

**Aufgabe 1**

Gegeben sei die Gruppe  $(\mathbb{Z}_4, \oplus_4)$ .

Nehmen Sie die 0 aus dieser Gruppe heraus und konstruieren Sie aus den restlichen drei Elementen eine Multiplikationsgruppe  $(\mathbb{Z}_4 \setminus \{0\}, \odot_4)$ , wobei 3 das neutrale Element sein soll.

Zeigen Sie an einem Beispiel, dass diese beiden Gruppen das Distributivgesetz verletzen und die Struktur  $(\mathbb{Z}_4, \oplus_4, \odot_4)$  offensichtlich kein Körper ist.

**Aufgabe 2**

Geben Sie an, zu welchen Zahlen  $q$  Sie einen Körper mit  $q$  Elementen konstruieren können und begründen Sie Ihre Antwort:

- a) 5      b) 15      c) 25      d) 39      e) 49      f) 59      g) 99      h) 121

**Aufgabe 3**

Schreiben Sie die Elemente der Gruppentafel für die multiplikative Gruppe von  $\text{GF}(8)$  von Folie DM5-21 in den Zeilen und Spalten in einer solchen Reihenfolge auf, dass man auf den ersten Blick sieht, dass die Gruppentafel zyklisch ist.

**Aufgabe 4**

Überprüfen Sie die Berechnung der folgenden Elemente aus  $\text{GF}(8)$  und  $\text{GF}(9)$  durch entsprechende Polynommultiplikation und eventuelle anschließende Reduktion mit Hilfe des irreduziblen Polynoms:

- a) aus Tabelle DM5-21:  
 $5 \odot 6, 7 \odot 4, 3 \odot 3$
- b) aus Tabelle DM5-22:  
 $6 \odot 3, 7 \odot 2, 5 \odot 5$

**Aufgabe 5**

- a) Geben Sie alle Elemente aus  $\text{GF}(25)$  in Polynomschreibweise an.
- b) Berechnen Sie  $(x + 4) \cdot (3x + 2)$ . (Finden Sie dafür ein geeignetes irreduzibles Polynom und weisen Sie die Irreduzibilität explizit nach!)

**Aufgabe 6**

- Berechnen Sie das Polynom  $(3x^4 + 4x^3 + 2x)$  modulo  $(x^3 + x + 4)$  in  $\mathbb{Z}_5[x]$ .
- Für welchen Körper ist diese Berechnung relevant?
- Welche Bedingung muss erfüllt sein, damit Sie diese Rechnung hier zur Erstellung einer Multiplikationstabelle verwenden können? Ist diese Bedingung hier erfüllt? (Begründung!)

**Aufgabe 7**

Untersuchen Sie den Körper mit 125 Elementen und vergleichen Sie Ihre Resultate mit einem der zur Verfügung stehenden Programme über Endliche Körper (herunterzuladen von der Seite: <http://intern.fh-wedel.de/mitarbeiter/iw/f-e/fertig/sw-projekte/galoisfeld/>)

- Geben Sie ein geeignetes irreduzibles Polynom an und weisen Sie die Irreduzibilität explizit nach!  
Hinweis: Arbeiten Sie mit möglichst kleinen Koeffizienten! Man findet schnell einen geeigneten Kandidaten.
- Überprüfen Sie das Resultat von  $60 \oplus 40$ , indem Sie die Vektoraddition explizit durchführen!
- Überprüfen Sie das Resultat von  $60 \odot 40$ , indem Sie die Polynommultiplikation und anschließende Reduktion explizit durchführen!
- Überprüfen Sie die Resultate von  $60 \ominus 40$  und  $60 \oslash 40$ , indem Sie diese mit jeweils einer anderen Operation im selben Programm überprüfen! Geben Sie auf dem Lösungsblatt an, mit welchen Operationen Sie das überprüft haben!  
Hinweis: Eines der 3 Programme arbeitet bei diesen Operationen fehlerhaft!

**Aufgabe 8**

- Stellen Sie mit Venn-Diagrammen den allgemeinen Fall dar, wie vielfach Elemente in anderen Mengen liegen können, wenn 4 Mengen vorgegeben sind. Geben Sie für jedes der entstehenden Gebiete an, in wie vielen Mengen gleichzeitig ein Element liegt, wenn es zu diesem Gebiet gehört.  
Hinweis: Stellen Sie 3 Mengen durch Kreise dar und die 4. durch eine bananen- oder wurstartige Form.
- Geben Sie die Siebformel für 4 Mengen explizit an.