$, die die Gleichung $5a^2 + 2b^2 \equiv 3 \pmod{12}$ erfüllen.
Hinweis: Lösen Sie zuerst die Gleichung $5x+2y \equiv 3 \pmod{12}$ und überlegen Sie dann, welche der Lösungen als Quadrate mod 12 darstellbar sind.

(c) Schreiben Sie Ihre Matrikelnummer auf. Die (von links gelesen) 5. Ziffer sei die Zahl a, die 6. Ziffer b und die 7. Ziffer c.
Bestimmen Sie die Lösungen des Kongruenzensystems

$$x \equiv a \,(\mathrm{mod}\, 5)$$
$$x \equiv b \,(\mathrm{mod}\, 6)$$
$$x \equiv c \,(\mathrm{mod}\, 7)$$

Die Aufgaben (a) und (c) sollten von jedem Mitglied Ihrer Gruppe separat gelöst werden.

V6.2 **Hausaufgabe (Vorbereitung) Abgabe vor Übungsbeginn**
Wir untersuchen in dieser Aufgabe die Gruppe $(\underline{\mathbb{Z}}_{15}^*, \cdot)$ (d.h. die Menge der Einheiten aus $\mathbb{Z}_{15}$ zusammen mit der Multiplikation $\pmod{15}$) (vgl. Vorlesung 2.28).

(a) Wie viele Elemente hat die Menge $\underline{\mathbb{Z}}_{15}^*$?

(b) Bestimmen Sie die Ordnungen aller Elemente. Geben Sie zu jedem Element sein Inverses an.
Hinweis: Nutzen Sie, dass $m \equiv m - 15 \,(\mathrm{mod}\, 15)$, also z.B. $13 \equiv -2 \,(\mathrm{mod}\, 15)$ gilt.

(c) Ist $(\underline{\mathbb{Z}}_{15}^*, \cdot)$ zyklisch?

(d) Finden Sie eine Untergruppe $(U, \cdot)$ von $(\underline{\mathbb{Z}}_{15}^*, \cdot)$, die isomorph zu $(\mathbb{Z}_4, +)$ ist (mit Begründung!)

(e) Finden Sie eine Untergruppe $(V, \cdot)$ von $(\underline{\mathbb{Z}}_{15}^*, \cdot)$, die isomorph zu $(V_4, +)$ (Kleinsche Vierergruppe) ist (mit Begründung!)

(f) Ist $(\mathbb{Z}_{15}, +, \cdot)$ ein Körper? Ist $(\underline{\mathbb{Z}}_{15}^*, +, \cdot)$ ein Körper? Begründen Sie Ihre Antworten!

Ü6.3 Beweisen Sie Bem. 3.5: Ist $(G, \circ)$ eine Gruppe und $A \subseteq G$ eine Teilmenge, dann gilt für die von A erzeugte Untergruppe $\langle A \rangle_{\underline{G}}$ die Beziehung

$$\langle A \rangle = \{a_1 \circ \ldots \circ a_n \mid n \in \mathbb{N} \setminus \{0\}, a_1, \ldots, a_n \in A \cup A^{-1} \cup \{e_{\underline{G}}\}\}.$$

Ü6.4 Die *Quaternionengruppe* $\underline{Q_8} = (Q_8, \circ)$ besteht aus $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$; die Gruppenoperation $\circ$ ist durch die folgenden Gleichungen eindeutig festgelegt:

(1) $\forall q \in Q_8 : 1 \circ q = q \circ 1 = q$ (2) $\forall q \in Q_8 : -1 \circ q = q \circ -1 = -q$
(3) $i \circ i = j \circ j = k \circ k = -1$ (4) $i \circ j = j \circ -i = k$
(5) $j \circ k = k \circ -j = i$ (6) $k \circ i = i \circ -k = j$
(7) $\forall q \in Q_8 : -(-q) = q$

(a) Bestimmen Sie $i \circ k$ und $j \circ i$; begründen Sie dabei Ihre Umformungsschritte durch die obigen Gleichungen.

(b) Stellen Sie die Gruppentafel auf.

(c) Bestimmen Sie alle Untergruppen der Quaternionengruppe.

Ü6.5 Beweisen Sie (vgl. Vorlesung 3.4):

Ist $(G, \cdot)$ eine Gruppe, $a \in G$ und $m, n \in \mathbb{N}$ beliebig, dann gilt:

(a) $a^{m+n} = a^m \cdot a^n$

(b) $(a^n)^{-1} = (a^{-1})^n$.

(c) Schlussfolgern Sie: Jede zyklische Gruppe ist abelsch.

Ü6.6 Ist G endlich und gilt $2 \mid |G|$, dann existiert ein $a \in G$ mit $\mathrm{ord}(a) = 2$.

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

H6.7 Beweisen Sie: Jede Untergruppe U von $(\mathbb{Z}, +)$ hat die Form

$$U = n\mathbb{Z} \quad \text{für ein} \quad n \in \mathbb{N} .$$

Dabei ist n die kleinste natürliche Zahl aus U.

H6.8 Zeigen Sie: eine Gruppe mit Primzahlordnung besitzt genau 2 Untergruppen.

Schlussfolgern Sie: Jede Gruppe von Primzahlordnung ist zyklisch.

H6.9 Beweisen Sie, dass jede Gruppe mit genau 4 Elementen abelsch ist.

H6.10 Bestimmen Sie die Operationstafel der Gruppe $(\mathbb{Z}_2^3, +)$ und der komponentenweisen Addition als Operation. Geben Sie alle Untergruppen an und begründen Sie, warum es keine weiteren Untergruppen gibt.