TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik und Naturwissenschaften Fachrichtung Mathematik, Institut für Algebra

Prof. Dr. A. Fehm, Dr. C. Zschalig

Algebra und Zahlentheorie (Modul ALGZTH), Sommersemester 2017

2. Übungsblatt für die Übungen vom 18.4.-21.4.2017

die ganzen Zahlen, Gruppen, Untergruppen

V7. **Vorbereitungsaufgabe: Bitte bereiten Sie diese Aufgabe zur Übung vor.**
Die *Einheitengruppe* $(\mathbb{Z}/n\mathbb{Z})^\times$ besteht aus allen Einheiten der Menge $\mathbb{Z}/n\mathbb{Z}$ zusammen mit der Multiplikation modulo n. Stellen Sie die Gruppentafel auf und bestimmen Sie alle Untergruppen für:
(a) $n = 10$, (b) $n = 12$, (c) $n = 24$.

Hinweis: Anstelle der Menge der Restklassen $\mathbb{Z}/n\mathbb{Z} := \{n\mathbb{Z} + k \mid k \in \mathbb{Z}\}$ wird oft die Menge der Reste $\mathbb{Z}_n := \{0, \ldots, n-1\}$ betrachtet. Da die Addition und Mutliplikation $\pmod n$ *repräsentantenunabhängig* ist, sind die zugehörigen Ringe $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ und $(\mathbb{Z}_n, +, \cdot)$ isomorph.

Ü8. (a) Berechnen Sie zu den angegebenen Paaren (a, b) den größten gemeinsamen Teiler und stellen Sie diesen als ganzzahlige Linearkombination von a und b (d.h. als $\operatorname{ggT}(a, b) = \alpha \cdot a + \beta \cdot b, \quad \alpha, \beta \in \mathbb{Z}$) dar. Verifizieren Sie Ihre Ergebnisse!

(i) $a = 24, b = 135$, (ii) $a = 21, b = 34$ (iii) $a = 94, b = 127$, (iv) $a = 511, b = 1001$

(b) Berechnen Sie $\operatorname{ggT}(\operatorname{ggT}(150, 105), 56) = \alpha \cdot 150 + \beta \cdot 105 + \gamma \cdot 56$ $(\alpha, \beta, \gamma \in \mathbb{Z})$. Zeigen Sie, dass beliebige Zahlen $a, b, c \in \mathbb{Z}$ die Beziehung $\operatorname{ggT}(\operatorname{ggT}(a, b), c) = \operatorname{ggT}(a, \operatorname{ggT}(b, c))$ erfüllen.

(c) Besitzen die folgenden Elemente x ein Inverses in $\mathbb{Z}_n$? Berechnen Sie ggf. das Inverse $x^{-1} \pmod n$.

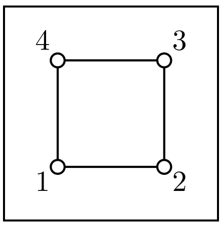
(i) $x=18, n=31$, (ii) $x=60, n=257$, (iii) $x=511, n=1001$, (iv) $x=512, n=1001$.

Ü9. (a) Beweisen Sie, dass für beliebige ganze Zahlen $a, b, c, d, s, t \in \mathbb{Z}$ folgende Implikationen gelten:

(i) $a|b \wedge c|d \implies ac|bd$, (ii) $a|b \wedge a|c \implies a|(sb + tc)$.

(b) Beweisen Sie für beliebige Zahlen $a, b, c \in \mathbb{N}$ folgende Beziehungen:
(i) $\operatorname{ggT}(ac, bc) = \operatorname{ggT}(a, b) \cdot c$
(ii) $\operatorname{ggT}\left(\frac{a}{\operatorname{ggT}(a,b)}, \frac{b}{\operatorname{ggT}(a,b)}\right) = 1$
(iii) $b|(a \cdot c) \wedge \operatorname{ggT}(a, b) = 1 \implies b|c$
(iv) $a|c \wedge b|c \wedge \operatorname{ggT}(a, b) = 1 \implies (a \cdot b)|c$

Ü10. Welche Bewegungen der Ebene bilden ein Quadrat auf sich selbst ab? Beschreiben Sie diese durch Permutationen der Knotenmenge $\{1, 2, 3, 4\}$ des rechts gegebenen Quadrats. Mit der Hintereinanderausführung bilden die Permutationen eine Gruppe, die *Diedergruppe* D_4. Stellen Sie eine Gruppentafel auf. Geben Sie zu jedem Element sein Inverses an und bestimmen Sie seine Ordnung.



Bitte wählen Sie 2 der folgenden 3 Hausaufgaben zur Abgabe aus.

A11. **Hausaufgabe, bitte bis zum 27.4.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**

(a) Zeigen Sie: Sind $a, b \in \mathbb{N}$ mit Primfaktorzerlegungen $a = \prod_{i=1}^{r} p_i^{\alpha_i}$ und $b = \prod_{i=1}^{r} p_i^{\beta_i}$ (mit Primzahlen $p_1, \ldots p_r$ und Exponenten $\alpha_i, \beta_i \geq 0$), dann gilt $a|b \iff \forall i \in \{1, \ldots, r\} : \alpha_i \leq \beta_i$.

(b) (i) Bestimmen Sie den größten gemeinsamen Teiler $\mathrm{ggT}(m, n)$ und das kleinste gemeinsame Vielfache $\mathrm{kgV}(m, n)$ der beiden Zahlen $m = 240 = 2^4 \cdot 3 \cdot 5$ und $n = 396 = 2^2 \cdot 3^2 \cdot 11$. Bilden Sie die Produkte $m \cdot n$ und $\mathrm{ggT}(m, n) \cdot \mathrm{kgV}(m, n)$. Was stellen Sie fest?

(ii) Beweisen Sie: Für je zwei natürliche Zahlen m, n gilt $m \cdot n = \mathrm{ggT}(m, n) \cdot \mathrm{kgV}(m, n)$.

A12. **Hausaufgabe, bitte bis zum 27.4.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**
Schreiben Sie Ihre Matrikelnummer (7-stellig) auf. Die letzten drei Ziffern bilden (als dreistellige Zahl gelesen) die Zahl z. Die Zahl y erhalten Sie nach der Vorschrift:

$$y := \begin{cases} z, & z > 99 \\ z + 100, & z \leq 99 \end{cases}$$

Bestimmen Sie mit dem Euklidischen Algorithmus den ggT von 1009 und y und stellen Sie ihn als Linearkombination von 1009 und y dar. Finden Sie das Inverse von y in $(\mathbb{Z}_{1009}, \cdot)$ oder begründen Sie, warum das Inverse nicht existiert. Machen Sie eine Probe!

A13. **Hausaufgabe, bitte bis zum 27.4.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**
Es sei G eine Gruppe mit neutralem Element e. Beweisen Sie die folgenden Aussagen:

(a) Gilt für alle $a, b \in G$ die Beziehung $(ab)^2 = a^2 b^2$, dann ist G abelsch.

(b) Gilt für alle $a \in G$ die Beziehung $a^2 = e$, dann ist G ist abelsch.

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

(d)* Existiert eine natürliche Zahl n, so dass für alle $a, b \in G$ und $\alpha \in \{n, n+1, n+2\}$ die Beziehung $(ab)^\alpha = a^\alpha b^\alpha$ gilt, dann ist G abelsch.

H14. Zeigen Sie, dass die Matrizen $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbb{C}^{2\times 2}$ und $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathbb{C}^{2\times 2}$ bezüglich der Matrixmultiplikation eine Untergruppe der Gruppe $\mathrm{GL}(2, \mathbb{C})$ der Ordnung 8, die sogenannte *Quaternionengruppe* Q_8 erzeugen:

(a) Bestimmen Sie die Ordnungen von A und B.

(b) Zeigen Sie, dass sich alle Elemente von Q_8 in der Form $A^n B^m$ (für geeignete $m, n \in \mathbb{N}_0$) schreiben lassen.

(c) Stellen Sie eine Gruppentafel auf.

(d) Die Diedergruppe D_4 hat ebenfalls 8 Elemente. Vergleichen Sie die Ordnungen der Elemente beider Gruppen, um zu entscheiden, ob die Gruppen D_4 und Q_8 zueinander isomorph sind.

H15. Finden Sie die kleinste natürliche Zahl $n \in \mathbb{N}$ mit der Eigenschaft

$$p | n \iff (p-1) | n \qquad \text{für alle Primzahlen } p.$$

Hinweis: Solch eine Zahl gibt es wirklich. Allerdings ist das Finden der Lösung durch pures Probieren sehr aufwendig. Falls Sie (bei 1 beginnend) pro Zahl 1 Minute zum Überprüfen brauchen, werden Sie n erst nach mehr als einem Tag finden.

H16. Beweisen Sie Lemma 1.9 aus der Vorlesung: Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:

(1) $f(1) = 1$.

(2) $\forall x \in G : f(x^{-1}) = (f(x))^{-1}$.

(3) $\forall x_1, \ldots, x_n \in G : f(x_1 \cdot \ldots \cdot x_n) = f(x_1) \cdot \ldots \cdot f(x_n)$.

(4) $G_0 \leq G \implies f(G_0) \leq H$.

(5) $H_0 \leq H \implies f^{-1}(H_0) \leq G$.