Mathematisches Institut
Georg-August-Universität Göttingen
Prof. Dr. E. Viada, Dr. V. Cantoral

Diskrete Mathematik
Wintersemester 2023/24

Lösungen zu Übungsblatt 7.

Aufgabe 1 (10 Punkte)**.**

(i) Zeigen Sie, dass alle Restklassen $\mod 4$ mit der Operation $+$, definiert durch

$$\bar{a} + \bar{b} := \overline{a+b}$$

eine kommutative Gruppe bildet.

(ii) Zeigen Sie, dass die Restklassen $\bar{1}, \bar{2}, \bar{3} \mod 4$ mit der Operation $\cdot$, definiert durch

$$\bar{a} \cdot \bar{b} := \overline{a \cdot b}$$

keine Gruppe bildet.

Lösung zu Aufgabe 1. Lösung zu i) (5 Punkte): Wir sehen, dass

(i) $\bar{0}$ ist das neutrale Element, da $\bar{a} + \bar{0} = \overline{a+0} = \bar{a}$,

(ii) $\overline{-a}$ ist das Inverse zu $\bar{a}$,

(iii) die Verknüpfung ist kommutative, da $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$,

(iv) die Verknüpfung ist assoziativ, da $(\bar{a}+\bar{b})+\bar{c} = \overline{a+b}+\bar{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \bar{a}+(\overline{b+c}) = \bar{a} + (\bar{b}+\bar{c})$.

Lösung zu ii) (5 Punkte): Wir haben $\bar{2} \cdot \bar{1} = \bar{2}$, $\bar{2} \cdot \bar{2} = \bar{0}$, $\bar{2} \cdot \bar{3} = \bar{6} = \bar{2}$. Somit hat $\bar{2}$ kein Inverses und daher ist die Operation keine Gruppe.

Aufgabe 2 (10 Punkte)**.**

(i) Bestimmen Sie die Einheitengruppe $(\mathbb{Z}/8\mathbb{Z})^*$, d.h. die bzgl. der Multiplikation invertierbaren Elemente in $\mathbb{Z}/8\mathbb{Z}$, und geben Sie zu jedem Element aus $(\mathbb{Z}/8\mathbb{Z})^*$ das Inverse an.

(ii) Zeigen Sie, dass $\mathbb{Z}/8\mathbb{Z}$ ein Ring. Ist dies ein Körper?

(iii) Zeigen Sie, dass $\mathbb{Z}/7\mathbb{Z}$ ein Körper ist.

Lösung zu Aufgabe 2. Lösung zu i) (2 Punkte): Wir wissen, dass $(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{a} : \mathrm{ggT}(8, \mathrm{a}) = 1\}$. Nun sind genau 1, 3, 5, 7 (aus dem Repräsentantensystem $\{1, \ldots, 8\}$) teilerfremd zu 8 und damit ist $(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. Die Inversen sind:

$$\bar{1} \cdot \bar{1} = \bar{1}, \quad \bar{3} \cdot \bar{3} = \bar{1} \quad \bar{5} \cdot \bar{5} = \bar{1} \quad \bar{7} \cdot \bar{7} = \bar{1}$$

Zu ii) (4 Punkte): Wegen $\bar{4} \cdot \bar{4} = \bar{0}$ ist $\mathbb{Z}/8\mathbb{Z}$ kein Körper. In einem Körper K gilt stets $ab \neq 0$ für $a, b \neq 0$. (Man spricht auch von Nullteilerfreiheit. Begründung: Ist $ab = 0$ mit $a \neq 0$, so folgt $0 = a^{-1}ab = b$, da jedes Element $\neq 0$ in einem Körper ein Inverses hat).

Die Ringaxiome vererben sich aus $\mathbb{Z}$, da die Operationen über die Repräsentant definiert sind und dies (wie nachgewiesen) wohldefiniert ist. Hierbei ist $\bar{0}$ das neutrale Element bzgl. der Addition, $\bar{1}$ ist das neutrale Element bzgl. der Multiplikation und der Ring ist kommutativ.

Zu iii) (4 Punkte): Dies ist ein Ring. Es bleibt zu prüfen, dass jedes Element $\neq 0$ ein Inverses besitzt. Dies aus der folgenden Multiplikationstabelle abzulesen:

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

In jeder Spalte bzw. Zeile findet sich die $\bar{1}$ wieder. Alternative: Wir bestimmten mit Hilfe des erweiterten euklidischen Algorithmus das Inverse.

- Wir haben $7 = 3 \cdot 2 + 1$ und damit ist $\bar{4} \cdot \bar{2} = \overline{-3} \cdot \bar{2} = \bar{1}$ und damit auch $\bar{3} \cdot \overline{-2} = \bar{3} \cdot \bar{5} = \bar{1}$.
- Auch gilt $7 = 1 \cdot 6 + 1$ und daher $\bar{6} \cdot \overline{-1} = \bar{6} \cdot \bar{6} = \bar{1}$.

Aufgabe 3 (10 Punkte)**.** Beweisen Sie, dass für alle Primzahlen p (und $a, b \in \mathbb{Z}$) gilt

$$(a+b)^p \equiv a^p + b^p \mod p$$

Hinweis: Zeigen Sie, dass der Binomialkoeffizient $\binom{p}{i}$ für $1 \leq i \leq p-1$ durch p teilbar ist.

Lösung zu Aufgabe 3. Der binomische Lehrsatz besagt (2 Punkte), dass

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}. \tag{1}$$

Nun ist für $1 \leq i \leq p-1$

$$\binom{p}{i} = p \frac{(p-1)!}{i!(p-i)!}.$$

der rechte Term eine ganze Zahl, da im Nenner nur Primzahlen $< p$ vorkommen können. D.h. $\binom{p}{i}$ ist für $1 \leq i \leq p-1$ durch p teilbar. (4 Punkte)

Nehmen wir (1) modulo p, so folgt daher

$$(a+b)^p = a^p + b^p,$$

da alle Terme mit $1 \leq i \leq p1$ durch p teilbar sind. (4 Punkte)

Aufgabe 4 (10 Punkte)**.** Zeigen Sie für $a, b, c, d \in \mathbb{Z}$ die folgenden Aussagen.

(i) Gilt $\mathrm{ggT(a, b)} = 1$, $c|a$ und $d|b$, so auch $\mathrm{ggT(c, d)} = 1$.

(ii) Gilt $a, b|c$ und $\mathrm{ggT(a, b)} = 1$, so ist $ab|c$.

Lösung zu Aufgabe 4. Lösung zu i) (5 Punkte): In der Primzahlzerlegung von c, bzw. von d, können nur Primzahlen vorkommen, die in a, bzw. b, vorkommen (wegen $c|a$, bzw. $d|b$). Wegen $\mathrm{ggT(a, b)} = 1$ kommen nur verschiedene Primzahlen vor und daher ist auch $\mathrm{ggT(c, d)} = 1$. Zu ii) (5 Punkte): In der Primzahlzerlegung von c können keine gemeinsamen Primzahlen von a und b auftreten, da a und b teilerfremd sind. Wegen $a|c$ und $b|c$ folgt daher sofort $ab|c$.

Zusatzaufgabe 5. Lea feiert ihren Geburtstag mit Pia und Mia. Es verbleiben noch 10 Bonbons, die vollständing auf die Kinder verteilt werden sollen.

(i) Wie viele verschiedene Möglichkeiten gibt es hierfür, wenn jedes Kind mindestens ein Bonbon erhalten soll.

(ii) Wie viele verschiedene Möglichkeiten gibt es hierfür, wenn Lea mindestens vier Bonbons erhalten soll.

Lösung zu Aufgabe 5. Lösung zu (i). (5 Punkte) Zunächst geben wir jedem der Mädchen einen Bonbon, da dies auf jeden Fall passieren muss. Damit bleiben noch sieben Bonbon zu verteilen, wobei es keine Einschränkungen mehr an die Verteilung gibt. Wir wählen jetzt also sieben mal eins der drei Mädchen aus, um ihr einen Bonbon zu geben, wobei uns die Reihenfolge nicht interessiert. Die Formel um $k = 7$ Elemente aus $n = 3$ Elementen mit Wiederholung und ohne Beachtung der Reihenfolge auszuwählen ergibt, dass die Anzahl der Möglichkeiten (2 Punkte) geben ist durch

$$\binom{n+k-1}{k} = \binom{9}{7} = 36.$$

Lösung zu (ii). (5 Punkte) Wir geben zunächst vier der Bonbons an Lea, da sie diese sowieso bekommt. Dann bleiben noch 6 Bonbons zu verteilen, ohne dass weitere Einschränkungen erfüllt werden müssen. Nach der Überlegung aus Teil (i) gibt es hierfür dann $\binom{8}{2} = 28$ Möglichkeiten (2 Punkte).