Österreichische Mathematische Gesellschaft

MATHE-BRIEF

November 2021 — Nr. 111

Herausgegeben von der Österreichischen Mathematischen Gesellschaft
http://www.oemg.ac.at/Mathe–Brief ——— mathe–brief@oemg.ac.at

50 Jahre Teilraumsatz

Nächstes Jahr sind es genau 50 Jahre, dass der herausragende österreichische Zahlentheoretiker Wolfgang M. Schmidt ein Ergebnis auf dem Gebiet der Diophantischen Approximation publiziert hat, das heute als *Teilraumsatz*, im englischen Sprachraum als *Subspace Theorem* bekannt ist. Der Satz gilt heute als eines der bedeutendsten Resultate des 20. Jahrhunderts in der Zahlentheorie. Seit seiner Publikation sind unzählige Verallgemeinerungen und immer neue Anwendungsmöglichkeiten entdeckt worden, was den Teilraumsatz zu einem wesentlichen Katalysator der Forschung auf diesem Gebiet werden ließ.

Der Teilraumsatz in seiner ursprünglichen Version ist relativ einfach zu formulieren, doch um seine Bedeutung auch nur annäherungsweise erahnen zu können, muss man zunächst ein wenig in die Geschichte der Diophantischen Approximation eindringen. Dieses Teilgebiet der Zahlentheorie geht zurück auf das 19. Jahrhundert, genauer auf zwei Resultate zur Approximierbarkeit von irrationalen Zahlen durch rationale Zahlen, also Brüche. Dabei wird die Güte einer Approximation der irrationalen Zahl α durch den Bruch y/x quantifiziert mittels einer Abschätzung der Differenz $|\alpha - y/x|$ durch eine Funktion des Nenners x des approximierenden Bruchs. Das erste von beiden, der *Dirichletsche Approximationssatz*, besagt, dass zu jeder irrationalen Zahl α unendlich viele Brüche y/x existieren mit

$$\left|\alpha - \frac{y}{x}\right| < \frac{1}{x^2}. \tag{1}$$

Betrachtet man unter allen irrationalen Zahlen α lediglich diejenigen, die Nullstellen von Polynomen mit ganzen Koeffizienten sind (also die sogenannten *algebraischen Zahlen*), so hat Joseph Liouville umgekehrt gezeigt, dass man x^2 im Nenner der rechten Seite von (1) nicht durch eine beliebig grosse Potenz von x ersetzen kann, wenn man weiterhin unendlich viele Lösungen erhalten will. Genauer, ist α algebraisch vom Grad d, d.h. der kleinstmögliche Grad eines Polynoms P mit $P(\alpha) = 0$ ist d, so existiert eine Konstante $c(\alpha)$, sodass für alle Brüche y/x gilt:

$$\left|\alpha - \frac{y}{x}\right| > \frac{c(\alpha)}{x^d}. \tag{2}$$

Während Dirichlets Resultat in seiner Allgemeinheit bestmöglich ist, hat Liouvilles Ergebnis zahlreiche Verbesserungen hinsichtlich des Exponenten im Nenner der Abschätzung erfahren, bis schließlich K. F. Roth 1955 am Ende einer langen Reihe von Verbesserungen zeigen konnte, dass der Exponent d in Gleichung (2) durch jeden Wert grösser als 2 ersetzt werden kann. Der *Satz von Thue-Siegel-Roth* lautet im Detail:

Satz 1. *Sei $\delta > 0$ und $\alpha \in \mathbb{C}$ eine irrationale algebraische Zahl. Dann existieren nur endlich viele Paare $(y, x) \in \mathbb{Z} \times \mathbb{N}$ mit*

$$\left|\alpha - \frac{y}{x}\right| < \frac{1}{x^{2+\delta}}. \tag{3}$$

Daraus ergibt sich unmittelbar die Existenz einer Konstanten $c(\alpha, \delta)$, für die

$$\left|\alpha - \frac{y}{x}\right| > \frac{c(\alpha, \delta)}{x^{2+\delta}}, \tag{4}$$

wenn man $c(\alpha, \delta)$ nur klein genug wählt, um die endlich vielen Ausnahmepaare in Satz 1 auszuschließen. Der Satz von Thue-Siegel-Roth liefert also eine Verschärfung des Ergebnis von Liouville, die sogar bestmöglich ist, wenn man bedenkt, dass im Fall $d = 2$ von quadratischen Irrationalzahlen der Satz von Dirichlet belegt, dass δ nicht als 0 gewählt werden kann.

Bestmögliche Ergebnisse sind aber in der Mathematik keineswegs ultimativ: die Suche nach Verallgemeinerungen enthüllt oft noch tieferliegende Zusammenhänge. Im Falle der hier vorgestellten Resultate geht es um die Verallgemeinerung auf die *gleichzeitige* Approximation mehrerer irrationaler Zahlen durch ebensoviele Brüche mit demselben Nenner. Die mehrdimensionale Version des Satzes von Dirichlet lautet etwa:

Satz 2. *Seien $\alpha_1, \ldots, \alpha_m$ reelle Zahlen, unter denen mindestens eine irrational ist. Dann existieren unendlich viele rationale*

$$\frac{y_1}{x}, \ \ldots, \ \frac{y_m}{x}$$

mit einem ganzzahligen Nenner $x > 0$ und

$$\left|\alpha_i - \frac{y_i}{x}\right| < \frac{1}{x^{1+1/m}} \tag{5}$$

für $i = 1, \ldots, m$.

Um noch einen Schritt weiterzugehen, betrachten wir nun eine andere Variante von Satz 2. Diese parametrische Version des Satzes ist durch die Anwendung der Geometrie der Zahlen motiviert und lautet:

Satz 3. *Seien $\alpha_1, \ldots, \alpha_m$ reelle Zahlen und $Q > 1$. Dann existieren ganzzahlige (sogar teilerfremde) $x, y_1, \ldots, y_m$ mit*

$$1 \leq x \leq Q^m \quad \text{und} \quad |\alpha_i x - y_i| \leq \frac{1}{Q} \quad (1 \leq i \leq m). \tag{6}$$

Man beachte, dass aus den Ungleichungen in (6) die Ungleichungen in (5) folgen, wenn man durch x dividiert und benützt, dass $1/Q \leq 1/x^{1/m}$ ist. Setzt man zusätzlich voraus, dass zumindest ein α_i, etwa α_1, irrational ist, so ist $|\alpha_1 x - y_1| \neq 0$ und somit kann (6) bei festem $x, y_1, \ldots, y_m$ nur für Q unter einer festen Schranke erfüllt sein. Mit $Q \to \infty$ folgt somit die Existenz unendlich vieler Brüche mit (5).

Analysiert man Satz 3 genauer, so erkennt man, dass er die Existenz einer nichttrivialen ganzzahligen Lösung eines speziellen Systems von Ungleichen garantiert. H. Minkowski hat erkannt, dass dabei nicht die genaue Gestalt der Ungleichungen von Bedeutung ist, sondern lediglich die Tatsache, dass es sich bei deren jeweils linken Seiten um Linearformen handelt und das Produkt der Werte, durch die sie abgeschätzt werden, mit der Determinante der zugehörigen Koeffizientenmatrix korreliert. Dies ist der Inhalt des *Linearformensatzes* von Minkowski:

Satz 4. *Seien $L_i = c_{i1}x_1 + \cdots + c_{in}x_n$, $i = 1, \ldots, n$, linear unabhängige Linearformen mit reellen Koeffizienten und $\Delta := \det(c_{ij})_{1\le i,j\le n} = \det(L_1, \ldots, L_n)$ deren Determinante. Sind $C_1, \ldots, C_n$ positive reelle Zahlen mit $C_1 \cdots C_n = |\Delta|$, so existiert ein $\mathbf{x} := (x_1, \ldots, x_n) \neq \mathbf{0}$ aus $\mathbb{Z}^n$ mit*

$$\begin{aligned} |L_i(\mathbf{x})| &< C_i \ (i = 1, \ldots, n-1) \\ |L_n(\mathbf{x})| &\le C_n. \end{aligned}$$

Setzt man $n = m + 1$ sowie $x_1 = x, x_2 = y_1, \ldots, x_n = y_m$ und wählt man im Linearformensatz $L_i(\mathbf{x}) = \alpha_i x - y_i$ für $i = 1, \ldots, m$, $L_n(\mathbf{x}) = x$, so ist die Voraussetzung der linearen Unabhängigkeit der L_i erfüllt, die Determinante $\Delta = 1$. Mit $C_i = 1/Q$ für $i = 1, \ldots, m$ und $C_n = Q^m$ folgt Satz 3 unmittelbar. Satz 4 ist also tatsächlich eine Verallgemeinerung von Satz 3.

Betrachtet man das Produkt der Ungleichungen aus Satz 4, so ergibt sich als Folgerung die Existenz einer nichttrivialen, ganzen Lösung $\mathbf{x}$ von

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < |\Delta|. \tag{7}$$

Dieses Resultat ist jedoch weit schwächer als Satz 4, da es keine Aussage über die Abschätzung der einzelnen Linearformen macht.

Wollte man hingegen das Ergebnis von Roth auf die simultane Approximierbarkeit von m algebraischen Zahlen $\alpha_1, \ldots, \alpha_m$ verallgemeinern, so wäre das Ziel, nachzuweisen, dass das System von Ungleichungen

$$\left|\alpha_i - \frac{y_i}{x}\right| < \frac{1}{x^{1+1/m+\delta}}, \quad 1 \le i \le m, \tag{8}$$

für gegebenes $\delta > 0$ höchstens endlich viele Lösungen $(x, y_1, \ldots, y_m) \in \mathbb{N} \times \mathbb{Z}^m$ besitzt. Sollte auch in diesem Fall eine weitere Verallgemeinerung auf Linearformen möglich sein, so wäre die Situation genau entgegengesetzt zu der im vorigen Abschnitt beschriebenen: kann man zeigen, dass es nur endlich viele Ausnahmen für eine Abschätzung des Produkts von Linearformen gibt wie in (7), so folgt daraus, dass es auch nur endlich viele Ausnahmen für jede damit kompatible individuelle Abschätzungen der einzelnen Linearformen geben kann. An die Stelle von (8) sollte also eine Ungleichung treten, die das Produkt von Linearformen $\alpha_i x - y_i$ beschränkt.

Eine solche ultimative Verallgemeinerung hat W. M. Schmidt 1972 mit seinem *Teilraumsatz* gefunden, vgl. [2, 3]. Schreibt man $\|\mathbf{x}\| := \max\{|x_1|, \ldots, |x_n|\}$, so lautet sein Ergebnis:

Satz 5. *Seien $n \ge 2$, $\delta > 0$ und $L_i(\mathbf{x}) = c_{i1}x_1 + \ldots + c_{in}x_n$, $i = 1, \ldots, n$, linear unabhängige Linearformen mit algebraischen Koeffizienten aus $\mathbb{C}$. Dann liegen die Lösungen $\mathbf{x} \in \mathbb{Z}^n$ von*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < \|\mathbf{x}\|^{-\delta} \tag{9}$$

in der Vereinigung von endlich vielen echten linearen Teilräumen von $\mathbb{Q}^n$.

Zunächst ist dazu zu bemerken, dass lineare Teilräume von $\mathbb{Q}^n$ der Dimension r, $0 \le r \le n$, aus den $\mathbb{Q}$-Linearkombinationen von r festen, linear unabhängigen Vektoren aus $\mathbb{Q}^n$ bestehen und für echte Teilräume auch $r < n$ gelten muss (d.h. ihre Dimension ist kleiner als n). Anders als im Fall des Linearformensatzes von Minkowski, von dem wir gerade gezeigt haben, dass er den mehrdimensionalen Approximationssatz von Dirichlet beinhaltet, ist hier nicht so leicht zu erkennen, dass es sich beim Teilraumsatz um eine Verallgemeinerung von Satz 1 bzw. die in (8) angedeutete mehrdimensionale Variante handelt. Daher wollen wir uns dies, zumindest für Satz 1, also $n = 2$ in Satz 5, noch im Detail überlegen.

Dazu muss gezeigt werden, dass für gegebenes $\delta > 0$ und algebraisches α die Ungleichung (3) höchstens endlich viele Lösungen $(y, x) \in \mathbb{Z} \times \mathbb{N}$ besitzt. Angenommen (y, x) sei eine solche Lösung. Dann folgt durch Multiplikation mit x^2:

$$|x|\,|\alpha x - y| \leq x^{-\delta}. \tag{10}$$

Wählt man $L_1(x, y) = x$ und $L_2(x, y) = \alpha x - y$, so sind L_1, L_2 linear unabhängige Linearformen mit algebraischen Koeffizienten wie in den Voraussetzungen des Teilraumsatzes verlangt. Aus (3) folgt zudem $|y/x| \leq |\alpha| + 1/x^2$, sodass $|y| \leq Cx$ mit $C := (|\alpha| + 1)$ und aus (10) die Ungleichung

$$|x|\,|\alpha x - y| \leq C^{\delta}\|x\|^{-\delta}$$

folgt. Aus dem Teilraumsatz folgt nun, dass solche (y, x) in der Vereinigung endlich vieler echter, also eindimensionaler Teilräume $T_1, \ldots, T_t$ von $\mathbb{Q}^2$ liegen und wir behaupten, dass jeder dieser endlich vielen Teilräume T nur endlich viele Lösungen von (3) enthalten kann. Wird nämlich T von einem ganzzahligen Vektor $(a, b) \in \mathbb{Z}^2$ aufgespannt und und gilt $(y, x) \in T \cap \mathbb{Z}^2$, so folgt $(y, x) = \lambda(a, b)$ für ein $\lambda \in \mathbb{Q}$. Wir dürfen sogar $\text{ggT}(a, b) = 1$ annehmen, was am Teilraum T nichts ändert, aber $\lambda \in \mathbb{Z}$ erzwingt. Es gilt dann

$$0 < \left|\alpha - \frac{a}{b}\right| = \left|\alpha - \frac{y}{x}\right| < \frac{1}{x^{2+\delta}} \leq \frac{1}{x^2} = \frac{1}{\lambda^2 b^2},$$

sodass $|\lambda|$ abhängig von (a, b), also von T, beschränkt sein muss. Damit liegen in jedem der Teilräume $T_1, \ldots, T_t$ nur endlich viele Lösungen von (3), und der Satz von Thue-Siegel-Roth ist aus dem Teilraumsatz im Fall $n = 2$ gefolgert.

Abschließend sei noch angemerkt, dass die Aussage des Teilraumsatzes bestmöglich in zweierlei Hinsicht ist: einerseits, was den Exponenten im Nenner der Abschätzung betrifft (was schon daraus folgt, dass dieser im Satz von Roth bestmöglich ist), andererseits hinsichtlich der Menge der Lösungen. Man kann nämlich zeigen, dass es echte Teilräume geben kann, in denen unendlich viele Lösungen von (9) liegen, selbst wenn man Nullstellen der einzelnen Linearformen ausschließt – siehe dazu [1].

Leonhard Summerer

LITERATUR

[1] Jan-Hendrik Evertse, *The subspace Theorem*. *http://www.math.leidenuniv.nl/~evertse/dio2011-subspace.pdf*, aufgerufen im Oktober 2021.
[2] Wolfgang M. Schmidt, Norm Form equations. *Annals of Mathematics* 96 (1972), 526–551.
[3] Wolfgang M. Schmidt, Diophantine Approximation (Lecture Notes in Mathematics Bd. 785), Springer Verlag 1980