# ANZAHLEN ENDLICHER GRUPPEN I: EINFÜHRUNG INS THEMA

JAN MORITZ PETSCHICK

## 1. Die Fragestellung und ihre Formulierung

Dieses Seminar beschäftigt sich mit folgender Fragestellung:

Wieviele Gruppen der Ordnung $n \in \mathbb{N}$ gibt es?

Liest man dies wörtlich erhält man keine sinnvolle Antwort, denn natürlich kann man durch Umbennung der Elemente einer einzigen Gruppe beliebig viele neue Gruppen erhalten. Jede Menge derselben Kardinalität stellte eine Gruppe dar, und die folgerichtige Antwort auf die Frage wäre: „Die Klasse aller Gruppen der Ordnung $n$ ist unabhängig von $n$ eine echte Klasse (und damit keine Menge)."

Diese Antwort ist nicht jene, die wir suchen. Daher schränken wir uns weiter ein und fragen:

Wieviele Isomorphieklassen von Gruppen der Ordnung $n \in \mathbb{N}$ gibt es?

Die Antwort auf diese Frage kann man nun in einer Funktion darstellen. Als generelle Konvention nennen wir diese

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto \#\text{ Menge aller Isomorphieklassen von Gruppen der Ordnung } n. \end{aligned}$$

Andere solche *Zählfunktionen* werden wir ähnlich benennen und eventuell mit Subskripten ausstatten.

Zurück zu unserer Frage. Ein sinnvoller erster Versuch zu einer Antwort wäre es, die ersten Werte von $f$ zu berechnen. Für kleine Zahlen sind diese Werte schon lange bekannt, und mit Hilfe grundlegender Sätze und Methoden kann man sie selbst nachrechnen. Bis $n = 16$ sind die Werte in Tabelle 1 wiedergegeben.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f(n)$ | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 5 | 2 | 2 | 1 | 5 | 1 | 2 | 1 | 14 |

Tabelle 1. $f(n)$ für kleine Werte von $n$.

Wer mehr sehen möchte, kann sich diese (die erste!) Folge der *The On-Line Encyclopedia of Integer Sequences* ansehen. Noch mehr findet man in der Arbeit von Besche, Eick und O'Brien, wobei wir vor allen an den beiden folgenden Resultaten daraus interessiert sind:

$$f(2^{10}) = f(1024) = 49487365422$$
$$\sum_{n=1}^{2000} f(n) = 49910529484$$

Das heißt, dass $\frac{49487365422}{49910529484} \approx 99,15\%$ aller (Isomorphieklassen von) Gruppen der Ordnung $\leq 2000$ von Ordnung $2^{10}$ sind! Schaut man sich die obige Tabelle noch einmal an, stellt man ein ganz ähnliches Verhalten im kleinen fest. Es sind 14 von 42, also immerhin ein Drittel, der Gruppen von Ordnung $\leq 16$ genau von Ordnung 16.

Auf der anderen Seite kennen wir den Satz, dass alle Gruppen von Primzahlordnung zyklisch sind, das heißt, dass für alle Primzahlen $p$ gerade $f(p) = 1$ gilt. (Andersherum gilt das nicht: Obwohl 15 nicht prim ist, gilt $f(15) = 1$.) Damit drängt sich folgende Vermutung auf: Der Wert $f(n)$ is groß, wenn $n$ viele Teiler hat, und klein, wenn $n$ wenige Teiler hat. Konkreter wollen wir folgende Maße für die *arithmetische Größe* einer natürlichen Zahl definieren:

**Definition 1.1.** Sei $n \in \mathbb{N}$ eine positive ganze Zahl mit Primfaktorzerlegung

$$n = \prod_{i=1}^{\ell} p_i^{\alpha_i},$$

dass heißt $p_i$ ist prim und $\alpha_i \in \mathbb{N}$ für $i = 1, \ldots, \ell$, und $p_i = p_j$ impliziert $i = j$. Wir definieren

$$\mu(n) := \max_{i=1}^{\ell} \alpha_i$$
$$\lambda(n) := \sum_{i=1}^{\ell} \alpha.$$

Achtung! Die Funktion $\mu$ ist *nicht* die häufig in der Zahlentheorie verwendete *Möbius-Funktion*, die oft ebenfalls mit $\mu$ bezeichnet wird.

Außerdem erkennen wir, dass unmöglich scheint eine exakte Formel für $f(n)$ anzugeben. Was wir suchen ist also eine *Abschätzung* für den Wert von $f$ abhängig von $n$. Um auch dieses zu präzisieren definieren wir:

**Definition 1.2.** Seien $k, l : \mathbb{N} \to \mathbb{R}$ zwei Funktionen. Wir schreiben

$$k(n) \leq \mathcal{O}(l(n))$$

(und analog $\leq, =$) falls eine positive Zahl $M \in \mathbb{R}_+$ existiert, sodass ein $n_0 \in \mathbb{N}$ exisiert, ab welchem für alle $n > n_0 \in N$ die folgende Abschätzung gilt:

$$k(n) \leq Ml(n).$$

Diese Konvention nennt man *Landau-$\mathcal{O}$-Notation*.

**Beispiel 1.3.**

(1) Einige Klassen von Funktionen lassen sich durch das Landau-$\mathcal{O}$ einfach beschreiben. Zum Beispiel sind die beschränkten Funktionen gerade die

Funktionen $k$, für welche $k \leq \mathcal{O}(1)$ gilt. Dabei beschreibt 1 die konstante Funktion.

(2) Von großem Interesse ist es, wie sich Zählfunktionen in die Hierarchie von polynomiellen, also $\mathcal{O}(P)$ mit einem Polynom $P$, und exponentiellen, also $\mathcal{O}(\exp)$, einordnen.

## 2. Resultate

Im Verlaufe des Seminars werden wir die Beweise für die beiden folgenden Resultate über die approximative von $f$ untersuchen. Dabei gelten diese zunächst nur für Primzahlpotenzen, was aber im Angesicht der im vorherigen Abschnitt erklärten Vermutung ein plausibler Startpunkt ist.

**Satz 2.1.** *Sei $p$ eine Primzahl. Dann gilt für natürliche Zahlen $m \in \mathbb{N}$*

$$f(p^m) \geq p^{\frac{2}{27}m^3 - \mathcal{O}(m^2)}.$$

**Satz 2.2.** *Sei $p$ eine Primzahl. Dann gilt für natürliche Zahlen $m \in \mathbb{N}$*

$$f(p^m) \leq p^{\frac{2}{27}m^3 + \mathcal{O}(m^{\frac{8}{3}})}.$$

Tatsächlich liegen wir damit schon in einem engen Wachstumsfenster. Beachtet man, dass $\mu(p^m) = m = \lambda(p^m)$ gilt, stellt sich die Frage danach, welches arithmetische Größenmaß die Potenz verallgemeinert.

In der zweiten Hälfte des Seminars beschäftigen wir uns mit einem Spezialfall des Satzes von Pyber, dessen allgemeine Form eine sehr präzise Antwort auf unsere zentrale Frage liefert:

**Satz 2.3.** *Es gilt:*

$$f(n) \leq n^{\frac{2}{27}\mu(n)^3 + \mathcal{O}(\mu(n)^{\frac{5}{3}})}.$$

## 3. Elementare Abschätzungen

**Definition 3.1** (Hierachie von gruppenähnlichen algebraischen Strukturen)**.**

(1) Eine nicht-leere Menge $M$ mit einer Operation

$$\cdot : M \times M \to M$$

heißt *Magma*.

(2) Ein Magma $M$ mit einem Element $1_M$ mit der Eigenschaft

$$1_M \cdot m = m = m \cdot 1_M$$

für alle $m \in M$ heißt *unitäres Magma*. Das Element $1_M$ heißt neutrales Element.

(3) Ein Magma, in dem das Assoziativgesetz gilt, heißt *Halbgruppe*.

(4) Ein Magma $M$ mit der Eigenschaft, daß für alle $m, n \in M$ Elemente $x, y \in M$ existieren, sodaß

$$m \cdot x = n \text{ und } y \cdot m = n$$

gelten, heißt *Quasigruppe*.

Jedes endliche Magma wird vollständig durch seine Multiplikationstafel (auch *Cayley-Tafel* genannt) beschrieben, also durch die Matrix $(m \cdot n)_{m,n \in M} \in M^{|M|^2}$. Dadurch läßt sich die Anzahl der möglichen Magmas einer bestimmten Größe einfach abschätzen. Es gilt:

$$f_{\text{Magma}}(n) \leq n^{n^2}.$$

Da Magmas keine algebraischen Eigenschaften (wie Assoziativität, Kommutativität, &c.) erfüllen müssen, definieren wir den *Isomorphimsus von Magmas* als Bijektion der unterliegenden Mengen. Natürlich soll $f_{\text{Magma}}$ die Zahl der Magmas bis auf Isomorphie beschreiben. Also wissen wir, daß eine untere Schranke für $f_{\text{Magma}}$ durch

$$\frac{n^{n^2}}{n!}$$

gegeben wird.

Wie zu erwarten bringt uns diese Abschätzung noch kaum einen Schritt an die Resultate für Gruppen heran. Auch der Übergang zu unitären Magmas ist nicht bedeutsam, da bei diesen lediglich eine Spalte und Zeile in der Cayley-Tafel festgelegt ist (die des neutralen Elementes), d.h.

$$\frac{n^{n-1^2}}{(n-1)!} \leq f_{\text{uni.Magma}}(n) \leq n^{n-1^2}.$$

Größere Hoffnung einer Annäherung an die Ergebnisse für Gruppen liegt im Übergang zu Halb- oder Quasigruppen.

**Satz 3.2.** *Sei $\epsilon > 0$. Dann existiert ein $n_0 \in \mathbb{N}$, sodaß für alle $n > n_0$ folgendes gilt:*

$$f_{\text{Halbgruppen}}(n) \geq n^{(1-\epsilon)n^2}.$$

*Beweis.* Die Idee ist es, strukturell sehr einfach zu beschreibenden Halbgruppen zu konstruieren. Sei $M \neq \emptyset$ eine durch $<$ linear geordnete Menge, d.h. bis auf Umbenennung $\{0, \ldots, |M|-1\}$ mit der natürlichen Ordnung. Wähle $m \in M$ beliebig und definiere

$$i \cdot j = \begin{cases} 0, & \text{falls } i < m \text{ oder } j < m \\ \text{beliebig in } \{n \in M \mid n < m\} & \text{andernfalls.} \end{cases}$$

Unabhängig von der konkreten Wahl im zweiten Fall erhalten wir eine Halbgruppe: Es gilt für alle $i, j, k \in M$

$$\underbrace{(i \cdot j)}_{<m} \cdot k = 0 = i \cdot \underbrace{(j \cdot k)}_{<m}.$$

Es gilt also für jedes $m \in M$

$$f_{\text{Halbgruppen}}(n) \geq \frac{m^{(n-m)^2}}{n!}.$$

Wählt man $m := n^{(1-\frac{1}{2}\epsilon)}$ ergibt sich

$$f_{\text{Halbgruppen}}(n) \geq n^{(1-\frac{1}{2}\epsilon)(n-n^{1-\frac{1}{2}\epsilon})}.$$

Für große $n \in N$ gilt damit $f_{\text{Halbgruppen}}(n) \geq n^{(1-\epsilon)n^2}$. □

Trotz Assoziativität bleiben wir also sehr dicht an $n^{n^2}$. Die nächste Hoffnung sind die Quasi-Gruppen. Um diese besser zu verstehen betrachten wir folgendes Lemma:

**Lemma 3.3.** *Ein Magma $M$ ist genau dann eine Quasigruppe, wenn seine Multiplikationstafel ein* lateinisches Quadrat *ist, d.h. wenn in jeder Zalte und Speile jedes Element von $M$ genau einmal vorkommt.*

*Beweis.* Angenommen $M$ ist eine Quasigruppe. In der Spalte von $m \in M$ taucht $n \in M$ auf, denn es existiert $x \in M$ mit $m \cdot x = n$. Analoges gilt für die Zeilen der Tafel, mit der Existenz von $y \in M$, sodaß $y \cdot m = n$. Die Rückrichtung ist klar. □

Leider ist die Zahl der Lateinischen Quadrate einer fixen Größe ein Mysterium; es ist keine Asymptotik bekannt. Aber ein Satz von M. Hall besagt:

$$n^{\frac{1}{2}n^2-\mathcal{O}(n)} \leq f_{\text{Lateinische Quadrate}}(n) \leq n^{n^2}.$$

Also reicht auch die Invertierbarkeit nicht für eine signifikante Reduktion der Anzahl der Objekte aus. Man muß also tatsächlich alle drei Eigenschaften der Gruppe – Assoziativität, Invertierbarkeit und Unitarität – gleichzeitig betrachten.

**Satz 3.4** (Elementare obere Schranke)**.** *Es gilt*

$$f(n) \leq n^{n\lambda(n)}.$$

*Beweis.* Definiere den Rang von $G$ durch

$$\mathrm{d}(G) := \min\{|X| \mid X \subseteq G, \langle X\rangle = G\},$$

also als die minimale Größe eines Erzeugendensystems von $G$. Dann gilt

$$\lambda(|G|) \geq \mathrm{d}(G).$$

Dies wird wie folgt bewiesen: Sei

$$G = G_r > G_{r-1} > \cdots > G_1 > G_0 = \{1\}$$

eine maximale Kette ineinander enthaltener Untergruppen von $G$. Wähle für jedes $i \in \{1,\dots,r\}$ ein Element $g_i \in G_i \setminus G_{i-1}$. Dann gilt $\langle g_i \mid i \in \{1,\dots,j\}\rangle = G_j$, denn wäre $\langle g_i \mid i \in \{1,\dots,j\}\rangle < G_j$ könnte man die Kette verfeinern. Damit ist $r > \mathrm{d}(G)$. Nach dem Satz von Lagrange gilt

$$|G| = \prod_{i=1}^{r} |G_i : G_{i-1}|.$$

Damit ist nun $r \leq \lambda(|G|)$, denn $\lambda(|G|)$ ist die maximale Länge eines Produktes von Zahlen aus $\mathbb{N}_{>1}$, welches $|G|$ ergibt. Dies beweist die Behauptung $\lambda(|G|) \geq \mathrm{d}(G)$.

Nach dem Satz von Cayley gilt bis auf Isomorphie $G \leq \mathsf{Sym}(|G|)$. Also

$$\begin{aligned} f(n) &\leq \#\text{Untergruppen der Ordnung } n \text{ von } \mathsf{Sym}(n) \\ &\leq \#\lambda(n)\text{-erzeugte Untergruppen der Ordnung } n \text{ von } \mathsf{Sym}(n), \end{aligned}$$

nach obiger Behauptung, und konsequenterweise

$$\begin{aligned} f(n) &\leq \#\lambda(n)\text{-elementige Teilmengen von } \mathsf{Sym}(n) \\ &= (n!)^{\lambda(n)} \\ &\leq n^{n\lambda(n)}. \end{aligned}$$

□