Mathematische Semesterberichte

Zur Pflege des Zusammenhangs von Schule und Universität

Begründet 1932 von H. Behnke und O. Toeplitz

Herausgegeben von:
K. P. Grotemeyer in Bielefeld / D. Kahle in Göttingen / Th. Kaluza in Hannover / A. Kirsch in Kassel / N. Knoche in Essen / D. Morgenstern in Hannover / G. Pickert in Gießen / H.-G. Steiner in Bielefeld / H. Tietz in Hannover

BAND XXXIV

V&R

GÖTTINGEN · VANDENHOECK & RUPRECHT · 1987

ISSN 0720–728X

Gesamtherstellung: Hubert & Co., Göttingen

Eine Bemerkung über endliche abelsche Gruppen

Von DIETER JUNGNICKEL in Gießen

Das folgende Lemma ist eine der bekanntesten Aussagen der elementaren Gruppentheorie; man findet es - zumindest als Übungsaufgabe - in nahezu jedem Lehrbuch.

Lemma. G *sei eine endliche abelsche Gruppe, und* a *bzw.* b *seien Elemente der Ordnung* m *bzw.* n. *Wenn* m *und* n *teilerfremd sind, hat* ab *die Ordnung* mn.

Mit diesem Lemma zeigt man z. B. leicht, daß der Exponent von G (also die kleinste natürliche Zahl e mit $x^e=1$ für alle $x \in G$) die maximale Ordnung eines Elements von G ist; insbesondere ist G genau dann zyklisch, wenn $|G| = \exp G$ gilt. Daraus folgt wiederum leicht, daß jede endliche Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist. Man vergleiche hierzu etwa Jacobson [1], Theorem 1.4 und Theorem 2.18, sowie van der Waerden [2], §§ 42 und 43.

Es liegt nun nahe, sich zu fragen, was über die Ordnung von ab ausgesagt werden kann, wenn man auf die Voraussetzung der Teilerfremdheit von m und n verzichtet. Erstaunlicherweise schweigen die Lehrbücher zu dieser Frage, abgesehen von der trivialen Beobachtung, daß $(ab)^{kgV(m,n)} = 1$ gilt. Ich will im folgenden zeigen, wie man mit ganz elementaren Überlegungen einige meines Erachtens durchaus interessante Ergebnisse erzielen kann, die das genannte Problem zwar nicht im Sinne der ursprünglichen Fragestellung lösen, aber doch einiges zu seiner Klärung beitragen.

Zunächst wollen wir uns davon überzeugen, daß man keine allgemeine Formel für die Ordnung o(ab) erwarten kann; insbesondere ist es keineswegs so, daß immer o(ab)=kgV(m,n)

gilt. Wie das folgende Beispiel zeigen wird, kann man selbst bei fester Wahl der Gruppe G für festes m und n verschiedene Resultate erhalten:

Beispiel 1. Wir betrachten die Gruppe $\mathbb{Z}_{30}$ der Restklassen modulo 30 (natürlich additiv geschrieben). Dann hat 2*) die Ordnung 15, und 5 und 25 haben jeweils die Ordnung 6; es gilt aber $o(2+5) = 30 \neq 10 = o(2+25)$.

Damit wird es schon verständlicher, warum unser Problem anscheinend noch nicht untersucht worden ist. Man sollte aber an dieser Stelle noch nicht aufgeben, sondern nach vernünftigen Schranken für o(ab) fragen. Die Antwort darauf gibt der folgende Satz 1.

Satz 1. a *und* b *seien zwei Elemente einer endlichen abelschen Gruppe* G. *Man setze* $m=o(a)$, $n=o(b)$ *und* $d=ggT(m,n)$. *Dann gilt die folgende Teilerkette:*

(*) $\quad mn/d^2 \mid o(ab) \mid mn/d = kgV(m,n)$.

Beweis. Wie schon erwähnt, gilt trivialerweise $ab^{kgV(m,n)} = 1$, weswegen o(ab) ein Teiler von mn/d ist. Wir setzen nun $o(ab)=k$ und wollen zeigen, daß mn/d^2 ein Teiler von k ist. Aus $(ab)^k=1$ folgt

$$c := a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle;$$

damit muß o(c) sowohl ein Teiler von o(a) als auch von o(b) sein, also ein Teiler von d. Da $\langle a^{m/d} \rangle$ die eindeutig bestimmte Untergruppe der Ordnung d von $\langle a \rangle$ ist, hat c die Form $c = a^{xm/d}$ für ein geeignetes x; analog gilt auch $c = b^{yn/d}$ für ein geeignetes y. Somit erhalten wir die Kongruenzen

$$k \equiv xm/d \bmod m \quad \text{und} \quad k \equiv yn/d \bmod n,$$

weswegen m/d und n/d Teiler von k sind. Da d=ggT(m,n) ist, gilt ggT(m/d,n/d)=1; also folgt - wie behauptet - $mn/d^2 \mid k$. □

---

*) Wir schreiben (inkorrekterweise) für die Restklasse einer ganzen Zahl z (bei gegebenem Modul k) wieder z.

Sind die in Satz 1 angegebenen Schranken bestmöglich? Das gilt jedenfalls für m=15 und n=6, wie unser Beispiel 1 zeigt. Natürlich fragt man dann nach Serien von Beispielen, für die eine der beiden Schranken in Satz 1 angenommen wird; besser noch, man möchte die Paare (m,n) bestimmen, für die die jeweilige Schranke angenommen werden kann. Das ist für die obere Schranke leicht:

Satz 2. *Für gegebene natürliche Zahlen* m *und* n *existiert stets eine abelsche Gruppe* G *mit zwei Elementen* a *und* b *der Ordnungen* m *bzw.* n, *so daß* o(ab) = kgV(m,n) *ist.*

Beweis. Es sei G das direkte Produkt $\langle a \rangle \times \langle b \rangle$ zweier zyklischer Gruppen; dabei gelte o(a)=m und o(b)=n. Dann hat ab = (a,b) offenbar die Ordnung kgV(m,n). □

Dagegen bereitet die untere Schranke in Satz 1 wesentlich größere Schwierigkeiten. Wir geben zunächst eine Klasse von Beispielen an, die vielleicht ein Gefühl dafür vermittelt, wodurch die Ordnung von ab kleiner werden kann als kgV(m,n).

Beispiel 2. G sei die zyklische Gruppe $\mathbb{Z}_{2pq}$, wobei p und q verschiedene ungerade Primzahlen seien. Wir setzen a=p, b=q; dann gilt o(a)=m=2q, o(b)=n=2p und kgV(m,n)=2pq. Da a+b gerade ist, hat a+b höchstens die Ordnung $pq=mn/d^2$ (also genau diese Ordnung).

Nach der Untersuchung einiger weiterer Beispiele gelangt man bald zu der Einsicht, daß $o(ab)=mn/d^2$ wohl genau dann möglich ist, wenn ggT(m/d,d) = ggT(n/d,d) = 1 gilt. Damit bleibt uns nur noch die Aufgabe, dieses Resultat zu beweisen, was im folgenden Satz 3 geschehen soll.

Satz 3. m *und* n *seien natürliche Zahlen*, d=ggT(m,n), m'=m/d *und* n'=n/d. *Genau dann gibt es eine abelsche Gruppe* G *mit Elementen* a *und* b *der Ordnungen* m *bzw.*

n, *für die* $o(ab)=mn/d^2=m'n'$ *gilt, wenn* $ggT(m',d)=ggT(n',d)=1$ *ist.*

Beweis. Zunächst seien a und b Elemente einer abelschen Gruppe G mit $o(a)=m$, $o(b)=n$ und $o(ab)=m'n'$. Wir betrachten das im Beweis von Satz 1 eingeführte Element $c=a^k=b^{-k}$, dessen Ordnung d teilt, etwas näher und behaupten, daß wegen $k=m'n'$ hier $o(c)=d$ gilt. Dazu sei $o(c)=d'$ und $d=d'd''$. Wie im Beweis von Satz 1 (mit d' statt d) zeigt man, daß $m/d'=m'd''$ und $n/d'=n'd''$ Teiler von $k=m'n'$ sind; damit muß d" ein Teiler von $ggT(m',n')=1$ sein. Also gilt $d''=1$ und somit, wie behauptet, $o(c)=d$. Daher ist c ein erzeugendes Element der Gruppe $\langle a^{m'}\rangle$ und hat also die Form $c=a^{xm'}$ für ein x mit $ggT(x,d)=1$. Da auch $c=a^k$ ist, folgt $xm' \equiv m'n' \mod m'd$, also $n' \equiv x \mod d$. Aus $ggT(x,d)=1$ ergibt sich unmittelbar die Behauptung $ggT(n',d)=1$. Analog zeigt man auch $ggT(m',d)=1$, indem man $\langle b^{n'}\rangle$ betrachtet.

Umgekehrt sei jetzt die Bedingung $ggT(m',d)=ggT(n',d)=1$ erfüllt. Wir wählen für G die zyklische Gruppe $\mathbb{Z}_{m'n'd}$. Die Elemente n' bzw. m' haben dann die Ordnungen m bzw. n. Wir wollen für a und b geeignete Vielfache dieser Elemente wählen, also $a=xn'$ und $b=ym'$. Damit $o(a)=m$ und $o(b)=n$ gilt, müssen wir dabei $ggT(x,m)=ggT(y,n)=1$ verlangen. Nach Voraussetzung ist n' zu m' und zu d, also auch zu $m=m'd$, teilerfremd; mit anderen Worten, n' ist ein primer Rest modulo n. Da die primen Reste modulo m bezüglich der Multiplikation eine Gruppe bilden, durchläuft mit x auch xn' alle primen Reste. Insbesondere können wir x so wählen, daß $a=xn' \equiv 1 \mod m$ gilt. Analog kann y so gewählt werden, daß $b=ym' \equiv -1 \mod n$ gilt. Da d sowohl m wie n teilt, gelten beide Kongruenzen erst recht modulo d; wir erhalten also $a+b = xn'+ym' \equiv 1-1 \equiv 0 \mod d$. Daher ist $m'n'(a+b)$ durch $m'n'd$ teilbar, woraus sofort $o(a+b) = m'n'$ folgt. □

Meiner Meinung nach haben diese Ergebnisse einen gewissen intuitiven Reiz und eignen sich dank ihrer elementaren

Beweise gut für eine einführende Algebra- (oder Zahlentheorie-)Vorlesung, eventuell auch als (mit Hinweisen versehene) etwas anspruchsvollere Übung.

Literatur

[1] JACOBSON, N.L.: Basic Algebra I. Freeman, 2. Aufl. 1985.

[2] VAN DER WAERDEN, B.L.: Algebra I. Springer, 8. Aufl. 1971.

Eingegangen: 21.04.1986