# 6. Übungsblatt zu Mathematik für Informatiker II, SS 2004

JOACHIM VON ZUR GATHEN & MICHAEL NÜSKEN

Abgabe bis Montag, 14. Juni 2004, $12^{23}$ Uhr
in den jeweils richtigen Kasten auf dem D1-Flur.

**Aufgabe 6.1** (Quadrismus). (7 Punkte)

Wir wollen untersuchen, was Quadrieren in den multiplikativen Gruppen $\mathbb{Z}_p^\times$ mit $p$ prim bewirkt.

(i) Zeichne für $p = 11, 13, 17$ je einen Graphen: Zeichne für jedes Element in $\mathbb{Z}_p^\times$ einen Punkt und von einem Element $x \in \mathbb{Z}_p^\times$ soll ein Pfeil zu dessen Quadrat $x^2$ zeigen. Ordne die Punkte dazu übersichtlich an.

(ii) Markiere alle Punkte, an denen Pfeile enden. Zähle zu jedem Punkt, wieviele Pfeile dort ankommen.

Betrachte nun allgemein die Quadrierungsabbildung

$$q\colon \begin{array}{ccc} \mathbb{Z}_p^\times & \longrightarrow & \mathbb{Z}_p^\times, \\ x & \longmapsto & x^2 \end{array}$$

für $p$ prim.

(iii) Zeige, dass $q$ ein Homomorphismus ist.

(iv) Bestimme den Kern $\ker q$ von $q$ und dessen Anzahl. [Ein Polynom vom Grad $n$ hat in einem Körper — wie $\mathbb{Z}_p$ für $p$ prim einer ist — höchstens $n$ Nullstellen.]

(v) Bestimme die Größe $\#\operatorname{im} q$ des Bildes von $q$.

**Aufgabe 6.2** (Verschiedene Moduln). (6 Punkte)

Betrachte folgenden Versuch einer Definition:

Sei $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$ die Abbildung mit $f(a \bmod m) = a \bmod n$.

(i) Wann ist das in Ordnung, wann ist die Abbildung wohldefiniert? [Unterscheide gegebenenfalls Fälle und gib Gegenbeispiele bzw. Beweise.]

(ii) Wann ist $f$ ein Homomorphismus?

(iii) Wann ist $f$ surjektiv?

(iv) Wann ist $f$ injektiv?

(v) Wann ist $f$ bijektiv?

**Aufgabe 6.3** (Zyklisch?). (5 Punkte)

Untersuche jeweils, ob die angegebene Gruppe zyklisch ist und gib gegebenenfalls einen Erzeuger an.

(i) $\mathbb{Z}_7^\times$.

(ii) $\mathbb{Z}_8^\times$.

(iii) $\mathbb{Z}_9^\times$.

(iv) $\mathbb{Z}_{10}^\times$.

(v) $\mathbb{Z}_{11}^\times$.

**Aufgabe 6.4** (Permutationen). (5 Punkte)

Wir betrachten die Menge $A_5$ aller Permutationen auf fünf Elementen, die sich als ein Produkt einer geraden Anzahl von Vertauschungen angeben lassen.

**Fakt.**
- *Jede Permutation $\sigma$ lässt sich tatsächlich als ein Produkt von Vertauschungen schreiben, und zwar sogar auf beliebig viele Arten.*
- *Wenn eine Permutation $\sigma$ sich als Produkt einer geraden Anzahl von Vertauschungen schreiben lässt, dann lässt sie sich nicht als Produkt einer ungeraden Anzahl von Vertauschungen schreiben und umgekehrt.*

(i) Bestimme die Zykelschreibweise der Elemente $(12)(23)$, $(12)(23)(31)(41)$, $(12)(23)(31)(45)$ und $(12)(23)(34)(45)$. [Achtung: Die Verknüpfung von Zykeln steht für die Hintereinanderausführung von rechts nach links.]

(ii) Welche der Elemente $(123)$, $(1342)$, $(13425)$ sind in $A_5$ enthalten?

(iii) Ist $A_5$ eine Gruppe? Ist $A_5$ kommutativ?

(iv) Ist $H = \{(), (12)(34), (13)(24), (14)(23)\}$ eine Untergruppe von $A_5$? (Der Zykel $()$ steht für die identische Permutation.)

(v) Ist $H$ ein Normalteiler in $A_5$?

(vi) Ist $A_5$ ein Normalteiler in $S_5$?

# 6. Übungsblatt zu Mathematik für Informatiker II, SS 2004, Mündlicher Teil

JOACHIM VON ZUR GATHEN & MICHAEL NÜSKEN

**Mündliche Aufgabe 6.5** (Kubismus).

Wir wollen untersuchen, was Kubieren in den multiplikativen Gruppen $\mathbb{Z}_p^\times$ mit $p$ prim bewirkt.

(i) Zeichne für $p = 11, 13, 17$ je einen Graphen: Zeichne für jedes Element in $\mathbb{Z}_p^\times$ einen Punkt und von einem Element $x \in \mathbb{Z}_p^\times$ soll ein Pfeil zu dessen Kubus $x^3$ zeigen. Ordne die Punkte dazu übersichtlich an.

(ii) Markiere alle Punkte, an denen Pfeile enden. Zähle zu jedem Punkt, wieviele Pfeile dort ankommen.

Betrachte nun allgemein die Kubierungsabbildung

$$k\colon \begin{array}{ccc} \mathbb{Z}_p^\times & \longrightarrow & \mathbb{Z}_p^\times, \\ x & \longmapsto & x^3 \end{array}$$

für $p$ prim.

(iii) Zeige, dass $k$ ein Homomorphismus ist.

(iv) Bestimme die Größe $\#\ker k$ des Kerns von $k$ in Abhängigkeit von $p$. [*Tipp*: Unterscheide die Fälle, je nachdem ob $3$ ein Teiler von $p-1$ ist oder nicht.]

**Mündliche Aufgabe 6.6** (Verschiedene Moduln).

Betrachte folgenden beiden Versuch einer Definition:

Sei $f\colon \mathbb{Z}_7 \to \mathbb{Z}_3$ die Abbildung mit $f(a \bmod 7) = a \bmod 3$.

Sei $f\colon \mathbb{Z}_{21} \to \mathbb{Z}_3$ die Abbildung mit $f(a \bmod 21) = a \bmod 3$.

(i) Ist das in Ordnung, ist die Abbildung wohldefiniert?

(ii) Ist $f$ ein Homomorphismus?

(iii) Ist $f$ surjektiv?

(iv) Ist $f$ injektiv?

(v) Ist $f$ bijektiv?

**Mündliche Aufgabe 6.7** (Zyklisch?).

Untersuche jeweils, ob die angegebene Gruppe zyklisch ist und gib gegebenenfalls einen Erzeuger an.

(i) $\mathbb{Z}_2^\times$.

(ii) $\mathbb{Z}_3^\times$.

(iii) $\mathbb{Z}_4^\times$.

(iv) $\mathbb{Z}_5^\times$.

(v) $\mathbb{Z}_6^\times$.

**Mündliche Aufgabe 6.8** (Permutationen).

Wir betrachten die Menge $A_4$ aller Permutationen auf vier Elementen, die sich als ein Produkt einer geraden Anzahl von Vertauschungen angeben lassen.

(i) Bestimme die Zykelschreibweise der Elemente $(12)(23)$, $(12)(23)(31)(41)$, $(12)(23)(21)(43)$ und $(12)(23)(34)$.

(ii) Welche der Elemente $(123)$, $(1342)$ sind in $A_4$ enthalten?

(iii) Ist $A_4$ eine Gruppe? Ist $A_4$ kommutativ?

(iv) Ist $H = \{(), (12)(34), (13)(24), (14)(23)\}$ eine Untergruppe von $A_4$? (Der Zykel $()$ steht für die identische Permutation.)

(v) Ist $H$ ein Normalteiler in $A_4$?

(vi) Ist $A_4$ ein Normalteiler in $S_4$?