Dr. Markus Junker — Diskrete Algebraische Strukturen — Sommer 2011
Übungsblatt 3

Verantwortlich für die Übungen:
Dr. Fritz Hörmann (fritz.hoermann@math.uni-freiburg.de)

1. **Kern und Bild** (2 Punkte). Seien G und H zwei Gruppen und
$$f : G \to H$$
ein Gruppenhomomorphismus. Beweisen Sie, dass
$$\ker(f) = \{g \in G \mid f(g) = e\}$$
eine Untergruppe von G ist.
Beweisen Sie, dass
$$\mathrm{bild}(f) = \{f(g) \mid g \in G\}$$
eine Untergruppe von H ist.

2. **Restklassen** (8 Punkte). Sei $N > 0$ eine natürliche Zahl. Wir definieren auf der Menge $\mathbb{Z}$ der ganzen Zahlen die folgende Relation
$$x \sim y \;\Leftrightarrow\; N \text{ teilt } x - y,$$
d.h. zwei Zahlen heißen äquivalent, wenn ihre Differenz durch N teilbar ist.

   (a) Beweisen Sie, dass dies eine Äquivalenzrelation ist. Die zugehörigen Äquivalenzklassen werden **Restklassen** modulo N genannt. Die Menge dieser Restklassen bezeichnen wir mit $\mathbb{Z}/N\mathbb{Z}$. Die zu x gehörige Äquivalenzklasse wird mit $\overline{x}$ bezeichnet.

   (b) Begründen Sie, dass $\{0, \ldots, N-1\}$ ein Vertretersystem ist.

   (c) Zeigen Sie, dass
$$\overline{x} + \overline{y} := \overline{x + y}$$
und
$$\overline{x} \cdot \overline{y} := \overline{x \cdot y}$$
gültige Definitionen einer Operation auf der Menge der Restklassen sind, d.h. nicht von der Wahl der Vertreter x und y abhängen.

   (d) Zeigen Sie, dass die Menge der Restklassen zusammen mit der oben definierten Operation „+“ eine zyklische Gruppe mit N Elementen ist, also isomorph zu $\mathbb{Z}_N$ ist.

   (e) Definiere
$$(\mathbb{Z}/N\mathbb{Z})^* := \{\overline{x} \in \mathbb{Z}/N\mathbb{Z} \mid \mathrm{ggT}(x, N) = 1\}.$$
Zeigen Sie, dass dies eine sinnvolle Definition ist, d.h. dass die Bedingung $\mathrm{ggT}(x, N) = 1$ nicht von der Wahl des Vertreters x abhängt. Wir werden später sehen, dass die Menge $(\mathbb{Z}/N\mathbb{Z})^*$ bzgl. der Operation „$\cdot$“ eine Gruppe bildet. Rechnen Sie dies für die Mengen $(\mathbb{Z}/5\mathbb{Z})^*$ und $(\mathbb{Z}/8\mathbb{Z})^*$ nach. Welche Ordnung haben diese Gruppen? Welche der Gruppen sind zyklisch?

Bitte wenden!

3. **Der euklidische Algorithmus** (2 Punkte). Wenden Sie den euklidischen Algorithmus auf die Zahlen 26 und 42 an, und finden Sie eine Darstellung

$$x \cdot 26 + y \cdot 42 = \mathrm{ggT}(26, 42).$$

mit ganzen Zahlen x und y. Geben Sie alle Zwischenschritte an.

4. **Programmieraufgabe** (4 Punkte). Schreiben Sie eine Funktion, welche den g.g.T. zweier natürlicher Zahlen $a > 0$ und $b > 0$ mit dem euklidischen Algorithmus berechnet und eine Darstellung

$$x \cdot a + y \cdot b = \mathrm{ggT}(a, b).$$

mit ganzen Zahlen x und y findet. Wenden Sie dies auf die Zahlen $a := p^5 - 1$ und $b := p^8 - 1$, für $p \in \{2, 3, 5, 7, 11\}$ an. Vermutung?

Abgabe am 23.5.2011 im Hörsaal vor Beginn der Vorlesung