Internationale Mathematische Nachrichten

International Mathematical News

Nouvelles Mathématiques Internationales

Die IMN wurden 1947 von R. Inzinger als „Nachrichten der Mathematischen Gesellschaft in Wien“ gegründet. 1952 wurde die Zeitschrift in „Internationale Mathematische Nachrichten“ umbenannt und war bis 1971 offizielles Publikationsorgan der „Internationalen Mathematischen Union“.

Von 1953 bis 1977 betreute W. Wunderlich, der bereits seit der Gründung als Redakteur mitwirkte, als Herausgeber die IMN. Die weiteren Herausgeber waren H. Vogler (1978–79), U. Dieter (1980–81, 1984–85), L. Reich (1982–83), P. Flor (1986–99) und M. Drmota (2000–2007).

Herausgeber:

Österreichische Mathematische Gesellschaft, Wiedner Hauptstraße 8–10/104, A-1040 Wien. email *imn@tuwien.ac.at*, *http://www.oemg.ac.at/*

Bezug:

Die IMN erscheinen dreimal jährlich und werden von den Mitgliedern der Österreichischen Mathematischen Gesellschaft bezogen.
Jahresbeitrag: € 20,–

Bankverbindung: Konto Nr. 229-103-892-00 der Bank Austria–Creditanstalt (IBAN AT83-1200-0229-1038-9200, BLZ 12000, BIC/SWIFT-Code BKAUATWW).

Eigentümer, Herausgeber und Verleger: Österr. Math. Gesellschaft. Satz: Österr. Math. Gesellschaft. Druck: Grafisches Zentrum, Wiedner Hauptstraße 8–10, 1040 Wien.

ISSN 0020-7926

Österreichische Mathematische Gesellschaft

Gegründet 1903

http://www.oemg.ac.at/
email: *oemg@oemg.ac.at*

Sekretariat:

TU Wien, Institut 104,
Wiedner Hauptstr. 8–10, A 1040 Wien.
Tel. +43-1-58801-11823
email: *sekr@oemg.ac.at*

Vorstand des Vereinsjahres 2010:

M. Drmota (TU Wien): Vorsitzender
M. Oberguggenberger (Univ. Innsbruck): Stellvertretender Vorsitzender
J. Wallner (TU Graz):
Herausgeber der IMN
B. Lamel (Univ. Wien): Schriftführer
A. Ostermann (Univ. Unnsbruck):
Stellvertretender Schriftführer
G. Larcher (Univ Linz): Kassier
P. Kirschenhofer (MU Leoben):
Stellvertretender Kassier
G. Schranz-Kirlinger (TU Wien):
Beauftragte für Frauenförderung
G. Teschl (Univ. Wien):
Beauftragter f. Öffentlichkeitsarbeit

Beirat:

A. Binder (Linz)
C. Christian (Univ. Wien)
U. Dieter (TU Graz)
H. Engl (Öst. Akad. Wissenschaften)
P. M. Gruber (TU Wien)
G. Helmberg (Univ. Innsbruck)
H. Heugl (Wien)
W. Imrich (MU Leoben)
M. Koth (Univ. Wien)
C. Krattenthaler (Univ. Wien)
W. Kuich (TU Wien)
R. Mlitz (TU Wien)
W. Müller (Univ. Klagenfurt)
W. G. Nowak (Univ. Bodenkult. Wien)
L. Reich (Univ. Graz)
N. Rozsenich (Wien)
W. Schachermayer (Univ Wien)
F. Schweiger (Univ. Salzburg)
K. Sigmund (Univ. Wien)
H. Sorger (Wien)
H. Strasser (WU Wien)
W. Wurm (Wien)

Vorstand, Sektions- und Kommissionsvorsitzende gehören statutengemäß dem Beirat an.

Vorsitzende der Sektionen und Kommissionen:

W. Woess (Graz)
G. Kirchner (Innsbruck)
H. Kautschitsch (Klagenfurt)
F. Pillichshammer (Linz)
P. Hellekalek (Salzburg)
C. Krattenthaler (Wien)
H. Humenberger (Didaktikkommission)

Mitgliedsbeitrag:

Jahresbeitrag: € 20,–

Bankverbindung: Konto Nr. 229-103-892-00 der Bank Austria–Creditanstalt (IBAN AT83-1200-0229-1038-9200, BLZ 12000, BIC BKAUATWW).

Internationale Mathematische Nachrichten

International Mathematical News

Nouvelles Mathématiques Internationales

Nr. 212 (63. Jahrgang) **Dezember 2009**

Inhalt

Die Titelseite illustriert die Ungleichung von Hornich-Hlawka,

$$\|a\| + \|b\| + \|c\| + \|a+b+c\| \geq \|a+b\| + \|a+c\| + \|b+c\|,$$

die in euklidischen Vektorräumen genauso wie etwa in $L_1[0,1]$ und für linear abhängige a,b,c sogar in allen normierten Räumen gilt. In ℓ_p^n für $p,n \geq 3$ ist sie zum Beispiel nicht gültig.

Internat. Math. Nachrichten
Nr. 212 (2009), 1–10

Graphen, Ziffern und Kryptographie

Clemens Heuberger
TU Graz

Ziel dieses Artikels ist es, Einblicke in zwei meiner Arbeitsgebiete der letzten Zeit zu geben[1]. In beiden treten Graphen und Ziffernsysteme auf, allerdings in unterschiedlichen Rollen. Einmal führen graphentheoretische Fragestellungen zu Ergebnissen, die durch Ziffernsysteme beschrieben werden können. Andererseits führen Fragestellungen aus der Kryptographie zu Ziffernproblemen, die durch graphentheoretische Hilfsmittel gelöst werden können.

1 Eine Klasse „optimaler" Graphen

In der mathematischen Chemie werden verschiedene graphentheoretische Indizes untersucht, da sie Aufschluss über physiko-chemische Eigenschaften von Molekülen erlauben. Einer dieser Indizes ist der sogenannte Merrifield-Simmons-Index [12] (vgl. auch [16]), die Anzahl der unabhängigen Teilmengen der Knotenmenge eines Graphen. Eine Teilmenge von Knoten heißt unabhängig, wenn keine zwei in ihr enthaltenen Knoten adjazent sind. Von Interesse ist dann die Frage, welche Graphen einer gegebenen Klasse von Graphen (typischerweise Bäumen) von gegebener Ordnung diese Indizes minimierien bzw. maximieren.

Im konkreten Fall des Merrifield-Simmons-Index ist bekannt, dass dieser von einem Pfad minimiert und von einem Stern maximiert wird. Die Anwendungen in der Chemie motivieren allerdings die Einschränkung des Maximalgrads der Bäume. In einer gemeinsamen Arbeit mit Stephan Wagner [7] untersuchen wir jene Bäume von gegebenem Maximalgrad und gegebener Ordnung, die den Merrifield-Simmons-Index maximieren. An dieser Stelle soll darüber berichtet werden,

[1] *Anmerkung des Herausgebes:* Die Österreichische Mathematische Gesellschaft hat Clemens Heuberger eingeladen, als Förderungspreisträger 2008 an dieser Stelle einen Überblick über seine Arbeit zu geben.

ISSN 0020-7926

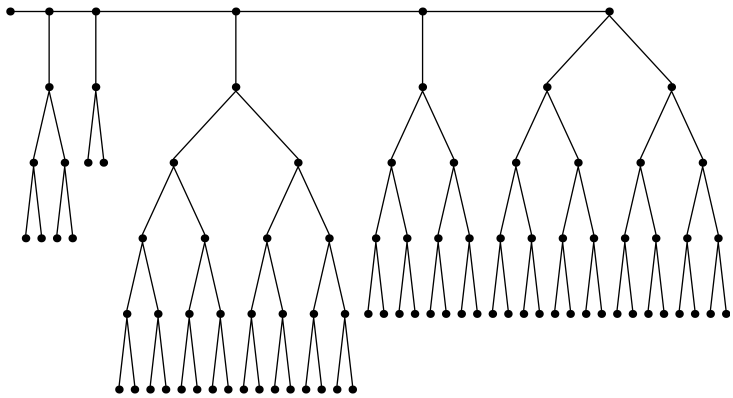

Abbildung 1: Optimaler Baum des Maximalgrads 3 der Ordnung 92.

wobei wir uns der einfacheren Darstellung halber auf den Fall von Maximalgrad 3 beschränken. Bäume, die den Merrifield-Simmons-Index für gegebene Ordnung maximieren, werden der Einfachheit halber im Folgenden als „optimale Bäume“ bezeichnet.

Durch eine effizient angelegte Computersuche [19] ist es möglich, für eine feste Ordnung n den optimalen Baum zu bestimmen. Beispielsweise ist das Ergebnis für $n = 92$ in Abbildung 1 dargestellt; dieser Baum besitzt übrigens 248 216 656 107 898 447 698 unabhängige Mengen.

Es erweist sich als günstig, *Wurzelbäume* zu betrachten, d.h., man zeichnet einen Knoten als Wurzel aus. Um dann die Anzahl der unabhängigen Mengen eines Baums T rekursiv zu bestimmen, definiert man zwei Hilfsgrößen: $\sigma_0(T)$ sei die Anzahl der unabhängigen Mengen, die die Wurzel nicht enthalten und $\sigma_1(T)$ sei die Anzahl der unabhängigen Mengen, die die Wurzel enthalten. Der Merrifield-Simmons-Index $\sigma(T)$ ergibt sich dann selbstverständlich als $\sigma(T) = \sigma_0(T) + \sigma_1(T)$. Zerlegt man einen Baum T in seine Wurzel v und Teilbäume T_1, $\dots$, T_k wie in Abbildung 2, so ergeben sich sofort die Rekursionen

$$\begin{aligned} \sigma_0(T) &= \prod_{j=1}^{k} \sigma(T_j), \\ \sigma_1(T) &= \prod_{j=1}^{k} \sigma_0(T_j). \end{aligned} \tag{1}$$

Weiters stellt sich heraus, dass die Größe $\rho(T) = \sigma_0(T)/\sigma(T)$ eine besondere Rolle spielt. Aus den Rekursionen (1) ergibt sich sofort

$$\rho(T) = \frac{1}{1 + \prod_{j=1}^{k} \rho(T_j)}.$$

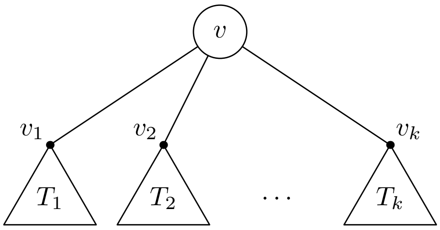

Abbildung 2: Zerlegung eines Wurzelbaums in Teilbäume.

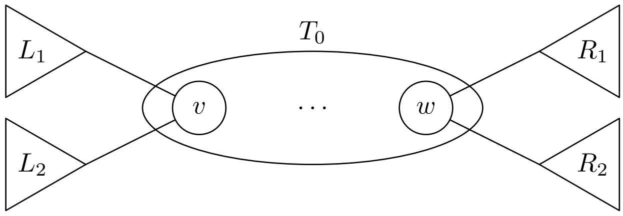

Abbildung 3: Zerlegung des Baums im notwendigen Optimalitätskriterium.

Den wesentlichen Zusammenhang zwischen den ρ-Werten von Teilbäumen und der Optimalität stellt das folgende notwendige Optimalitätskriterium her:

Lemma 1. *Sei T ein optimaler Baum. Wenn T wie in Abbildung 3 in (möglicherweise leere) Teilbäume L_1, L_2, R_1, R_2 und einen Baum T_0 mit $\rho(L_1) < \rho(R_1)$ zerlegt werden kann, dann gilt*

$$\max\{\rho(L_1), \rho(L_2)\} \leq \min\{\rho(R_1), \rho(R_2)\}.$$

Die Idee hinter dem Beweis ist die, nötigenfalls Teilbäume zu vertauschen, was wegen der angenommenen Optimalität von T zu einem Widerspruch geführt werden kann.

Lemma 1 wird nun wiederholt angewandt, um mehr über die Struktur optimaler Bäume zu erfahren. Als Endergebnis eines involvierten Induktionsbeweises erhält man schließlich folgende Beschreibung optimaler Bäume:

Satz 1 ([7])**.** *Jeder optimale Baum T vom Maximalgrad 3 kann in die in Abbildung 4 angegebene Form zerlegt werden, wobei $M_k \in \{B_k, B_{k+2}\}$ für $0 \leq k < \ell$ und $M_\ell \in \{B_\ell, B_{\ell+1}, B_{\ell+2}\}$. Hier bezeichnet B_h den vollständigen Binärbaum der Höhe $h-1$.*

Durch Einführung eines geeigneten Ziffernsystems können wir daraus ersehen, dass diese Beschreibung optimale Bäume eindeutig beschreibt: Ein Binärbaum B_j der Höhe $j-1$ besteht aus $2^j - 1$ Knoten. Damit erhalten wir aus der Zerlegung in Abbildung 4 die Beziehung

$$n = \ell + \left(2^{0+\delta_0} - 1\right) + \left(2^{1+\delta_1} - 1\right) + \left(2^{2+\delta_2} - 1\right) + \cdots + \left(2^{\ell+\delta_\ell} - 1\right), \qquad (2)$$

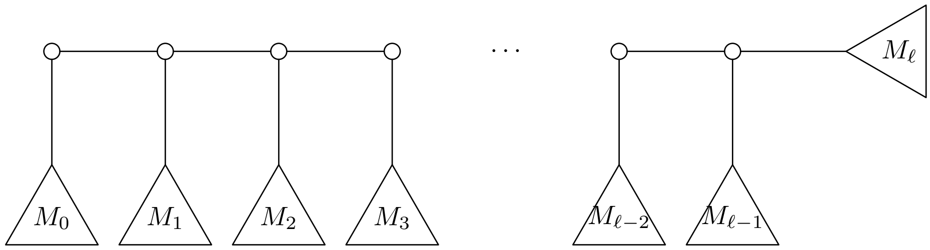

Abbildung 4: Zerlegung optimaler Bäume.

wobei $\delta_k \in \{0,1,2\}$ so gewählt wurde, dass $M_k = B_{k+\delta_k}$. Laut Satz 1 tritt $\delta_k = 1$ nur für $k = \ell$ auf. Setzt man $d_k = 2^{\delta_k}$, so ist (2) äquivalent zu

$$n+1 = \sum_{k=0}^{\ell} d_k 2^k.$$

Es handelt sich dabei offensichtlich um eine Ziffernentwicklung von $n+1$ zur Basis 2 mit Ziffern $\{1,2,4\}$, wobei die Ziffer 2 nur an der höchstwertigen Stelle zulässig ist.

In der Tat besitzt jede positive ganze Zahl m genau eine solche Zifferndarstellung: Für ungerades m ist die Ziffer $d_0 = 1$ an der niedrigstwertigen Stelle zu wählen, während für gerades $m > 2$ die Ziffer $d_0 = 4$ zu wählen ist. Man setzt dann rekursiv mit $(m-d_0)/2$ fort. Genau im Fall $m = 2$ ist die Ziffer $d_0 = 2$ zu wählen.

Diese Zifferndarstellung erlaubt also, die Eindeutigkeit der Zerlegung in Abbildung 4 festzustellen und auch optimale Bäume zu bestimmen.

Diese optimalen Bäume minimieren übrigens auch die Anzahl der unabhängigen Kantenteilmengen („Matchings“) [7] sowie die Energie (Summe der Absolutbeträge der Eigenwerte der Adjazenzmatrix) [8] über alle Bäume mit Maximalgrad 3 gegebener Ordnung. Für höheren Maximalgrad $b+1$ ergeben sich ähnliche Resultate; hier hat man es mit einer Ziffernentwicklung von $(b-1)n+1$ zur Basis b mit Ziffern aus $\{(b-1)+(b^2-1)r \mid 0 \leq r \leq b-1\}$ sowie zusätzlichen Ziffern an der höchstwertigen Stelle zu tun [7], [8].

2 Ziffernentwicklungen in der Kryptographie

Asymmetrische Kryptographieverfahren („Public-Key“-Kryptographie) beruhen auf Einwegfunktionen, d.h. Funktionen, deren Umkehrung als schwer gilt. Ein Beispiel ist die Skalarmultiplikation in geeigneten abelschen Gruppen: Gegeben sind eine Gruppe G und ein Element $P \in G$. Ein Skalar $n \in \mathbb{Z}$ wird dann auf nP abgebildet. Typische Gruppen sind die multiplikative Gruppe eines endlichen Körpers oder die Punktgruppe einer elliptischen Kurve über einem endlichen

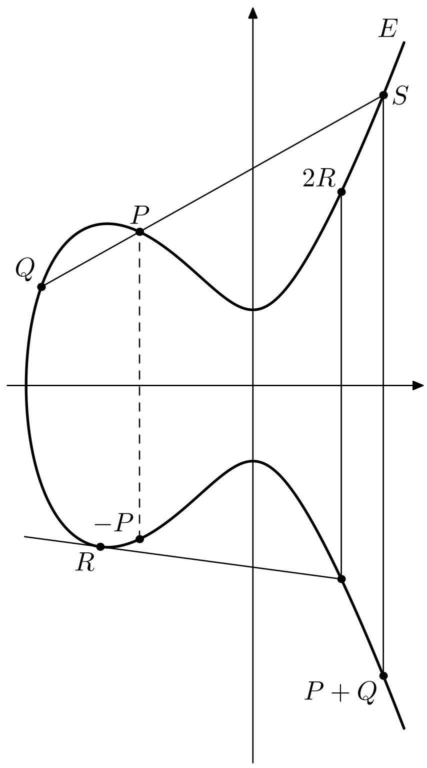

Abbildung 5: Addition von Punkten auf elliptischen Kurven.

Körper. Wir konzentrieren uns hier auf den letzteren Fall, unabhängig voneinander vorgeschlagen von Miller [13] und Koblitz [10], vgl. auch [1].

Über Körpern K, deren Charakteristik nicht 2 oder 3 ist – in diesen Fällen weichen die Formeln etwas ab –, kann eine elliptische Kurve in der Weierstraß-Form $Y^2 = X^3 + aX + b$ für konstante a und b geschrieben werden, wobei das kubische Polynom als quadratfrei vorausgesetzt wird. Die Punkte auf dieser Kurve bilden zusammen mit einem Fernpunkt 0 der projektiven Ebene eine abelsche Gruppe: Um zwei Punkte P und Q zu addieren, wird die Gerade durch P und Q mit der Kurve geschnitten, der dritte Schnittpunkt sei S. Anschließend wird die Gerade durch 0 und S ebenfalls mit der Kurve geschnitten. Der dritte Schnittpunkt ist dann das Ergebnis $P+Q$, vgl. Abbildung 5 im reellen Fall. Im Fall $P = Q$ ist die Tangente an die Kurve in diesem Punkt zu wählen.

Eine Methode, nP in einer beliebigen Gruppe zu berechnen, ist die additiv geschriebene Fassung der binären Exponentiation (vgl. Knuth [9]): Man bestimmt die Binärdarstellung $n = \sum_{j=0}^{\ell} d_j 2^j$ und berechnet nP als

$$nP = 2(2(\ldots 2(2(2(d_\ell P) + d_{\ell-1}P) + d_{\ell-2}P) \ldots + d_2P) + d_1P) + d_0P. \qquad (3)$$

Dabei führt man Additionen von $0P$ nicht durch. Dadurch ist die Anzahl der Additionen gleich dem (Hamming-)Gewicht von $d_\ell d_{\ell-1}\dots d_1 d_0$ (minus 1), d.h. die Anzahl der von 0 verschiedenen Ziffern, und die Anzahl der Verdoppelungen ist gleich ℓ, also im Wesentlichen $\log_2 n$.

In der Punktgruppe einer elliptischen Gruppe ist die Subtraktion von Punkten etwa gleich teuer wie eine Addition. Daher wurde vorgeschlagen [14], auch negative Ziffern in der Ziffernentwicklung von n zuzulassen. Beispielsweise gilt $62 = (111110)_2 = (10000\bar{1}0)_2$, wobei wir $\bar{1}$ für -1 schreiben. Wieder berechnet man nP entsprechend dem Horner-Schema (3); die Länge der Entwicklung bestimmt nach wie vor die Anzahl der Verdoppelungen und das Gewicht der Entwicklung entspricht der Anzahl der Additionen bzw. Subtraktionen. Im konkreten Beispiel wurde die Entwicklung zwar um eine Stelle länger, allerdings sank das Gewicht von 5 auf 2.

Durch das Zulassen der Ziffer -1 besitzt jede ganze Zahl mehrere Entwicklungen (wenn man die Länge nicht beschränkt, dann sogar unendlich viele). Diese Redundanz kann man dazu benutzen, um das Gewicht zu reduzieren. Unter allen Binärdarstellungen einer ganzen Zahl n sucht man also eine, die das Gewicht minimiert. Eine Lösung dieses Optimierungsproblems wurde bereits von Reitwiesner [17] im Kontext effizienter arithmetischer Operationen angegeben.

Satz 2 (Reitwiesner [17]). *Sei n eine ganze Zahl. Dann gibt es eine eindeutige Ziffernentwicklung $n = \sum_{j=0}^{\ell} \varepsilon_j 2^j$ mit Ziffern $\varepsilon_j \in \{0, \pm 1\}$, sodass $\varepsilon_j \varepsilon_{j+1} = 0$ für alle $0 \le j < \ell$ gilt.*

Diese Ziffernentwicklung minimiert das Gewicht über alle binären Ziffernentwicklungen von n mit Ziffern $\{0, \pm 1\}$.

Entsprechend der syntaktischen Bedingung $\varepsilon_j \varepsilon_{j+1} = 0$ wird diese Entwicklung als *Non-Adjacent-Form (NAF)* bezeichnet. Wir skizzieren hier kurz, wie die NAF einer ganzen Zahl n bestimmt wird. Wenn n gerade ist, so ist zwingend $\varepsilon_0 = 0$ zu wählen; man setzt dann mit $n/2$ fort. Wenn hingegen n ungerade ist, so ist die Restklasse von n modulo 4 zu betrachten. Wenn $n \equiv 1 \pmod 4$, so ist $\varepsilon_0 = 1$ und $\varepsilon_1 = 0$ zu setzen und mit $(n-1)/4$ fortzusetzen; wenn hingegen $n \equiv -1 \pmod 4$, so ist $\varepsilon_0 = -1$ und $\varepsilon_1 = 0$ zu setzen und mit $(n+1)/4$ fortzufahren.

Diese Regeln lassen sich auch in der Form eines endlichen Transduktors, d.h. eines endlichen Automaten, der einen Eingabestring in einen Ausgabestring übersetzt, schreiben. In unserem Fall besteht die Eingabe aus der üblichen Binärentwicklung einer positiven ganzen Zahl n, die Ausgabe aus ihrer NAF, der entsprechende Transduktor findet sich in Abbildung 6. Hier werden sämtliche Wörter von rechts nach links gelesen.

Der Transduktor ist also folgendermaßen zu lesen: Man startet im Zustand „0“. Wird in der Binärdarstellung eine 0 gelesen, so wird eine 0 in der NAF geschrieben und man ist nach wie vor in Zustand „0“. Wird hingegen eine 1 gelesen, so wird das leere Wort ε geschrieben und man ist in Zustand „odd“. Wird nun eine 0 gelesen, so sind wir im Fall $\equiv 1 \pmod 4$, schreiben 01 und sind wieder

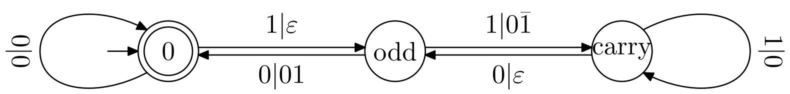

Abbildung 6: Transduktor zur Bestimmung der NAF aus der Binärentwicklung.

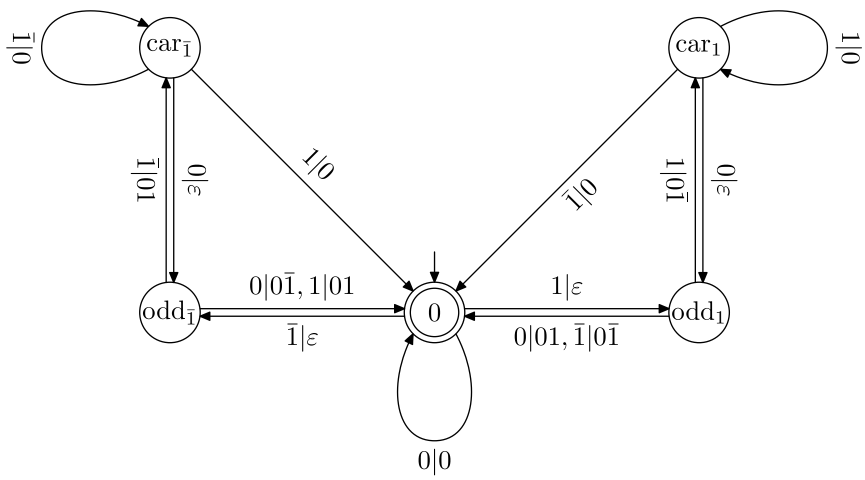

Abbildung 7: Transduktor zur Bestimmung der NAF aus einer beliebigen Binärentwicklung mit Ziffern 0, 1 und -1.

im Ausgangszustand. Folgt allerdings im Zustand „odd“ eine 1, so ist die derzeit gespeicherte Zahl kongruent zu $3 \pmod 4$, es ist also $0\bar{1}$ zu schreiben und ein Übertrag von 1 vorzumerken. Das entspricht dem Zustand „carry“. In diesem Zustand ist beim Auftreten von 1 die Zahl durch den Übertrag gerade, also ist 0 zu schreiben und wieder der Übertrag vorzumerken. Wird in der Binärentwicklung jedoch eine 0 gelesen, so ist die Zahl inklusive Übertrag ungerade, es ist das leere Wort ε zu schreiben und wieder in den Zustand „odd“ zu wechseln.

In analoger Weise kann man auch beliebige Binärentwicklungen mit Ziffern aus $\{0, \pm 1\}$ in die NAF übersetzen; der entsprechende Transduktor findet sich in Abbildung 7.

Dieser Transduktor kann auch für einen „automatischen“ Beweis der Optimalität der NAF verwendet werden: Man setzt das Gewicht einer Kante auf das Gewicht des Eingabeworts minus dem Gewicht des Ausgabeworts. Eine geschlossene Wanderung vom Startknoten „0“ zurück zu diesem Knoten von negativem Gewicht entspräche damit einer Darstellung einer Zahl mit Ziffern 0, 1, -1, deren Gewicht geringer als das Gewicht der NAF derselben Zahl ist. Berechnet man den kürzesten Weg von „0“ zu „0“ in diesem gewichteten gerichteten Graphen mit dem Bellman-Ford-Algorithmus, so stellt sich heraus, dass dieser Länge 0 hat. Das zeigt die Optimalität der NAF.

Die NAF ist inzwischen wohluntersucht, es gibt zum Beispiel eine präzise asymptotische Analyse des erwarteten Gewichts [18], des erwarteten Auftretens von Ziffernblöcken [4], Untersuchungen dynamischer Aspekte [2].

Eine Verallgemeinerung beruht auf der Tatsache, dass größere Ziffernmengen die Redundanz weiter erhöhen können und dadurch das Gewicht senken können. Für die Skalarmultiplikation nach (3) erfordert das dann die Vorausberechnung von dP für alle d aus der zulässigen Ziffernmenge. Eine optimale Entwicklung für eine Ziffernmenge der Form $\{\ell,\dots,0,1,\dots,u\}$ für ein $\ell \le 0$ und ein $u > 0$ wird von Philips und Burgess [15] angegeben.

Weiters wird untersucht, wie Linearkombinationen $mP + nQ$ effizient berechnet werden können. Effizienter als die einzelne Berechnung von mP und nQ ist es, eine gemeinsame Entwicklung von (m,n) zu bestimmen und dann bei der Linearkombination in einem Durchgang von links nach rechts entsprechende vorberechnete Linearkombinationen m_jP+n_jQ mit z.B. $|m_j|$, $|n_j| \le 1$ zu addieren. Optimale Entwicklungen für die von Philips und Burgess angegebene Ziffernmenge finden sich in [6].

3 Komplexe Basen

Auf speziellen elliptischen Kurven können noch Entwicklungen zu anderen, i.A. komplexen, Basen untersucht werden. Koblitz [11] führte die (seither nach ihm benannten) Kurven

$$Y^2 + XY = X^3 + aX^2 + 1,$$

über dem endlichen Körper $\mathbb{F}_{2^m}$ der Charakteristik 2 ein, wobei $a \in \{0,1\}$.

Der Frobenius-Automorphismus $\tau : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ mit $x \mapsto x^2$ kann durch komponentenweise Anwendung zu einem Endomorphismus der elliptischen Kurve fortgesetzt werden. Da für alle Punkte P auf der Kurve die Beziehung

$$\tau(\tau(P)) + 2P = \mu\tau(P) \text{ mit } \mu = (-1)^{1-a}$$

gilt, erfüllt τ im Endomorphismenring der Kurve die Gleichung

$$\tau^2 + 2 = \mu\tau$$

und kann damit mit der komplexen Zahl

$$\frac{\mu + \sqrt{-7}}{2}$$

identifiziert werden.

Hat man ein $n \in \mathbb{Z}$ als Entwicklung zur Basis τ gegeben, so kann eine Skalarmultiplikation nun durch wiederholte Anwendung des Frobenius-Automorphismus und durch Addition ausgeführt werden. Dabei ist zu bemerken, dass der Frobenius-Automorphismus (zwei Quadrate im Körper) deutlich schneller als eine Verdoppelung auf der Kurve ist.

Nun können einige der Konzepte aus dem binären Fall auf den Fall von Basis τ verallgemeinert werden; insbesondere besitzt wieder jedes $n \in \mathbb{Z}$ (und auch jedes $n \in \mathbb{Z}[\tau]$) eine τ-NAF, also wieder eine Entwicklung mit derselben syntaktischen Bedingung $\varepsilon_j \varepsilon_{j+1} = 0$ wie die klassische NAF. Diese τ-NAF ist wiederum optimal [3].

Versucht man allerdings wieder die Ziffernmenge zu vergrößern oder Linearkombinationen zu betrachten, so geht meist die Optimalität verloren. Man kann in vielen Fällen sogar zeigen [5], dass es unmöglich ist, optimale Entwicklungen durch einen Transduktor zu berechnen: Es gibt Zahlen, die τ-adisch beliebig nahe sind, deren niedrigstwertige Stelle in jeder optimalen Darstellung jedoch verschieden sein muss. Für den Beweis konstruiert man wiederum einen entsprechenden gerichteten Graphen, in dem kürzeste Wege berechnet werden.

Literatur

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, and K. Nguyen, *Handbook of elliptic and hyperelliptic curve cryptography*, CRC Press Series on Discrete Mathematics and its Applications, vol. 34, Chapman & Hall/CRC, Boca Raton, FL, 2005.

[2] K. Dajani, C. Kraaikamp, and P. Liardet, *Ergodic properties of signed binary expansions*, Discrete Contin. Dyn. Syst. **15** (2006), 87–119.

[3] D. M. Gordon, *A survey of fast exponentiation methods*, J. Algorithms **27** (1998), 129–146.

[4] P. J. Grabner, C. Heuberger, and H. Prodinger, *Subblock occurrences in signed digit representations*, Glasg. Math. J. **45** (2003), 427–440.

[5] C. Heuberger, *Redundant τ-adic expansions II: Non-optimality and chaotic behaviour*, to appear in Math. Comput. Sci. electronically available in the Cryptology ePrint Archive, Report 2008/153, *http://eprint.iacr.org/*.

[6] C. Heuberger and J. A. Muir, *Minimal weight and colexicographically minimal integer representations*, J. Math. Cryptol. **1** (2007), 297–328.

[7] C. Heuberger and S. G. Wagner, *Maximizing the number of independent subsets over trees with bounded degree*, J. Graph Theory **58** (2008), 49–68.

[8] ______, *Chemical trees minimizing energy and Hosoya index*, J. Math. Chem. **46** (2009), 214–230.

[9] D. E. Knuth, *Seminumerical algorithms*, third ed., The Art of Computer Programming, vol. 2, Addison-Wesley, 1998.

[10] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), 203–209.

[11] N. Koblitz, *CM-curves with good cryptographic properties*, Advances in cryptology – CRYPTO '91 (Santa Barbara, CA, 1991), Lecture Notes in Comput. Sci., vol. 576, Springer, Berlin, 1992, pp. 279–287.

[12] R. E. Merrifield and H. E. Simmons, *Topological Methods in Chemistry*, Wiley, New York, 1989.

[13] V. S. Miller, *Use of elliptic curves in cryptography*, Advances in cryptology – CRYPTO '85, Lecture Notes in Comput. Sci., vol. 218, Springer-Verlag, Berlin, 1986, pp. 417–426.

[14] F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO Inform. Théor. Appl. **24** (1990), 531–543.

[15] B. Phillips and N. Burgess, *Minimal weight digit set conversions*, IEEE Trans. Comput. **53** (2004), 666–677.

[16] H. Prodinger and R. F. Tichy, *Fibonacci numbers of graphs*, Fibonacci Quart. **20** (1982), 16–21.

[17] G. W. Reitwiesner, *Binary arithmetic*, Advances in computers, vol. 1, Academic Press, New York, 1960, pp. 231–308.

[18] J. M. Thuswaldner, *Summatory functions of digital sums occurring in cryptography*, Period. Math. Hungar. **38** (1999), 111–130.

[19] R. F. Tichy and S. G. Wagner, *Algorithmic generation of molecular graphs with large Merrifield-Simmons index*, MATCH Commun. Math. Comput. Chem. **59** (2008), 239–252.

Adresse des Autors:

Clemens Heuberger
Technische Universität Graz
Institut für Optimierung und Diskrete Mathematik (Math B)
Steyrergasse 30, 8010 Graz
email clemens.heuberger@tugraz.at,
http://www.math.tugraz.at/∼cheub

Internat. Math. Nachrichten
Nr. 212 (2009), 11–21

Transfinite Dimensionen

Gerald Kuba
Universität für Bodenkultur, Wien

Für eine beliebige Menge I ist $\mathbb{R}^I$ die Menge aller Abbildungen von I nach $\mathbb{R}$. Ein Element f von $\mathbb{R}^I$ schreibt man gern in der Form $(x_i)_{i\in I}$ und meint damit, dass $x_i = f(i)$ für alle $i \in I$ gilt. Man nennt in diesem Zusammenhang die Menge I eine *Indexmenge*. Für jedes $i \in I$ ist x_i die i-te *Komponente* von $(x_i)_{i\in I}$. Ist I gleich der endlichen Menge $\{1,2,\dots,n\}$, so ist $\mathbb{R}^I$ natürlich nichts anderes als der wohlvertraute euklidische Raum $\mathbb{R}^n$, der genau die n-Tupel $(x_1,x_2,\dots,x_n)$ reeller Zahlen enthält. Hat man $I = \mathbb{N}$, so ist $\mathbb{R}^I$ die Menge aller Folgen $(x_0,x_1,x_2,\dots)$ reeller Zahlen.

Für jede Indexmenge I ist der Raum $\mathbb{R}^I$ auf kanonische Weise ein reeller Vektorraum: Die Addition zweier Vektoren und die Multiplikation eines Vektors mit einer reellen Zahl ist komponentenweise definiert. Die Dimension des Vektorraums $\mathbb{R}^I$ ist bei beliebig gewählter endlicher Indexmenge I natürlich stets gleich $|I|$. (Allgemein ist die *Dimension* eines beliebigen Vektorraums $\mathcal{V}$ die wohldefinierte Kardinalzahl einer Basis von $\mathcal{V}$.)

Die *Kardinalzahlen* sind ausgezeichnete Mengen dergestalt, dass jede Menge M mit genau einer Kardinalzahl $|M|$ gleichmächtig ist. Insbesondere gilt $|A| = |B|$ dann und nur dann, wenn man A bijektiv auf B abbilden kann. Die *endlichen* bzw. *finiten* Kardinalzahlen werden mit den Elementen von $\mathbb{N}$ identifiziert, wobei $0 \in \mathbb{N}$ gelten soll, sodass für jede endliche Menge E die Kardinalzahl $|E|$ die Anzahl der Elemente von E ist. Wichtige *transfinite* Kardinalzahlen sind $\aleph_0 := |\mathbb{N}|$ und $c := |\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$. (Dabei ist $\mathcal{P}(M) = \{X \mid X \subset M\}$ die Potenzmenge von M.) Man definiert ferner $|A|^{|B|} := |A^B|$, wobei A^B die Menge aller Abbildungen von B nach A ist. Mit der mengentheoretischen Standarddefinition $2 = \{0,1\}$ gilt allgemein $2^{|M|} = |\{0,1\}^M| = |\mathcal{P}(M)|$ und insbesondere $2^{\aleph_0} = c$. Stets gilt $|M| < 2^{|M|}$, wobei $|A| < |B|$ heißt, dass es eine injektive Abbildung von A nach B, aber keine bijektive Abbildung von A nach B gibt. Insbesondere ist $\aleph_0$ die kleinste transfinite Kardinalzahl, da $|A| < \aleph_0$ mit $|A| \in \mathbb{N}$ gleichbedeutend ist. Ferner ist $\aleph_1$ die kleinste überabzählbare Kardinalzahl, d.h. allgemein gilt $|A| < \aleph_1$ genau dann, wenn A abzählbar ist.

Dass die Dimension von $\mathbb{R}^I$ gleich $|I|$ ist, ist (wie wir sehen werden) jedoch nur für endliche Indexmengen richtig. So ist bereits im Falle $|I| = \aleph_0$ und speziell für $I = \mathbb{N}$ die Dimension von $\mathbb{R}^I$ größer als $\aleph_0$, also überabzählbar. Dies scheint

ISSN 0020-7926

ein wenig merkwürdig, interpretiert man doch gern die kleinste transfinite Kardinalzahl $\aleph_0$ als durch die finiten Kardinalzahlen $n \in \mathbb{N}$ *extrapoliert*. (Im strengen Sinn ist ja auch $\aleph_0$ das *Supremum* der Menge $\mathbb{N}$.) Der Raum $\mathbb{R}^n$ besteht aus allen Zahlenfolgen $(x_i)_{i<n}$ mit genau n Eintragungen und ist auch n-dimensional. Der Raum $\mathbb{R}^{\mathbb{N}}$ besteht aus allen Zahlenfolgen $(x_i)_{i\in\mathbb{N}}$ mit genau $\aleph_0$ Eintragungen und hat trotzdem nicht die Dimension $\aleph_0$!

Der Grund für diese Unstetigkeit der Funktion, die jeder Kardinalzahl κ die Dimension $\dim \mathbb{R}^\kappa$ des Vektorraums $\mathbb{R}^\kappa$ zuordnet, liegt darin, dass der Raum $\mathbb{R}^{\mathbb{N}}$ nicht die einzige und im Zusammenhang mit der Dimension nicht die richtige Extrapolation der endlichdimensionalen Räume $\mathbb{R}^n$ $(n \in \mathbb{N})$ ist. Die andere bzw. richtige Extrapolation ist der Polynomring $\mathbb{R}[X]$, dessen Dimension als reeller Vektorraum nun wirklich gleich $\aleph_0$ ist, hat er doch die kanonische Basis $\{1, X, X^2, X^3, \dots\}$. Für $n \in \mathbb{N}$ entspricht der Raum $\mathbb{R}^n$ dem Teilraum von $\mathbb{R}[X]$, der alle reellen Polynome vom Grad kleiner als n enthält.[1] In diesem Sinne ist $\mathbb{R}[X]$ nichts anderes als der lineare Teilraum von $\mathbb{R}^{\mathbb{N}}$, der aus genau den Zahlenfolgen $(x_n)_{n\in\mathbb{N}}$ besteht, deren Komponenten *fast alle verschwinden*, soll heißen: die Menge $\{n \in \mathbb{N} \mid x_n \neq 0\}$ ist stets endlich.

Denkt man sich den Vektorraum $\mathbb{R}^{\mathbb{N}}$ mit seiner kanonischen Topologie der komponentenweisen Konvergenz versehen, so liegt (offensichtlich) der $\aleph_0$-dimensionale Teilraum $\mathbb{R}[X]$ dicht in $\mathbb{R}^{\mathbb{N}}$. Auch deshalb ist es, wenn auch nicht merkwürdig, durchaus bemerkenswert, dass die Funktion $\kappa \mapsto \dim \mathbb{R}^\kappa$ die Kardinalzahl $\aleph_0$ überspringt.

Satz 1. *Es gilt* $\dim \mathbb{R}^{\mathbb{N}} = c$. *Insbesondere ist die Dimension des Raumes $\mathbb{R}^{\mathbb{N}}$ identisch mit der Kardinalzahl der Menge $\mathbb{R}^{\mathbb{N}}$.*

Da $|\mathbb{R}^{\mathbb{N}}| = c$ gilt, genügt es zum Beweis von Satz 1, eine linear unabhängige Teilmenge $\mathcal{L}$ von $\mathbb{R}^{\mathbb{N}}$ anzugeben, für die $|\mathcal{L}| = c$ gilt. Um eine solche Menge zu gewinnen, verwenden wir das folgende Lemma.

Lemma 1. *Ist A eine abzählbar unendliche Menge, so gibt es eine Familie $\mathcal{F}$ von Mengen $F \subset A$ dergestalt, dass*

(1) F unendlich für alle $F \in \mathcal{F}$ ist,

(2) $F_1 \cap F_2$ für verschiedene $F_1, F_2 \in \mathcal{F}$ endlich ist,

(3) $\mathcal{F}$ von der Mächtigkeit des Kontinuums ist.

Beweis. O.B.d.A. sei $A = \mathbb{Q}$. Zu jeder reellen Zahl ξ konstruieren wir eine Folge $\big(r_n(\xi)\big)_{n\in\mathbb{N}}$ rationaler Zahlen dergestalt, dass

$$\xi + \frac{1}{n+2} < r_n(\xi) < \xi + \frac{1}{n+1}$$

[1] Formal ist diese Entsprechung (nach der üblichen Definition eines Polynoms) sogar die Identität.

für alle $n \in \mathbb{N}$ gilt. Da $\mathbb{Q}$ dicht in $\mathbb{R}$ liegt, ist dies natürlich möglich. Nun setzen wir $F_\xi = \{r_n(\xi) \mid n \in \mathbb{N}\}$ und haben damit für alle $\xi \in \mathbb{R}$ eine unendliche Teilmenge F_ξ von $\mathbb{Q}$ definiert. Da konstruktionsgemäß $\lim\limits_{n\to\infty} r_n(\xi) = \xi$ für alle $\xi \in \mathbb{R}$ gilt, muss die Menge $F_\xi \cap F_{\xi'}$ für verschiedene $\xi, \xi' \in \mathbb{R}$ stets endlich sein. Insbesondere gilt stets $F_\xi \neq F_{\xi'}$ für verschiedene $\xi, \xi' \in \mathbb{R}$. Somit ist $\mathcal{F} = \{F_\xi \mid \xi \in \mathbb{R}\}$ eine Familie von Teilmengen von $\mathbb{Q}$, die (1), (2) und (3) erfüllt. $\square$

Beweis. (von Satz 1). Um nun Satz 1 mithilfe von Lemma 1 zu beweisen, sei $\mathcal{F}$ eine Familie wie in Lemma 1 mit $A = \mathbb{N}$. Für $M \subset \mathbb{N}$ sei 1_M die charakteristische Funktion der Menge M. Es ist also 1_M eine Abbildung von $\mathbb{N}$ nach $\mathbb{R}$ dergestalt, dass $1_M(x) \in \{0,1\}$ für alle $x \in \mathbb{N}$ gilt, und zwar gilt $1_M(x) = 1$ im Falle $x \in M$ und $1_M(x) = 0$ im Falle $x \notin M$. Im Lichte von Lemma 1 (3) sind wir mit dem Nachweis, dass $\mathcal{L} := \{1_F \mid F \in \mathcal{F}\}$ linear unabhängig ist, fertig.

Es seien paarweise verschiedene $f_1, f_2, \ldots, f_m \in \mathcal{L}$ beliebig gewählt und es gelte

$$(*) \qquad \textstyle\sum_{k=1}^{m} \lambda_k \cdot f_k = 1_\emptyset$$

mit $\lambda_k \in \mathbb{R}$. (Die Funktion $1_\emptyset : n \mapsto 0$ ist der Nullvektor im Raum $\mathbb{R}^\mathbb{N}$.)

Sind nun $F_1, \ldots, F_m \subset \mathbb{N}$ dergestalt, dass $f_i = 1_{F_i}$, so sind die Mengen $F_1, F_2, \ldots, F_m$ paarweise verschieden. Wegen Lemma 1 (2) kann jede der Mengen F_i die Vereinigung aller anderen Mengen nur in endlich vielen Elementen von $\mathbb{N}$ treffen. Daher können wir wegen Lemma 1 (1) in jeder Menge F_i leicht ein x_i bestimmen, das nicht in der Vereinigung der anderen Mengen liegt. Dann sind die m Vektoren

$$\big(f_1(x_i), f_2(x_i), \ldots, f_m(x_i)\big) \quad (i = 1, 2, \ldots, m)$$

aber offensichtlich genau die *Standardbasisvektoren* des $\mathbb{R}^m$ und daher erhält man durch Belegung der Funktionalgleichung $(*)$ mit den Argumenten $x_1, x_2, \ldots, x_m$ ein Gleichungssystem, das nur die triviale Lösung $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$ besitzt. Damit ist Satz 1 bewiesen. $\square$

Nachdem wir die Dimensionsfrage für den Raum $\mathbb{R}^\mathbb{N}$ (und damit zugleich für alle Räume $\mathbb{R}^I$ mit $|I| = \aleph_0$) erledigt haben, wenden wir uns den Räumen $\mathbb{R}^I$ mit *überabzählbarer* Indexmenge zu. Der wichtigste dieser Räume ist natürlich der Raum $\mathbb{R}^\mathbb{R}$ aller Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Für diesen Raum gibt es ein Analogon zum Polynomring $\mathbb{R}[X]$ im Raum $\mathbb{R}^\mathbb{N}$, nämlich die Menge

$$\mathcal{Y} := \big\{(x_i)_{i\in\mathbb{R}} \in \mathbb{R}^\mathbb{R} \mid |\{i \in \mathbb{R} \mid x_i \neq 0\}| < \aleph_0\big\},$$

die natürlich einen Teilraum von $\mathbb{R}^\mathbb{R}$ bildet. Es gilt $|\mathcal{Y}| = c$, während $|\mathbb{R}^\mathbb{R}| = 2^c > c$ gilt. Die Dimension von $\mathcal{Y}$ ist gleich c, da die Vektoren $(\delta_{ij})_{i\in\mathbb{R}}$ $(j \in \mathbb{R})$ offensichtlich eine Basis von $\mathcal{Y}$ bilden (in der Kroneckerschen Schreibweise $\delta_{ij} = 1$ im Falle $i = j$ und $\delta_{ij} = 0$ im Falle $i \neq j$). Und bezüglich der kanonischen Topologie der punktweisen Konvergenz des Raums $\mathbb{R}^{\mathbb{R}}$ liegt $\mathcal{Y}$ dicht in $\mathbb{R}^{\mathbb{R}}$, ist doch eine Menge $U \subset \mathbb{R}^{\mathbb{R}}$ genau dann offen, wenn sie eine Menge der Form $\prod_{i \in \mathbb{R}} U_i$ enthält mit $U_i \subset \mathbb{R}$ offen in $\mathbb{R}$ und $|\{i \in \mathbb{R} \mid U_i \neq \mathbb{R}\}| < \aleph_0$.

Wie schon für $I = \mathbb{N}$ ist nun für $I = \mathbb{R}$ die Dimension des Raums $\mathbb{R}^I$ größer als $|I|$, es gilt also $\dim \mathbb{R}^{\mathbb{R}} > c$. Die Dimension des Raums $\mathbb{R}^{\mathbb{R}}$ kann ebenfalls exakt bestimmt werden: Es gilt $\dim \mathbb{R}^{\mathbb{R}} = 2^c$. Dies resultiert aus dem folgenden Satz, den wir später in einem allgemeineren Zusammenhang beweisen werden.

Satz 2. *Für alle unendlichen Indexmengen I gilt* $\dim \mathbb{R}^I = 2^{|I|}$.

Bie jetzt haben wir nur *reelle* Vektorräume betrachtet. Da die algebraische Struktur von $\mathbb{R}$ keine wesentliche Rolle spielt, bleiben die Sätze 1 und 2 gültig, wenn man den Körper $\mathbb{R}$ durch den Körper $\mathbb{C}$ oder auch durch irgendeinen Körper $\mathbb{K}$ mit $|\mathbb{K}| = c$ ersetzt. Für Vektorräume über beliebigen Körpern ist der folgende Satz sehr hilfreich.

Satz 3. *Für jeden Körper $\mathbb{K}$ ist $\mathcal{U} = \{(a^n)_{n \in \mathbb{N}} \mid 0 \neq a \in \mathbb{K}\}$ eine linear unabhängige Teilmenge des $\mathbb{K}$-Vektorraums $\mathbb{K}^{\mathbb{N}}$.*

Beweis. Es seien $a_1, a_2, \ldots, a_m \in \mathbb{K}$ paarweise verschieden. Zu zeigen ist, dass für beliebige $\lambda_1, \lambda_2, \ldots, \lambda_m \in \mathbb{K}$

$$\textstyle\sum_{k=1}^{m} \lambda_k \cdot (a_k^n)_{n \in \mathbb{N}}$$

nur dann der Nullvektor $(0, 0, 0, \ldots)$ im Raum $\mathbb{K}^{\mathbb{N}}$ ist, wenn $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$ gilt. Dies heißt nichts anderes, als dass

$$\forall n \in \mathbb{N}: \quad \textstyle\sum_{k=1}^{m} \lambda_k \cdot a_k^n = 0$$

nur dann gilt, wenn $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$ gilt. Nun folgt $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$ aber bereits aus der schwächeren Voraussetzung

$$\forall n \in \{0, 1, \ldots, m-1\}: \quad \textstyle\sum_{k=1}^{m} \lambda_k \cdot a_k^n = 0,$$

da dieses Gleichungssystem quadratisch mit der Koeffizientenmatrix

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_m \\ a_1^2 & a_2^2 & \ldots & a_m^2 \\ \vdots & \vdots & & \vdots \\ a_1^{m-1} & a_2^{m-1} & \ldots & a_m^{m-1} \end{pmatrix}$$

ist. Denn die Determinante dieser Matrix ist eine Vandermondesche und somit gleich

$$\textstyle\prod_{1 \leq i < j \leq m} (a_j - a_i) \neq 0. \qquad \square$$

Bemerkung: Satz 3 liefert einen alternativen Beweis von Satz 1, ist doch in Satz 3 die Menge $\mathcal{U}$ offensichtlich gleichmächtig mit der Menge $\mathbb{K} \setminus \{0\}$ und somit gleichmächtig mit $\mathbb{K}$, falls $\mathbb{K}$ ein unendlicher Körper ist. Für einen endlichen Körper $\mathbb{K}$ ist Satz 3 ohne Nutzen für die Bestimmung der Dimension des Raums $\mathbb{K}^{\mathbb{N}}$. Mithilfe des folgenden Satzes bekommt man jedoch sofort $\dim \mathbb{K}^{\mathbb{N}} = c$ für jeden endlichen Körper $\mathbb{K}$.

Satz 4. *Ist $\mathbb{K}$ ein endlicher Körper und I eine unendliche Indexmenge, so gilt stets* $\dim \mathbb{K}^I = 2^{|I|}$.

Da für eine endliche Menge K mit $|K| \geq 2$ und eine unendliche Menge I wegen $2^{|I|} = |\{0,1\}^I| \leq |K^I| \leq |I^I| = 2^{|I|}$ stets $|K^I| = 2^{|I|}$ gilt, folgt Satz 4 sofort aus

Satz 5. *Ist $\mathbb{K}$ ein beliebiger Körper und I eine unendliche Indexmenge, so gilt immer* $\dim \mathbb{K}^I = |\mathbb{K}^I|$, *falls* $|\mathbb{K}| < |\mathbb{K}^I|$ *gewährleistet ist.*

Beweis. Trivialerweise gilt $\dim \mathbb{K}^I \leq |\mathbb{K}^I|$. Indirekt angenommen, $\dim \mathbb{K}^I < |\mathbb{K}^I|$. Dann gibt es eine Kardinalzahl $\kappa < |\mathbb{K}^I|$, sodass $|\mathcal{B}| = \kappa$ für irgendeine Basis $\mathcal{B}$ des Vektorraums $\mathbb{K}^I$ gilt. Ist $T(E)$ der Teilraum von $\mathbb{K}^I$, der von einer *endlichen* Menge $E \subset \mathcal{B}$ erzeugt wird, so haben wir $\mathbb{K}^I = \bigcup\{T(E) \mid E \in \mathcal{E}\}$, wobei $\mathcal{E}$ die Familie aller endlichen Teilmengen von $\mathcal{B}$ ist. Da $|T(E)|$ für einen endlichen Körper $\mathbb{K}$ endlich ist, ansonsten aber nicht größer als $|\mathbb{K}|$ ist, und da entweder $\mathcal{E}$ endlich ist oder $|\mathcal{E}| = |\mathcal{B}| = \kappa$ gilt, bekommen wir $|\bigcup\{T(E) \mid E \in \mathcal{E}\}| \leq \max\{\kappa, |\mathbb{K}|, \aleph_0\} < |\mathbb{K}^I|$ und das ist ein Widerspruch zu $\mathbb{K}^I = \bigcup\{T(E) \mid E \in \mathcal{E}\}$.
Da für nichtleere Mengen K, I stets $|K| \leq |K^I|$ gilt, bleibt die Größe von $\dim \mathbb{K}^I$ nur noch im Falle $|\mathbb{K}| = |\mathbb{K}^I|$ zu bestimmen. Man beachte, dass $|K| = |K^I|$ für eine unendliche Menge I nur dann gilt, wenn K unendlich oder leer ist. Ein Körper $\mathbb{K}$, der $|\mathbb{K}| = |\mathbb{K}^I|$ für eine unendliche Indexmenge I erfüllt, muss also unendlich sein. □

Satz 6. *Ist $\mathbb{K}$ ein unendlicher Körper und I eine unendliche Indexmenge, so gilt stets* $\dim \mathbb{K}^I = |\mathbb{K}|$, *sofern* $|\mathbb{K}| = |\mathbb{K}^I|$ *gilt.*

Beweis. Die Indexmenge I enthält sicher eine abzählbar unendliche Teilmenge. Da I eine nackte Menge ist, können wir gleich $\mathbb{N} \subset I$ annehmen. Da man natürlich den Vektorraum $\mathbb{K}^{\mathbb{N}}$ in den Vektorraum $\mathbb{K}^I$ isomorph einbetten kann, gilt $\dim \mathbb{K}^{\mathbb{N}} \leq \dim \mathbb{K}^I$. Nach Satz 3 gilt $\dim \mathbb{K}^{\mathbb{N}} \geq |\mathbb{K}|$. Trivialerweise gilt $\dim \mathbb{K}^I \leq |\mathbb{K}^I|$. □

Zusammenfassend können wir somit den folgenden Satz formulieren:

Satz 7. *Ist $\mathbb{K}$ ein beliebiger Körper und I eine unendliche Indexmenge, so gilt stets* $\dim \mathbb{K}^I = |\mathbb{K}^I|$. *Insbesondere gilt stets* $\dim \mathbb{K}^I > |I|$.

Aus Satz 7 ergibt sich nun auch gleich der folgende Satz, der Satz 4 verallgemeinert und den noch unbewiesenen Satz 2 impliziert.

Satz 8. *Ist I eine unendliche Indexmenge und $\mathbb{K}$ ein Körper, dessen Kardinalität nicht größer als $2^{|I|}$ ist, so gilt stets* $\dim \mathbb{K}^I = 2^{|I|}$.

Beweis. Im Lichte von Satz 7 ist lediglich $|\mathbb{K}^I| = 2^{|I|}$ zu verifizieren. Dies ist aber eine mengentheoretische Trivialität: Für beliebige Kardinalzahlen κ, λ mit $2 \leq \kappa \leq 2^\lambda$ und $\lambda \geq \aleph_0$ gilt natürlich $\kappa^\lambda = 2^\lambda$ wegen $\kappa^\lambda \geq 2^\lambda$ und $\kappa^\lambda \leq (2^\lambda)^\lambda = 2^\lambda$. □

Kehren wir nun wieder zu den reellen (bzw. komplexen) Vektorräumen zurück. Hier liefert Satz 8 sofort folgenden Satz, der dem bekannten Satz entspricht, dass jeder n-dimensionale Vektorraum über $\mathbb{R}$ bzw. $\mathbb{C}$ isomorph mit dem Koordinatenraum $\mathbb{R}^n$ bzw. $\mathbb{C}^n$ ist.

Satz 9. *Ist $\mathcal{V}$ ein reeller bzw. komplexer Vektorraum der Dimension λ für eine transfinite Kardinalzahl λ, so ist $\mathcal{V}$ genau dann isomorph zu einem Komponentenraum $\mathbb{R}^I$ bzw. $\mathbb{C}^I$, wenn $\lambda = 2^\kappa$ für eine Kardinalzahl κ ist. Trifft dies zu, kann man $|I| = \kappa$ wählen.*

Nach Satz 7 haben alle $\mathbb{K}$-Vektorräume der Gestalt $\mathbb{K}^I$ mit einer unendlichen Indexmenge die Eigenschaft, dass die Dimension des Raums identisch mit seiner Kardinalität ist. Der reelle Vektorraum $\mathbb{R}[X]$ hat diese Eigenschaft nicht. Jedoch hat, wie wir sehen werden, jeder unendlichdimensionale Hilbertraum diese Eigenschaft. Wir behandeln zunächst die wichtige Klasse der *separablen* Hilberträume.

Satz 10. *Ist $\mathcal{H}$ ein unendlichdimensionaler separabler Hilbertraum über $\mathbb{R}$ bzw. $\mathbb{C}$, so gilt* $\dim \mathcal{H} = |\mathcal{H}| = c$. *Insbesondere ist $\mathcal{H}$ (algebraisch) isomorph zum Vektorraum $\mathbb{R}^{\mathbb{N}}$ bzw. $\mathbb{C}^{\mathbb{N}}$.*

Beweis. Mit $\mathbb{K} = \mathbb{R}$ bzw. $\mathbb{K} = \mathbb{C}$ ist $\mathcal{H}$ bekanntlich *normisomorph* zum Hilbertraum

$$\ell^2 := \left\{ (x_k)_{k\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}} \;\middle|\; \textstyle\sum_{k=0}^\infty |x_k|^2 < \infty \right\}.$$

Rein algebraisch ist der Raum ℓ^2 ein Teilraum des Vektorraums $\mathbb{K}^{\mathbb{N}}$. Die Menge

$$\mathcal{U}_1 = \{(a^n)_{n\in\mathbb{N}} \mid 0 \neq |a| < 1\}$$

ist eine Teilmenge von ℓ^2, da die Reihe $\sum_{k=0}^\infty |a^n|^2 = \sum_{k=0}^\infty |a^2|^n$ als geometrische Reihe für $|a| < 1 \iff |a^2| < 1$ konvergiert. Trivialerweise gilt $|\mathcal{U}_1| = c$ und somit gilt wegen $|\mathbb{K}^{\mathbb{N}}| = c$ automatisch $|\ell^2| = c$. Schließlich ist $\mathcal{U}_1$ wegen Satz 3 a fortiori linear unabhängig. Somit gilt $c = |\mathcal{U}_1| \leq \dim \ell^2 \leq \dim \mathbb{K}^{\mathbb{N}} = c$. Wegen der Isomorphie zwischen ℓ^2 und $\mathcal{H}$ gilt daher tatsächlich $\dim \mathcal{H} = |\mathcal{H}| = c$. □

Betrachtet man des Weiteren auch *nichtseparable* Hilberträume, so sind dieselben (bis auf Isomorphie) durch die Räume $\ell^2(S)$ mit einer überabzählbaren Indexmenge S gegeben. Allgemein ist $\ell^2(S)$ ein Teilraum von $\mathbb{R}^S$ bzw. $\mathbb{C}^S$, der genau diejenigen Funktionen $(x_s)_{s\in S}$ enthält, für die erstens $S' = \{s \in S \mid x_s \neq 0\}$ eine (endlich oder unendlich) abzählbare Menge ist und zweitens die Reihe $\sum_{s\in S'} |x_s|^2$ konvergiert oder endlich (inklusive leer) ist.[2] Speziell ist $\ell^2(\mathbb{N})$ formal identisch mit ℓ^2 und $\ell^2(S)$ genau dann normisomorph mit ℓ^2, wenn S abzählbar unendlich ist. Für endliche Mengen S ist $\ell^2(S)$ natürlich isomorph mit $\mathbb{R}^{|S|}$ bzw. $\mathbb{C}^{|S|}$.

Liegen schließlich zwei Indexmengen S_1 und S_2 vor, so sind die beiden Hilberträume $\ell^2(S_1)$ und $\ell^2(S_2)$ genau dann normisomorph, wenn $|S_1| = |S_2|$ gilt. Für jeden Hilbertraum $\mathcal{H}$ ist somit die *Hilbertdimension* wohldefiniert: Dieselbe ist $|S|$, wobei S irgendeine Menge ist, für die $\mathcal{H}$ isomorph zu $\ell^2(S)$ ist. Die Hilbertraumdimension ist von größerer Bedeutung als die Vektorraumdimension von $\mathcal{H}$. Dieselbe ist nämlich gleich der Kardinalzahl einer *Orthonormalbasis* $\mathcal{B}$ des Hilbertraums $\mathcal{H}$, also eines maximalen Systems von Vektoren der Länge 1, die paarweise orthogonal sind. (Jeder Vektor in $\mathcal{H}$ kann dann in eine Fourierreihe über die Basisvektoren in $\mathcal{B}$ entwickelt werden.)

Ein Hilbertraum ist genau dann von endlicher Hilbertdimension m, wenn er als Vektorraum von endlicher Dimension n ist. Trifft dies zu, so gilt automatisch $m = n$. Im Unendlichdimensionalen können die beiden Dimensionsbegriffe ebenfalls zusammenfallen und tun dies auch oft, wie der folgende Satz zeigt, der Satz 10 verallgemeinert:

Satz 11. *Ist $\mathcal{H}$ ein unendlichdimensionaler Hilbertraum, so gilt* $\dim \mathcal{H} = |\mathcal{H}| = \sigma^{\aleph_0}$*, wobei σ die Hilbertdimension von $\mathcal{H}$ ist.*

Bemerkung: Alle transfiniten Kardinalzahlen κ der Form $\kappa = 2^\lambda$ (wie z.B. $\kappa = c$) erfüllen die Gleichung $\kappa^{\aleph_0} = \kappa$. Satz 10 nimmt Bezug auf den Fall $\kappa = \aleph_0$, wo natürlich $\kappa^{\aleph_0} > \kappa$ gilt. Es gibt eine *Unmenge* transfiniter Kardinalzahlen κ mit $\kappa^{\aleph_0} > \kappa$, d.h. zu jeder Menge K von Kardinalzahlen gibt es eine Kardinalzahl $\kappa \notin K$ mit $\kappa^{\aleph_0} > \kappa$. Ist nämlich S die Vereinigung von Mengen S_n mit $|S_n| < |S_{n+1}|$ für alle $n \in \mathbb{N}$, so gilt $|S^{\mathbb{N}}| > |S|$. (Eine Abbildung $G : S \to S^{\mathbb{N}}$ kann nämlich nicht surjektiv sein, da $G(s) \neq g$ für alle $s \in S$ gilt, wenn man $g \in S^{\mathbb{N}}$ so definiert, dass für jedes $n \in \mathbb{N}$ der Funktionswert $g(n)$ in der wegen $|S_n| < |S_{n+1}|$ nichtleeren Menge $S_{n+1} \setminus \{G(s)(n) \mid s \in S_n\}$ gewählt wird.) Nach Satz 11 ist im Falle $|S|^{\aleph_0} > |S|$ die Hilbertdimension des Raums $\ell^2(S)$ *kleiner* als die Vektorraumdimension. Diese Diskrepanz hat eine wesentliche Konsequenz in Bezug auf Isomorphien. Hat man S mit $|S|^{\aleph_0} > |S|$ und setzt man $S' = S^{\mathbb{N}}$, so sind die beiden Räume $\ell(S)$ und $\ell(S')$ isomorph als Vektorräume, aber nicht als Hilberträume! Dies ist z.B. bei den beiden in der Funktionalanalysis wichtigsten Hilberträumen ℓ^2 und $\ell^2(\mathbb{R})$ der Fall.

[2] Die Reihenfolge der Summation ist irrelevant, da bei unendlich vielen Summanden entweder immer absolute Konvergenz mit eindeutigem Grenzwert oder immer Divergenz herrscht.

Einen wesentlichen Teil des Beweises von Satz 11 erledigt das

Lemma 2. *Für jede unendliche Menge S gilt* $|\ell^2(S)| = |S|^{\aleph_0}$.

Beweis. Im folgenden sei $\mathbb{K}$ entweder gleich $\mathbb{R}$ oder gleich $\mathbb{C}$. Wir definieren den Raum $E(S)$ als die Menge aller Vektoren $(x_s)_{s\in S}$ im Raum $\mathbb{K}^S$, wo $x_s \neq 0$ nur für höchstens abzählbar viele $s \in S$ gilt. Dann gilt $\ell^2(S) \subset E(S)$.

Für jedes $n \in \mathbb{N}$ definieren wir das offene Intervall $I[n] :=]0, \frac{1}{n+1}[$. Da die Reihe $\sum_{n=0}^{\infty} \frac{1}{(n+1)^2}$ natürlich konvergiert, liegt ein Vektor $(x_s)_{s\in S}$ des Raums $E(S)$ sicher dann in $\ell^2(S)$, wenn man eine abzählbare Menge $A \subset S$ samt einer Injektion g von A nach $\mathbb{N}$ finden kann, sodass einerseits $x_s \in I[g(s)]$ für alle $s \in A$, andererseits $x_s = 0$ für alle $s \notin A$ gilt. Die Kardinalzahl der Menge all dieser Vektoren $(x_s)_{s\in S}$ muss nun gleich $|E(S)|$ sein, da $|I[n]| = |\mathbb{K}|$ für alle $n \in \mathbb{N}$ gilt. Daher gilt $|\ell^2(S)| \geq |E(S)|$ und wegen $\ell^2(S) \subset E(S)$ gilt somit $|\ell^2(S)| = |E(S)|$.

Die Berechnung von $|E(S)|$ wiederum stellt ein simples kombinatorisches Problem dar. Wir betrachten beliebige abzählbare Teilmengen A von S, deren Elemente $a \in A$ Zahlen $x \neq 0$ in $\mathbb{K}$ als x_a indizieren. Man erhält $|E(S)|$, indem man die Anzahl $|\mathbb{K}^A|$ aller Abbildungen von A nach $\mathbb{K} \setminus \{0\}$ über alle abzählbaren Teilmengen A von S summiert. Für eine abzählbare Menge $A \neq \emptyset$ gilt prinzipiell $|\mathbb{K}^A| = c$. Die Familie $\mathcal{A}$ aller abzählbaren Teilmengen A von S hat die Kardinalzahl $|S|^{\aleph_0}$.[3] Ergo gilt

$$|E(S)| = c \cdot |S|^{\aleph_0} = \max\{c, |S|^{\aleph_0}\} = |S|^{\aleph_0}$$

und wir sind fertig. $\square$

Dabei ist wie üblich das Produkt von Kardinalzahlen via $|A| \cdot |B| := |A \times B|$ definiert. (Für transfinite Kardinalzahlen $\kappa \leq \lambda$ gilt immer $\kappa \cdot \lambda = \lambda$.) Summiert man Kardinalzahlen $|A_i|$ über alle i aus einer Indexmenge I, so erhält man als Summe die Kardinalzahl $\Sigma = |\bigcup\{A_i \times \{i\} \mid i \in I\}|$. Hat man $|A_i| = \kappa$ für alle $i \in I$, so gilt $\Sigma = \kappa \cdot |I|$.

Um nun Satz 11 zu beweisen, genügt es – im Lichte von Lemma 2 – zu zeigen, dass $\dim \ell^2(S) = |\ell^2(S)|$ für jede unendliche Menge S gilt. Wir unterscheiden die beiden Fälle $|\ell^2(S)| = c$ und $|\ell^2(S)| > c$. (Der Fall $|\ell^2(S)| < c$ kann nur im Trivialfall $S = \emptyset$ eintreten.) Grundsätzlich kann man den Raum ℓ^2 immer in den Raum $\ell^2(S)$ isomorph einbetten. Daher gilt immer $\dim \ell^2(S) \geq \dim \ell^2 = c$. Und trivialerweise gilt $\dim \ell^2(S) \leq |\ell^2(S)|$. Im Falle $|\ell^2(S)| = c$ gilt also sicher $\dim \ell^2(S) = |\ell^2(S)|$. Den Fall $|\ell^2(S)| > c$ erledigt nun schließlich der folgende Satz, dessen Beweis eine simple Adaptation des Beweises von Satz 5 ist.

[3] Trivialerweise gilt $|\mathcal{A}| \leq |S^{\mathbb{N}}| = |S|^{\aleph_0}$ und umgekehrt gilt $|S^{\mathbb{N}}| \leq |\mathcal{A}|$, da wegen $|S| = |\mathbb{N} \times S|$ die Familie $\mathcal{A}'$ aller abzählbaren Teilmengen von $\mathbb{N} \times S$ gleichmächtig mit $\mathcal{A}$ ist und via $f \mapsto \{(n, f(n)) \mid n \in \mathbb{N}\}$ offensichtlich eine injektive Abbildung von $S^{\mathbb{N}}$ in $\mathcal{A}'$ definiert wird.

Satz 12. *Ist $\mathcal{V}$ ein Vektorraum über einem unendlichen Körper $\mathbb{K}$ mit $|\mathcal{V}| > |\mathbb{K}|$, so gilt* $\dim \mathcal{V} = |\mathcal{V}|$. *Insbesondere ist die Dimension eines reellen oder komplexen Vektorraums stets identisch mit seiner Kardinalität, falls letztere größer als das Kontinuum ist.*

Zur Klärung, ob $\dim \mathcal{V} = |\mathcal{V}|$ im Falle $|\mathcal{V}| = |\mathbb{K}|$ gilt, kann folgende Verallgemeinerung von Satz 7 hilfreich sein.

Satz 13. *Ist $\mathcal{V}$ ein Vektorraum über einem beliebigen Körper $\mathbb{K}$, so gilt* $\dim \mathcal{V} = |\mathcal{V}|$ *jedenfalls dann, wenn man den Vektorraum $\mathbb{K}^{\mathbb{N}}$ in den Raum $\mathcal{V}$ isomorph einbetten kann.*

Beweis. Im Falle $\aleph_0 \leq |\mathbb{K}| < |\mathcal{V}|$ ist wegen Satz 12 nichts zu zeigen. Im Falle $|\mathbb{K}| = |\mathcal{V}|$ ist, da man $\mathbb{K}^{\mathbb{N}}$ in $\mathcal{V}$ einbetten kann, einerseits $\mathbb{K}$ unendlich, andererseits enthält $\mathcal{V}$ eine Kopie der Menge $\mathcal{U}$ in Satz 3, was sofort $|\mathbb{K}| \leq \dim \mathcal{V}$ und somit die Behauptung nach sich zieht. Ist schließlich $\mathbb{K}$ endlich, so kann der Beweis von Satz 5 mit der Substitution $\mathbb{K}^I \leftrightarrow \mathcal{V}$ wörtlich übernommen werden. □

Bemerkung: Den $\mathbb{K}^{\mathbb{N}}$ in $\mathcal{V}$ isomorph einbetten zu können, ist natürlich äquivalent dazu, dass $\dim \mathcal{V} \geq |\mathbb{K}|^{\aleph_0}$ gilt. Allerdings kann die Einbettbarkeit des $\mathbb{K}^{\mathbb{N}}$ leichter verifizierbar sein als die Ungleichung $\dim \mathcal{V} \geq |\mathbb{K}|^{\aleph_0}$ durch Angabe einer linear unabhängigen Menge $\mathcal{M} \subset \mathcal{V}$ mit $|\mathcal{M}| = |\mathbb{K}|^{\aleph_0}$.

Für reelle und komplexe Vektorräume gibt es folgende Alternative zu Satz 13:

Satz 14. *Ist $\mathcal{V}$ ein reeller bzw. komplexer Vektorraum, so gilt* $\dim \mathcal{V} = |\mathcal{V}|$ *jedenfalls dann, wenn man den Hilbertraum ℓ^2 als Vektorraum in den Vektorraum $\mathcal{V}$ (rein algebraisch) isomorph einbetten kann.*

Beweis. Im Falle $|\mathcal{V}| > c$ ist wegen Satz 12 nichts zu zeigen. Im Falle $|\mathcal{V}| = c$ gilt wegen der Einbettbarkeit von ℓ^2 in den Raum $\mathcal{V}$ automatisch $c = \dim \ell^2 \leq \dim \mathcal{V}$ und die Behauptung folgt. □

Mittels Satz 14 lässt sich nun auch sofort die Dimension der folgenden (reellen bzw. komplexen) Banachräume bestimmen. Es gilt $\dim \mathcal{B} = |\mathcal{B}| = c$ für:

(1) $\mathcal{B} =$ Raum aller beschränkten Zahlenfolgen $(\xi_n)_{n\in\mathbb{N}}$
(2) $\mathcal{B} =$ Raum aller konvergenten Zahlenfolgen $(\xi_n)_{n\in\mathbb{N}}$
(3) $\mathcal{B} =$ Raum aller Nullfolgen $(\xi_n)_{n\in\mathbb{N}}$
(4) $\mathcal{B} = \ell^p :=$ Raum aller Folgen $(\xi_n)_{n\in\mathbb{N}}$ mit $\sum_{n=0}^{\infty} |\xi_n|^p < \infty$ ($p \in [1, \infty[$ fest).

Bei (4), wo für $1 \leq p < 2$ nicht $\ell^2 \subset \ell^p$ gilt, beachte man, dass Satz 14 natürlich richtig bleibt, wenn man ℓ^2 durch ℓ^p mit beliebigem $p \geq 1$ ersetzt.

Ist für $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ und eine Indexmenge S der Banachraum $\mathcal{B}(S)$ als derjenige Teilraum von $\mathbb{K}^S$ definiert, der genau die beschränkten Funktionen $f : S \to \mathbb{K}$ enthält und mit der Supremumsnorm $\sup f := \sup\{f(s) \mid s \in S\}$ versehen ist, so gilt

Satz 15. *Für jede unendliche Menge S gilt* $\dim \mathcal{B}(S) = |\mathcal{B}(S)| = 2^{|S|}$.

Beweis. Wegen $\ell^2(S) \subset \mathcal{B}(S)$ kann man den Raum ℓ^2 algebraisch in $\mathcal{B}(S)$ einbetten. Im Lichte von Satz 14 genügt es also, $|\mathcal{B}(S)| = 2^{|S|}$ zu verifizieren. Dies ergibt sich aber sofort aus $[0,1]^S \subset \mathcal{B}(S) \subset \mathbb{K}^S$ und (vgl. Beweis von Satz 8) $c^{|S|} = 2^{|S|}$. □

Satz 16. *Für den mit der Maximumnorm versehenen reellen Banachraum $\mathcal{C}[a,b]$ aller reellwertigen stetigen Funktionen auf dem kompakten Intervall $[a,b] \subset \mathbb{R}$ ($a < b$) gilt* $\dim \mathcal{C}[a,b] = |\mathcal{C}[a,b]| = c$.

Beweis. O.B.d.A. sei $[a,b] = [0,1]$. Da wegen $|\mathbb{R}^{\mathbb{Q}\cap[0,1]}| = c$ natürlich $|\mathcal{C}[0,1]| = c$ gilt, genügt es, den ℓ^2 in $\mathcal{C}[0,1]$ einzubetten: Jedem $(x_n)_{n\in\mathbb{N}}$ in ℓ^2 ordnen wir diejenige Funktion g in $\mathcal{C}[0,1]$ zu, für die $g(\frac{1}{n+1}) = x_n$ für jedes $n \in \mathbb{N}$ sowie $g(0) = 0$ gilt und die auf jedem Intervall $[\frac{1}{n+2}, \frac{1}{n+1}]$ affin-linear ist. (Der Graph von g ist also ein Streckenzug, der die Punkte $\left(\frac{1}{n+1}, x_n\right)$, $n = 0, 1, 2, \ldots$ verbindet.) Damit ist offensichtlich ein Monomorphismus von ℓ^2 nach $\mathcal{C}[0,1]$ definiert. Den hier im Hintergrund leuchtenden Satz 3 kann man auch ins Rampenlicht stellen und direkt eine im Wesentlichen der Menge $\mathcal{U}_1$ im Beweis von Satz 10 entsprechende linear unabhängige Teilmenge $\mathcal{U}_1^*$ von $\mathcal{C}[0,1]$ mit $|\mathcal{U}_1^*| = c$ angeben: Man setzt

$$\mathcal{U}_1^* = \{f_a \in \mathcal{C}[0,1] \mid 0 < a < 1\},$$

wobei f_a in $\mathcal{U}_1^*$ via $f_a(x) = a^{1/x}$ für $0 < x \leq 1$ sowie $f_a(0) = 0$ definiert sind. □

Schlussbemerkung. Für einen beliebigen unendlichdimensionalen Hilbertraum sei σ seine Hilbertdimension (also die Kardinalzahl einer Orthonormalbasis) und δ seine gewöhnliche Dimension. In [3] findet man die Abschätzung $\delta \geq 2^{\aleph_0}$ und in [4] findet man die Gleichung $\delta^{\aleph_0} = \delta$. Beide Aussagen sind unmittelbare Folgerungen aus unserem Satz 11, nach dem stets $\sigma^{\aleph_0} = \delta$ gilt. In [4] findet man auch (für Banachräume formuliert) die Gleichung $\vartheta^{\aleph_0} = \delta$, wobei ϑ die kleinste Kardinalzahl einer dichten Menge ist, aus der wiederum $\sigma^{\aleph_0} = \delta$ folgt, da im Falle $\delta \geq \aleph_0$ natürlich $\vartheta = \sigma$ gilt. Theorem 1 in [2] besagt, dass entweder $\delta = \sigma$ oder $\delta = 2^{\sigma}$ gilt. Tatsächlich ist diese Aussage aber unbeweisbar. Die Autoren haben in ihrem „Beweis“ nämlich die allgemeine Kontinuumshypothese verwendet, die ihnen so selbstverständlich erschien, dass sie diese in der Formulierung des Satzes gar nicht erwähnen. Heutzutage erkennt man immer deutlicher die Unhaltbarkeit dieser höchst fragwürdigen Hypothese, vgl. auch [5]. (Unter der unwiderlegbaren und nicht abwegigen Annahme $\aleph_1 < 2^{\aleph_0} < 2^{\aleph_1}$ erweist sich Theorem 1 in [2] auch prompt als falsch. Im Lichte von Satz 11 ist dann nämlich $\sigma = \aleph_1$ wegen $\aleph_1^{\aleph_0} = 2^{\aleph_0}$ ein triviales Gegenbeispiel zu $\delta \in \{\sigma, 2^\sigma\}$.) Wie Satz 11 demonstriert, benötigt man keine unbeweisbaren, fragwürdigen Hypothesen, um eine schöne und einfache Relation zwischen den beiden Dimensionsbegriffen bei Hilberträumen zu formulieren. Schließlich sei noch erwähnt, dass unser Satz 7 auch in [1] bewiesen wird (1, Ch.II§7 Ex.3), dort allerdings wesentlich komplizierter, da die multiplikative Kommutativität des Grundkörpers nicht verwendet wird.

Literatur

[1] Bourbaki: *Algebra I*, Elements of Mathematics Series, 2nd printing, Springer 1989.

[2] Evans, J.W., and Tapia, R.A.: *Hamel versus Schauder dimension.* American. Math. Monthly **77**/4, 385–388 (1970).

[3] Halmos, P.R.: *A Hilbert Space Problem Book.* Springer 1974.

[4] Kruse, A.H.: *Badly incomplete normed linear spaces.* Math. Z. **83**, 314–320 (1964).

[5] Kuba, G.: *Wie plausibel ist die Kontinuumshypothese?* Elemente d. Math. **61**, 89–98 (2006).

Adresse des Autors: Gerald Kuba
Institut für Mathematik
Universität für Bodenkultur
1180 Wien

Internat. Math. Nachrichten
Nr. 212 (2009), 23–28

Was leistet der Mathematikunterricht in der Schule und was soll bzw. kann er leisten?

Reinhard Winkler
TU Wien

Einleitung Wer die Einschätzung vertritt, dass es um den Mathematikunterricht an Österreichs Schulen nicht zum Besten steht, braucht von Seiten der Mathematiker an den Universitäten wenig Widerspruch zu fürchten. Eine zu deutliche Sprache sprechen unzählige Erfahrungen wie auch Ergebnisse von Tests, die an verschiedenen Universitäten – meist aus Eigeninitiative der dort Lehrenden – im Laufe der Jahre durchgeführt worden sind. (Nicht ausgeklammert sei dabei, dass nicht nur das Schulsystem, sondern auch die Universitäten selbst durchaus Anlass zur Selbstkritik haben.) Entsprechend widmet sich die Didaktikkommission der ÖMG seit Jahren der Frage nach Verbesserungsmöglichkeiten. Vor allem seit die internationale PISA-Studie darauf aufmerksam macht, dass Österreichs Schulsystem möglicherweise doch nicht das beste der Welt ist – also erst seit relativ kurzer Zeit –, wird auch in einer breiten Öffentlichkeit über mögliche, ja nötige Reformen diskutiert.

Vieles deutet darauf hin, dass in nächster Zeit sehr langfristige und nachhaltige Weichenstellungen zu erwarten sind (Schlagwort Zentralmatura). Deshalb hat die Didaktikkommission ihre Anstrengungen verstärkt, auch die Sicht der Fachwissenschaft und Fachdidaktik in den Diskurs einzubringen.

So wurde bei der gemeinsamen Tagung von ÖMG und DMV in Graz im Rahmen der Sektion „Didaktik und Popularisierung“ am 24.9.2009 eine Podiumsdiskussion veranstaltet. Universitätslehrer, die unterschiedliche Studienrichtungen mit mehr oder weniger unmittelbarem Mathematikbezug vertreten, waren eingeladen, sich mit Impulsreferaten einzubringen. Rudolf Freund (TU Wien, Informatik, Studiendekan), Gabriel Maresch (TU Wien, Mathematiker mit Lehrerfahrungen insbesondere aus den Studienrichtungen Maschinenbau und Bauingenieurwesen so-

ISSN 0020-7926

wie aus einem FH-Studiengang Angewandte Elektronik) und Bernhard Raschauer (Universität Wien, Professor am Institut für Staats- und Verwaltungsrecht der Juridischen Fakultät) konnten persönlich teilnehmen. Darüber hinaus stand schriftliches Material zur Verfügung, das ebenfalls in die Diskussion einfloss: von Marcel Widi (Mathematiker, bildet an der JKU Linz Studierende der Wirtschaftswissenschaften aus; außerdem FH Wels), von Gerhard Clemenz (Ökonomieprofessor an der Universität Wien) und die Dokumentation von Tests, die von Mathematikern an der Universität für Bodenkultur durchgeführt worden sind. Diese breite Streuung sollte der Rolle der Mathematik als eines allgemeinbildenden Fachs, dessen Wirkung weit über unmittelbare technisch-naturwissenschaftliche Anwendungen hinausreicht, Rechnung tragen. Moderiert wurde die Veranstaltung vom bisherigen Vorsitzenden der Didaktikkommission, Wolfgang Schlöglmann (Johannes Kepler-Universität Linz).

Als Ausgangspunkt der Diskussion waren die Referenten eingeladen, zu einigen der folgenden Fragen Stellung zu beziehen:

- Welche spezifischen Anforderungen im Bezug auf Mathematik bestehen zu Studienbeginn? Welche Inhalte benötigen Ihre Studierenden? Welche Algorithmen, Techniken, etc. erwarten Sie zu Studienbeginn?
- Welche Defizite im Bezug auf Inhalte, Operieren, Erfassen von Inhalten, Argumentieren, etc. haben Sie bei Ihren Studierenden festgestellt? Haben Sie den Eindruck, dass dabei der Schultyp eine wichtige Rolle spielt?
- Österreich plant, eine zentrale schriftliche Reifeprüfung einzuführen. Was sollte aus Ihrer Sicht im Rahmen dieser Reifeprüfung geprüft werden? Könnten Sie dies eventuell anhand einer konkreten Aufgabenstellung verdeutlichen?
- Was bedeutet aus Ihrer Sicht mathematische Bildung?

Trotz einiger Besonderheiten, welche den unterschiedlichen Erfahrungshintergrund der Diskussionsteilnehmer – Referenten wie Publikum – reflektieren, und trotz einiger Auffassungsunterschiede in manchen Einzelfragen wurde zu einigen wichtigen Aspekten ein breiter Konsens deutlich. Nicht durch protokollartige oder gar vollständige Wiedergabe der Diskussion, sondern durch Nachzeichnung der wichtigsten Themen will ich versuchen, vor allem die auffälligsten Übereinstimmungen zusammenzufassen. Doch auch die (wenigen) kontroversiellen Themen sollen angesprochen werden. Eine Weiterentwicklung derselben durch feinere Differenzierung ließe durchaus auf Fortschritte des Diskurses und Klärung einiger Fragen hoffen.

Zahlreiche interessante Beiträge auch aus dem Publikum kann ich, um den Rahmen dieses Berichts nicht zu sprengen, hier nicht angemessen würdigen. Auch bin ich nicht in der Lage, alle Autorinnen und Autoren solcher Beiträge namentlich zu erwähnen. Deshalb werde ich dies generell unterlassen, auch wo ich die Namen kenne, und bitte dafür um Verständnis.

1. Hauptmotiv: Mathematik und Sprache Die vielleicht auffälligste Gemeinsamkeit vieler Beiträge war die Betonung der vielfältigen Beziehungen zwischen Mathematik und Sprache. Aus Sicht der Informatik (Freund) z.B. ist die Fähigkeit zur Formalisierung, d.h. die Übertragung von Text in natürlicher in formale Sprache, von essenzieller Bedeutung. Dabei geht es keinesfalls darum, Symbolsprachen um ihrer selbst willen zu pflegen. Wichtiger ist der Brückenschlag von zunächst vielleicht mehrdeutigen Formulierungen, wie sie für die Alltagssprache typisch sind, zu ihren mathematisch korrekten und eindeutigen, oft formalisierten Übertragungen. Programmspezifikation für Softwareentwicklung ist ein typisches Beispiel, wo solche Fähigkeiten gefragt sind, die aus der Schule aber leider kaum mitgebracht werden.

Besonders bei der Ausbildung im Rahmen klassischer Ingenieursstudien falle eine „Sprachlosigkeit im Angesicht der Mathematik“ auf, wie es Maresch formulierte. Typisch sei, dass Studierende sehr wohl vernünftige mathematische Vorstellungen entwickeln, sehr häufig aber an der sprachlichen Umsetzung scheitern.

In der Rechtswissenschaft wird die große Bedeutung der Sprachkompetenz wenig überraschen. Raschauer brachte es auf den Punkt, indem er – einen Kollegen zitierend – als Testfragen für die Eignung zu einem Jusstudium vorschlug: „Wie warst du in Deutsch? Könntest du zu jedem beliebigen Thema 20 Seiten schreiben?“ Dabei – und hier wird die Relevanz für den Mathematikunterricht deutlich – komme es aber weniger auf Wörter an als auf Begriffe, jene gedanklichen Kategorien, mit denen wir die Welt ordnen. Begriffe müssen erarbeitet werden in einem Denken, das auch unerwartete Alternativen erlaubt. Der Jurist habe zwar große Freiheiten. Er müsse aber stets gute Argumente vorbringen, warum er eine bestimmte Position vertrete und keine andere. Sprachkompetente Argumentation wäre also aus juridischer Sicht eine sehr sinnvolle Zielvorgabe für den Mathematikunterricht, insbesondere wenn er über einen engen technischen Horizont hinaus wertvoll sein will.

Auch zahlreiche Meldungen aus dem Publikum griffen das Thema Sprache auf und ergänzten das Gesagte um weitere Aspekte, wobei teils auch interessante Unterschiede zwischen Sprachkompetenz aus mathematischer und juridischer Sicht zutage traten. Doch zurück zu den Gemeinsamkeiten.

2. Hauptmotiv: Syntax versus Semantik Bereits erwähnt habe ich das von Raschauer proklamierte Primat der Begriffe gegenüber den Wörtern. Eine mathematische Entsprechung dazu findet sich im Verhältnis von Semantik und Syntax, wie es in der mathematischen Logik im Zentrum des Interesses steht. Hierbei wird deutlich, dass jeder mathematische Begriff zunächst inhaltlich verstanden und möglichst in natürlicher Sprache gefasst werden muss, bevor eine Formalisierung am Platze ist. Maresch wies darauf hin, wie wichtig es sei, z.B. mit logischen Quantoren inhaltlich operieren zu können. Nicht zu sehr dürfe man sich von syntaktischen Gewohnheiten leiten lassen und den Symbolen falsche Autorität zugestehen. Legion sind die Beispiele kurioser Fehler im Hochschulalltag, die bei rein symbolischer Formelmanipulation vorkommen, sofern das Verständnis für die mathematische Bedeutung abgeht. Das Klischee des Mathematikers vor einer Tafel mit kryptischen Zeichen befördere das sehr problematische Missverständnis von der Mathematik als Herrschaftsbereich der Symbole, anstatt sich für das zu interessieren, was mit diesen Symbolen *bezeichnet* wird. Raschauer erwähnte in analogem Zusammenhang Platons Höhlengleichnis, wo die Realität (Semantik = mathematische Objekte, primär) in Kontrast gesetzt wird zu den Schatten (Syntax = mathematische Symbolik, sekundär), die diese Realität wirft.

Die Überbetonung von formaler Symbolsprache wird also sehr kritisch gesehen. Gefordert wird dagegen die Schulung des Abstraktionsvermögens. Es lohnt, sich die Unterschiede zwischen diesen beiden Phänomenen zu verdeutlichen.

3. Hauptmotiv: Abstraktion Aus Sicht der Didaktik besteht kaum ein Zweifel darin, dass mathematisches Verständnis nicht beim abstrakten Begriff beginnen kann, sondern zunächst der Anschauung des Konkreten bedarf. Je jünger die Kinder, desto offensichtlicher ist diese Tatsache. Ebenso unumstritten ist jedoch, dass Abstraktion ein Charakteristikum der Mathematik als Wissenschaft ist. Die Podiumsdiskussion zeigte, dass die innermathematische Rolle der Abstraktion aber nicht der einzige Grund ist, sich ihrer auch in der Schule anzunehmen, wenigstens anhand geeigneter Beispiele. Ziel sollte die Erfahrung sein, wie sehr der Weg der Abstraktion vom Konkreten hin zum Allgemeinen und Umfassenden ein wesentliches Element des Denkens ist; auch in vielen anderen Bereichen menschlicher Geistestätigkeit außerhalb der Mathematik.

Entsprechend führten alle drei Referenten die Bereitschaft und das Vermögen zur Abstraktion als zentrales Bildungsziel an. Maresch wies darauf hin, dass es dabei um die universell maßgebliche Fähigkeit gehe, zwischen Wesentlichem und Unwesentlichem zu unterscheiden. Und diese Fähigkeit sei nicht ausschließlich Begabungssache, sondern könne durchaus auch in der Schule gefördert werden. Raschauer entwickelte das Thema noch weiter, indem er die Denkkategorien Subsumption, Distinktion und Relation unterschied, durchaus in enger Verbindung mit dem bereits erwähnten begrifflichen Denken.

4. Hauptmotiv: Rezepte versus Konzepte Jeder Universitätslehrer weiß: Vielen Studierenden fallen Rezepte leichter als Konzepte. Es verwundert nicht, dass alle Referenten dieses Phänomen als unerwünscht ansahen. Freund berichtete von einem Studenten, der allen Ernstes ein allgemeingültiges Rezept verlangte, wie man Computerprogramme schreibt. In den klassischen Ingenieursfächern äußere sich eine ähnliche Mentalität oft in einer beachtlichen Bereitschaft für schematisches Rechnen, das laut Maresch aber meist mit einer Beschränkung auf sehr enge Methoden einhergehe. Mutatis mutandis finden sich Analogien auch in Raschauers Ausführungen. Er berichtete aus seiner eigenen Studienzeit. Einige Zeit trug er sich mit dem Gedanken, selbst Mathematik zu studieren. So lag es für ihn, nachdem er sich doch für Jus entschieden hatte, nicht fern, sich mit der algorithmischen Beschreibung juridischer Entscheidungsprozesse zu beschäftigen. Schließlich kam er aber zur Einsicht, dass dadurch nicht viel gewonnen werden könne. Denn juridische Regeln seien nicht starr und müssen fortlaufend weiterentwickelt werden. Auch sei der Gesetzestext unwichtig im Vergleich zu jenen Prozessen, die juridisches Denken im Kern ausmachen. Es sind also gerade nicht die schematisierbaren Aspekte der Mathematik, wo ihr Wert für die Jurisprudenz zu suchen sei, sondern die Schulung des konzeptuell-begrifflichen Denkens, von dem schon die Rede war.

Sehr lebendig war der Meinungsaustausch über die Wichtigkeit des Rechnens bzw. Kopfrechnens. Freund und Widi z.B. kritisieren, dass die Mathematik in der Schule meist zu einem bloßen Rechnen verkomme. Maresch betonte, dass die Beherrschung von Rechenregeln zwar wünschenswert sei, nicht aber entscheidend für den Studienerfolg. Generell könne die Vermittlung technischer Fähigkeiten weitgehend einem Fachstudium überlassen bleiben (Clemenz). In diesem Zusammenhang seien auch Wortmeldungen erwähnt, die einen Niedergang der Rechenfähigkeiten im Laufe der letzten Jahrzehnte beklagten, und solche, die den Wert des Kopfrechnens priesen.

Mir scheint dazu folgende Unterscheidung sinnvoll: Kopfrechnen zwecks Entwicklung des Vorstellungsvermögens und die Fähigkeit, mit Quantitäten zu operieren, ist besonders für Kinder am Anfang ihrer mathematischen Entwicklung eine unerlässliche geistige Erfahrung. Viel hat später darauf aufzubauen. Rechnen hingegen als Virtuosität in der Manipulation mathematischer Symbole (siehe auch weiter oben unter „Syntax versus Semantik“) ist, insofern sie über die Beherrschung der elementaren Grundrechenarten hinausgeht, nur von lokalem Nutzen für den jeweiligen Kontext. Nie jedoch kann sie Selbstzweck und Hauptziel des Mathematikunterrichts sein. Jedenfalls vermittelt werden muss die grundsätzliche Einsicht, dass Formalisierung möglich und nützlich, weil der automatisierten Verarbeitung durch den Computer zugänglich ist.

5. Hauptmotiv: Technologieeinsatz Widi z.B. sieht im ubiquitären Einsatz des Taschenrechners eine Gefahr, welche die elementare Fähigkeit des Kopfrechnens oder auch die schriftlich-algorithmische Beherrschung einfachster Rechenoperationen untergräbt. Er empfiehlt, den Taschenrechner im Schulunterricht überhaupt abzuschaffen und gleich vernünftige Computeralgebrasysteme einzusetzen. Für Letzteres sprechen auch Untersuchungen, wonach Schulklassen, die den Computer regelmäßig verwenden, bei Tests besser abschneiden als Klassen ohne Erfahrung damit. Bemerkenswerterweise, so wurde berichtet, beziehe sich das auch auf computerunabhängige Fähigkeiten. Zieht man auch Stellungnahmen von Skeptikern des Computereinsatzes in Betracht, so lässt sich auf allgemeiner Ebene ein

Konsens wahrscheinlich in der Einschätzung finden, dass Computereinsatz sowohl Chancen als auch Gefahren berge und daher besondere Sorgfalt verdiene.

Resümee und Ziele, auch für eine standardisierte („zentrale") Reifeprüfung

Abschließend will ich auszugsweise noch einige allgemeine Ziele erwähnen, die sich nicht speziell auf eines der fünf ausgeführten Hauptmotive beziehen, die aber in der Diskussion zur Sprache kamen.

Freund betonte, dass Mathematik ihrem Wesen nach ein aufbauendes Fach sei. Deshalb sei im Unterricht Nachhaltigkeit von ganz besonderer Wichtigkeit. Ein Grund für die gegenwärtig unbefriedigende Situation sei die zu große Anzahl von Prüfungen, in der Schule wie an der Universität. Laut Maresch solle keineswegs Perfektion das Ziel sein, sondern die Bereitschaft, sich auf mathematisches Denken einzulassen. Hierfür sei es wichtig, wenigstens an einfachen Beispielen zu vermitteln, dass mathematische Einsichten jedem möglich sind und ein Gefühl der Autonomie und Sicherheit im eigenständigen Denken geben. In eine ähnliche Richtung ging eine andere Wortmeldung, wonach man im Unterricht Fehler zulassen müsse, auch um das Selbstvertrauen zu stärken. Dies wäre sicher auch einem anderen wichtigen Ziel (Clemenz) dienlich, nämlich die leider sehr häufig zu beobachtende Schwellenangst gegenüber der Mathematik abzubauen. Mathematik müsse, so eine andere Wortwahl in ähnlichem Zusammenhang, als Denktechnologie verfügbar gemacht werden.

Die Einschätzungen, wie weit diese Ziele durch bevorstehende Reformen, insbesondere durch die Einführung der standardisierten Reifeprüfung erreicht werden können, variierten erwartungsgemäß. Einerseits war Zuversicht zu vernehmen, dass zurzeit ein Paradigmenwechsel stattfinde, der mit dem Schlagwort des kompetenzorientierten Unterrichts verbunden sei. Für die Umsetzung sinnvoller Reformen seien unbedingt zentrale Vorgaben notwendig. Nur dann gebe es Chancen für Verbesserungen. Insbesondere scheint die neue Reifeprüfung mehrheitlich als taugliches Instrument eingestuft zu werden, um mehr Aussagekraft und gewisse verbindliche Mindeststandards zu garantieren. Es gab aber auch skeptische Stimmen, die eine teilzentrale Lösung bevorzugen, wo den einzelnen Schulen und Lehrkräften ein gewisser Spielraum zur autonomen Gestaltung gelassen wird. Nur zwei Mathematikstunden wöchentlich, wie es in gewissen Schultypen vorkomme, sei aber sicher zu wenig, um einen vernünftigen einheitlichen Standard zu erreichen. Hier sollte die Schulautonomie Grenzen haben.

Anzustreben sei jedenfalls ein engerer Kontakt zwischen Schulen und Universitäten. Beide Seiten können, wie Freund abschließend meinte, sicher einiges voneinander lernen.

Adresse des Authors: Reinhard Winkler, TU Wien, Wiedner Hauptstraße 8–10/104, 1040 Wien

Internat. Math. Nachrichten
Nr. 212 (2009), 29–32

40 Jahre Mathematikolympiade

Michael Drmota
TU Wien

Bei einem Festakt zum 40jährigen Bestehen der Österreichischen Mathematikolympiade (ÖMO) am 12.6.2009, der gleichzeitig mit der Preisverleihung zum Bundeswettbewerb stattgefunden hat, hielt Michael Drmota (TU Wien) die folgende Ansprache.

Sehr geehrter Herr Regierungsrat, liebe Kolleginnen und Kollegen, liebe ehemalige und jetzige Preisträgerinnen und Preisträger!

Zunächst möchte ich mich ganz herzlich für die Einladung bedanken, bei dieser Gelegenheit ein paar Worte zu sprechen. Ich habe diese Einladung gerne angenommen, und es ist mir eine Freude und Ehre, hier zu sein.

Ich möchte mich zunächst kurz vorstellen. Ich bin Mathematiker an der TU Wien und stehe dem Institut für Diskrete Mathematik und Geometrie vor. Ich bin derzeit auch stellvertretender Vorsitzender der ÖMG. Ich bin mit der Mathematikolympiade mehrfach in Berührung gekommen, zunächst als Schüler ab der 7. Klasse – das ist schon einige Jahre her –, wo ich dann im anschließenden Maturajahr auch am Österreichisch-Polnischen Mathematikwettbewerb (ÖPMW) teilnehmen durfte. Einige Jahre später wurde ich Assistent bei Prof. Baron; damit war ich zwar nicht direkt in die Mathematikolympiade involviert, aber doch hautnah am Geschehen. Der Kreis hat sich in den letzten Jahren durch meine Tätigkeit im Vorstand der ÖMG wieder geschlossen, wo die Zusammenarbeit mit der Österreichischen Mathematikolympiade (ÖMO) intensiviert wurde und ich für diese Agenden zuständig wurde.

Nun zurück zum eigentlichen Thema, zum Geburtstagskind, der ÖMO. 40 Jahre sind schon eine beachtliche Zeit und es ließe sich hier sehr viel berichten. Ich möchte hier nur an einige besondere Ereignisse erinnern. Besonders erwähnenswert sind die Anfänge und untrennbar damit verbunden die Gründungsväter der ÖMO.

Ich gehe aber historisch noch einen Schritt zurück. Soviel ich weiß, fand die erste regionale Mathematikolympiade, die als solche bezeichnet wurde, 1934 in Leningrad statt. Diese Form der Wettbewerbe breitete sich rasch auf andere Städte, vor allem in der UdSSR, aus. Nationale Olympiaden gab es ab 1949, beginnend

ISSN 0020-7926

mit Polen. Die erste Internationale Mathematische Olympiade (IMO) fand dann 1959 in Rumänien statt. Daran nahmen 7 Länder teil, allerdings ausschließlich osteuropäische Staaten. Doch bereits nach wenigen Jahren wurden auch westliche Länder eingeladen, an den IMOs teilzunehmen, insbesondere auch Österreich, das 1968 nach Moskau eingeladen wurde. Von österreichischer Seite wurde zunächst nur ein Beobachter, der damalige Landesschulinspektor Alexander, entsandt, und nach seinem Bericht zeigte sich, dass es notwendig war, falls österreichische Schüler an der IMO teilnehmen sollten, eine zusätzliche Ausbildung anzubieten. Das war der Startschuss zur ÖMO. Es wurden unter der Federführung des damaligen MRs Szirucsek im Jahr 1969 30 Vorbereitungskurse eingerichtet. Kursleiter waren u.a. Gerd Baron, Wilhelm Körperth, Walter Kranzer und Herbert Vohla in Wien und Wolfgang Ratzinger, Franz Thannhausser und Erich und Gerhard Windischbacher in den Bundesländern. Nach diesen Vorbereitungen konnten im Jahr 1970 eine Schülerin und sieben Schüler zur 12. IMO nach Ungarn geschickt werden; Johann Hackl errang dabei übrigens eine Bronzemedaille. Schon damals war Thomas Mühlgassner Delegationsleiter, der diese Funktion bis vor drei oder vier Jahren ohne Unterbrechung innehatte. Wie gesagt, damit begann alles, die ÖMO besteht bis heute mit all ihren Strukturen: Anfänger- und Fortgeschrittenenkurse, die verschiedenen regionalen Wettbewerbe, der Vorbereitungskurs in Raach, der Bundeswettbewerb, aber auch Kursleiterfortbildungsseminare. An dieser Stelle möchte ich pars pro toto eine Person namentlich erwähnen, die mit der Entwicklung der ÖMO untrennbar verbunden ist, Prof. Gerd Baron. Er ist nicht nur einer der Gründungsväter, er hat sie in unermüdlicher Arbeit bis heute in einer Fülle von Funktionen wissenschaftlich und organisatorisch betreut. Es würde die Zeit, die mir hier zur Verfügung steht, bei Weitem sprengen, all seine Tätigkeiten aufzuzählen. Nicht unerwähnt lassen möchte ich aber seine Tätigkeit als Vorsitzender der Jury der 18. IMO, die 1976 in Österreich und damit erstmals außerhalb des Ostblocks stattfand, und den ÖPMW, der von 1977 bis 2006 von ihm als österr. Delegationsleiter geführt wurde. Dieser Wettbewerb hat in der neu gegründeten MEMO seine Fortsetzung gefunden, wo neben Österreich und Polen noch einige andere – mitteleuropäische – Länder teilnehmen. Wie gesagt, 40 Jahre sind eine beachtliche Zeit. Und es ist auch angebracht, darüber nachzudenken, wozu es mathematische Wettbewerbe und insbesondere die Mathematikolympiade gibt? Ist sie denn noch zeitgemäß?

Es gibt natürlich auch Kritik. Ist es richtig, Schüler frühzeitig mit abstrakter Materie zu konfrontieren, sie auch einseitig zu belasten? Soviel ich weiß, findet die Mathematikolympiade nicht an allen Schulen und nicht von allen Lehrern uneingeschränkte Unterstützung. Wie dem auch sei, aus meiner Sicht und meiner Erfahrung überwiegen die positiven Effekte bei Weitem. Selbstverständlich wird es da oder dort Verbesserungsmöglichkeiten geben. Aber mein Credo ist ein deutliches Ja zur Mathematikolympiade, und dafür gibt es meiner Meinung wirklich gute Gründe. Zunächst ist es meine Beobachtung, dass Tiefe und Breite einander nicht ausschließen. Gute Mathematiker haben oft eine Vielzahl von Begabungen: etwa Sprachen, Musik, Organisationstalent u.v.a. mehr. Auch sehe ich keinen Nachteil darin, abstrakt denken zu können.

Die Mathematikolympiade ist ohne Zweifel Begabtenförderung auf hohem Niveau und ist m.E. sicherlich zeitgemäß. Die Vorbereitungskurse bieten interessierten Schülern die Möglichkeit, sich in das Fach zu vertiefen und sind eine Schule des kreativen als auch des logisch strukturierten Denkens. Außerdem sind die Wettbewerbe zusätzlicher Ansporn und Motivation. In den letzten Jahren hat sich neben der Mathematikolympiade auch der sogenannte Kängurutest etabliert, der sich nicht nur an speziell interessierte Schüler wendet, sondern an dem flächendeckend alle Schüler teilnehmen. Ich empfinde diesen Wettbewerb als gute Ergänzung zur Mathematikolympiade; ich sage das auch aus der Erfahrung, die meine Kinder damit in der Schule haben. Er weckt auf breiter Basis Interesse für das Fach, aber auch für das logische und konzentriere Problemlösen. Etwas salopp formuliert könnte man sagen, der Kängurutest entspricht dem Breitensport und die Mathematikolympiade dem Spitzensport. Beide ergänzen einander.

Ich möchte nicht unerwähnt lassen, dass die Mathematikolympiade in ihrer Geschichte auch eine Vorreiterrolle gespielt hat. Erst später haben sich entsprechende Wettbewerbe für Physik, Chemie oder Latein etabliert.

Schließlich hat die Mathematikolympiade noch eine weitere Funktion, die mir als Universitätsmathematiker ganz besonders am Herzen liegt: Sie ist zweifellos eine Talenteschmiede. Außerordentlich viele österreichische Mathematiker, die national oder international tätig sind, sind durch die Schule der ÖMO gegangen, haben durch die Begegnung mit der ÖMO ihr Interesse für Mathematik geweckt bekommen, und ihre Studien- und Berufswahl wurde damit entsprechend beeinflusst. Ich möchte vielleicht wieder pars pro toto einen Namen herausgreifen: Christian Krattenthaler, Mathematiker an der Universität Wien und Wittgensteinpreisträger 2007 war – ich möchte fast sagen selbstverständlich – bei der ÖMO und auch bei der IMO. Nebenbei ist er ausgebildeter Konzertpianist und – was nicht alle wissen – ein hervorragender Fußballer. Noch einmal, Tiefe und Breite schließen einander nicht aus. Es ist natürlich nicht nur in Österreich so, dass die Mathematikolympiade hervorragende Wissenschaftler hervorbringt. Beispielsweise war Terence Tao Preisträger bei der IMO. Manche bezeichnen Tao als Mozart der Mathematik. Er ist jetzt knapp über 30 und hat bereits jetzt bahnbrechende Arbeiten in verschiedenen Mathematikdisziplinen geschrieben, z.B. in der Zahlentheorie und in der Theorie partieller Differentialgleichungen. Er wurde auch mit der Fields-Medaille ausgezeichnet, dem ranghöchsten mathematischen Preis.

Ich habe gerade versucht, eine Brücke zwischen Schulmathematik einerseits und Universitätsmathematik und wissenschaftlicher Forschung andererseits zu schlagen. Das ist für mich ein ganz wesentlicher Aspekt. Trotzdem muss man auch hier zu unterscheiden wissen und klar sagen, dass die Mathematikolympiade nicht die Funktion hat, ein Universitätsstudium vorwegzunehmen. Sie ist meines Erachtens eine wirklich wichtige Ergänzung der Schulmathematik. Alle Beispielaufgaben benötigen zum Verständnis und zur Lösung „nur“ schulmathematische Grundlagen. Im Universitätsstudium und insbesondere in der wissenschaftlichen Forschung kommen weitere inhaltliche Dimensionen, aber auch Handlungsdimensionen dazu. Mathematik benötigt das Lösen konkreter Probleme, ist aber noch viel mehr. Die Entwicklung der Mathematik ist ein Wechselspiel aus Fragestellungen der äußeren Welt wie z.B. der Physik, der Technik oder der Computerwissenschaften und dem Entwickeln mathematischer Theorien und Strukturen. So nebenbei gesagt: Es lohnt sich sehr, sich in diese Welt zu vertiefen, es ist wirklich bereichernd, in allen Ebenen. Das geht aber weit über das hinaus, was bei der Mathematikolympiade vermittelt werden kann. Trotzdem ist die Beschäftigung mit Mathematikolympiade-Beispielen eine hervorragende Grundlage für das, was dann noch kommen kann. Und sie bietet vor allem auch eines – und ich hoffe, ich habe das auch ein wenig vermitteln können – die Freude an der Betätigung mit Mathematik.

Ich persönlich habe der ÖMO einiges zu verdanken. Es war für mich eine große Bereicherung, in meiner Schulzeit daran teilnehmen zu können. Diese Erfahrungen, die ich damals sammeln konnte, waren für meine Studien- und Berufswahl entscheidend. Ich möchte hier aufrichtig „Danke“ sagen und damit gleichzeitig der Hoffnung Ausdruck geben, dass die ÖMO noch viele Jahre in Österreich bestehen wird; ich bin hier auch sehr zuversichtlich. Ich weiß, wie viele sich mit großem Einsatz dieser Sache widmen. Bitte bleiben Sie dabei!

Ich wünsche der ÖMO weiterhin alles Gute!

Adresse des Autors:
Michael Drmota
Technische Universität Wien
Wiedner Hauptstraße 8–10/104
1040 Wien

Buchbesprechungen

Featured Reviews

Allgemeines und Geschichte

Algebra und Diskrete Mathematik

Zahlentheorie

Geometrie, Topologie

Reelle und Komplexe Analysis

Angewandte und numerische Mathematik

P. Flajolet, R. Sedgewick: Analytic Combinatorics. Cambridge University Press, 2009, xiii+810 S. ISBN 978-0-521-89806-5 H/b £ 45,–.

Dieses ebenso umfangreiche wie informative Handbuch wird das Gebiet nachhaltig prägen, beziehungsweise hat es schon in seiner langen Entstehung geprägt. Lassen wir die Autoren selbst sprechen, aus dem Vorwort:

Analytic combinatorics starts from an exact enumerative description of combinatorial structures by means of generating functions: these make their first appearance as purely formal algebraic objects. Next, generating functions are interpreted as analytic objects, that is, as mappings of the complex plane into itself. Singularities determine a function's coefficients in asymptotic form and lead to precise estimates for counting sequences. The chain of reasoning applies to a large number of problems of discrete mathematics relative to words, compositions, partitions, trees, permutations, graphs, mappings, planar configurations, and so on. A suitable adaptation of the methods also opens the way to the quantitative analysis of charactersitic parameters of large random structures, via a perturbational approach.

Die Autoren waren an der Entstehung der analytischen Kombinatorik als eigenem Gebiet maßgeblich beteiligt. Man kann Flajolet als ihren „Gründervater" betrachten – natürlich in Kooperation mit anderen bedeutenden Mathematikern wie z.B. Odlyzko oder eben Sedgewick.

In Österreich konnte die Flajoletsche Schule, eingebettet in die Mathematik ebenso wie in die Theoretischen Computerwissenschaften, schon frühzeitig eigenständig Fuß fassen. Dies ist dem Wirkens von Helmut Prodinger zu verdanken, selbst vielfacher Koauthor von Flajolet und seinerseits Begründer einer österreichischen Schule der analytischen Kombinatorik, der sich hier auch weitere hervorragende Mathematiker angeschlossen haben. Lassen wir daher Helmut Prodinger persönlich zu Wort kommen, um die Darstellung des Werkes von Flajolet und Sedgewick zu komplettieren.

Wolfgang Woess (Graz)

P. Flajolet, R. Sedgewick: Analytic Combinatorics. Cambridge University Press, 2009, xiii+810 S. ISBN 978-0-521-89806-5 H/b £ 45,–.

Ich hatte das Privileg, die Entwicklung dieses Buches seit ca. 1992 persönlich mitzuverfolgen. Der ursprüngliche Plan war ein zweibändiges Werk; der erste Teil, *An Introduction to the Analysis of Algorithms*, ist tatsächlich 1995/6 erschienen. Der zweite Teil wäre dann dieser Text geworden, also keine Einführung, sondern eine Darstellung, die vor anspruchsvoller Mathematik nicht zurückschreckt. Im

Laufe der Entwicklung hat sich das Material immer mehr von den zu analysierenden Algorithmen verselbständigt; die dazu nötige Mathematik – Analytic Combinatorics – trat ganz in den Vordergrund. Mit dieser Neuorientierung und dem neuen Namen wurde auch der Verlag gewechselt.

Die einzelnen Kapitel wurden seit ca. 1992 als INRIA research reports publiziert. Seit dem großen Aufschwung des Internet wurden sie somit der ganzen Welt problemlos zugänglich. Es gab ein Kapitel über Anwendungen der Mellin-Transformation, das etwa 100 Seiten umfasste; es wurde letztlich (leider!) nicht aufgenommen und auf einen ganz kurzen Anhang reduziert. Diese INRIA reports wurden auch vielfach zitiert, und so kam es, dass dieses Buch, noch bevor es überhaupt existierte, sehr populär und vielfach erwähnt war. Die endgültige Fertigstellung hat sich ziemlich verzögert. Wir sind alle froh, dass es schließlich doch abgeschlossen wurde.

Autor Philippe Flajolet, der auch international als der Vater der Richtung „Analytische Kombinatorik" angesehen wird, wurde durch das Buch *Advanced Combinatorics* von L. Comtet beinflusst, auch hier einen Stil zu wählen, der sich an Beispielen orientiert. Das macht die Lektüre zum Vergnügen: man lernt doch, was man lernen soll, und wenn man ein bisschen etwas überschlägt, ist es auch nicht so schlimm.

Viel Material liegt hier vor, das von Philippe Flajolet (und seiner Schule) erst entwickelt wurde. Es gibt auch andere Ansätze, die Kombinatorik in symbolischer Weise zu erfassen. Der hier gewählte besticht sicher durch Durchsichtigkeit und Effizienz, insbesondere, was die Implementierung durch Computeralgorithmen (symbolic computation) betrifft. Mehr noch trifft das zu auf die analytischen Kapitel. Hier hat das Buch nun wirklich Handbuch-Charakter, und wer asymptotische Probleme im Zusammenhang mit Abzählung untersucht, kann an dem Buch nicht vorbei. Es stellt den *state of the art* dar.

Hier seien nur einige kurze Anmerkungen zum Inhalt verzeichnet: Teil A (symbolic methods) ist einem Lehrbuch der klassischen Kombinatorik vergleichbar, wobei *erzeugende Funktionen* und *kombinatorische Konstruktionen*, die sich in jene übersetzen lassen, im Mittelpunkt stehen. Part B (Complex asymptotics) hat 6 Kapitel. Rationale und meromorphe (erzeugende) Funktionen werden besprechen, sodann *Singularity analysis of generating functions*, was von Flajolet und Odlyzko entwickelt wurde, und die Sattelpunktsmethode. Das führt dann auch zu Haymans *Admissibility*. Teil C (Random structures) hat nur ein Kapitel, und widmet sich *Limit laws*. Im Vergleich zu traditionellen Methoden der Wahrscheinlichkeitstheorie führt der Zugang über erzeugende Funktionen und komplexe Analysis zu asymptotischen Aussagen, die nicht nur *first order*-Resultate liefern, sondern potientiell beliebig kleine Restglieder. Hervorzuheben ist etwa Hwangs *Quasi-power theorem*. Drei ausführliche Anhänge schließen allfällige Lücken des Lesers.

Das Buch ist ein lange erwarteter Meilenstein. Besonders löblich ist, dass es immer noch im Internet kostenlos erhältlich ist. Letzlich wird sich aber doch jeder Forscher ein gebundenes Exemplar leisten, denn so ein Buch begleitet einen das ganze Leben!

H. Prodinger (Stellenbosch)

Die Konvexgeometrie hat in der Person von Peter Gruber – dem jüngsten Ehrenmitglied der Österreichischen Mathematischen Gesellschaft – einen Vertreter, der Wesentliches zu diesem Gebiet beigetragen hat. Sein Referenzwerk "Convex and Discrete Geometry", dem er einen großen Teil seiner Arbeitszeit der letzten Jahre gewidmet hat, wird im Folgenden von R. Schneider gewürdigt.

P. M. Gruber: Convex and Discrete Geometry. (Grundlehren der mathematischen Wissenschaften, vol. 336) Springer, Berlin, 2007. ISBN 978-3-540-71132-2. € 106,95.

In this monograph, the author gives a broad and colourful picture of classic and contemporary convex geometry and discrete geometry. Although both subjects are subsumed under one heading in the AMS Mathematics Subject Classification, this is the first comprehensive presentation of the two related and interwoven subjects in one book. It is hard to think of any one better suited to mastering this huge task than Peter Gruber. The book is a careful introduction to the geometry of convex bodies, the theory of polytopes, and the geometry of numbers together with discrete geometry. In each part, it leads quickly to deep and important theorems and presents a wide variety of highly interesting and often surprising results. Naturally, a selection of topics had to be made; this was guided by excellent mathematical taste.

Each of the four parts, Convex Functions, Convex Bodies, Convex Polytopes, Geometry of Numbers and Aspects of Discrete Geometry, lays the foundations of its subject in a very precise and comprehensible way, at a level which is suitable for newcomers to the field. Therefore, large parts of this monograph can be used as textbook for different courses in geometry. A characteristic of this book is the great number of applications of convexity and outlooks to other fields, where results and arguments from convex or discrete geometry play an essential role. Such results are treated as soon as the tools for their understanding are available. Therefore, many nontrivial applications are suitable for the inclusion in introductory courses. Going on, even the experienced reader will find more and more results which he or she has not seen before in a monograph and perhaps not even in the original literature. The author has taken great care in selecting important and deep results and in detailing and remodelling their proofs, in order to present a clear and impeccable version.

To shed light on the wide scope of the book, I list here some examples of results in the first two parts where I was particularly pleased to find them in a book that addresses itself to a wider public and is accessible to students. My favourites are: 1.5 Characterization of the Γ function, 2.2 Alexandrov's theorem on the second order differentiability almost everywhere of a convex function, 4.3 Lyapunov's convexity theorem, 4.4 Pontryagin's minimum principle, 7.3 Hadwiger's characterization theorem for the intrinsic volumes, 8.4 Wulff's theorem in crystallography, 9.4 Isoperimetric inequalities of mathematical physics, 12.2 Characterization of balls by their gravitational fields. There are many other examples, all over the book, of theorems which earlier one had to dig out from the original literature and which are now conveniently accessible.

The part on Convex Polytopes has a character different from the existent books on polytopes, since it lays equal stress on the combinatorial theory, the metric theory, and the applications to linear optimization. It is well balanced between classical results, going back to Cauchy, Minkowski, Alexandrov and others, in a modern presentation, and more recent developments, like results on lattice point enumerators, the Betke-Kneser characterization of valuations on lattice polytopes, and Newton polytopes. The fourth part, Geometry of Numbers and Aspects of Discrete Geometry, gives a systematic introduction to the basic facts of the geometry of numbers, treats a series of special problems, and in discrete geometry lays the emphasis on packing, covering, tiling. Besides the lucid presentation of the great classical results, there is an ample treatment of more recent developments, of which I mention only the LLL basis reduction algorithm, the characterization of translative tiles due to Venkov and McMullen, a chapter on optimum quantization with its many applications, and a description of the connection between circle packings and the Riemann mapping theorem.

About the proofs taken from the original literature, one can say that every one of them has been scrutinized, clarified, enriched with details, and often completely rewritten. Many theorems, which have been important during the development of convex or discrete geometry, and the proofs of which are still too intricate to be presented in a non-specialized book, are stated and explained clearly without proof, but with reliable references (the list of more than 1000 references is a treasure). In this way, a fairly complete picture of the subject is obtained, with new aspects certainly also for experts in the field, containing many deep results and detailed proofs not to be found elsewhere, and exhibiting a wealth of beautiful results for everyone.

In my view, this book, written by a passionate geometer, serves three purposes equally well: it is an introduction for beginners in convex and discrete geometry, a valuable source for experienced workers in the field, and an invitation to a wider mathematical public to get aquainted with the various different aspects of convex and discrete geometry and their many fascinating relations to other areas.

R. Schneider (Freiburg i.Br.)

E. Behrends, P. Gritzmann, G. M. Ziegler (Hrsg.): π und Co. Kaleidoskop der Mathematik. Springer, Berlin, Heidelberg, 2008, ix+391 S. ISBN 978-3-540-77888-2 H/b € 24,95.

Das ist kein kein Lehrbuch der Mathematik und auch keine Monographie, sondern das vorliegende Buch stellt vielmehr eine bunte Collage aus 39 Artikeln und Buchbeiträgen zahlreicher namhafter Mathematikerinnen und Mathematiker dar. Viele (v.a. nicht mathematische) Aspekte der Mathematik werden beleuchtet.

Ein sehr empfehlenswertes, unterhaltsames, spannendes und äußerst vielseitiges Buch sowohl für interessierte Laien als auch für Fachleute.

G. Schranz-Kirlinger (Wien)

J. Borwein, K. Devlin: The Computer as Crucible. An Introduction to Experimental Mathematics. With Illustrations by K. H. Hofmann. A. K. Peters, Wellesley, Massachusetts, 2009, xi+158 S. ISBN 978-1-56881-343-1 P/b $ 29,95.

Die beiden Autoren bilden ein interessantes Team: Borwein ist neben zahlreichen anderen Aktivitäten ein Pionier der *Experimentellen Mathematik*, und Keith Devlin ist ein britischer Mathematiker, der sich (auch) als "popular science writer" einen Namen gemacht hat. Diese Öffentlichkeitsarbeit im Wissenschaftsbetrieb wird immer wichtiger und ist insbesondere in Österreich hervorragend durch Rudolf Taschner und seine *math.space*-Aktivitäten vertreten. Dazu kommt dann noch ein enthusiastischer Verleger, Klaus Peters, der selbst promovierter Mathematiker ist. Herausgekommen ist ein entzückendes Bändchen, das auch sehr von den geschmackvollen Illustrationen Karl Heinrich Hofmanns profitiert; dieser ist im Hauptberuf ebenfalls Mathematiker. Diese Art von Illustrationen weiß man seit Donald Knuth's TEXbook sehr zu schätzen.

Die Themen (Kapitel) des Buches kennt man vielleicht schon, insbesondere, wenn man drei frühere Bücher Borweins zu Hause hat. Aber das wahre Potential des Buches ist es, Menschen zur Beschäftigung mit Mathematik (und dem Computer als Hilfsmittel) anzuregen, die eben noch nicht mit der Materie vertraut sind. Und das ist hervorragend gelungen!

Gauss, Euler und Ramanujan waren zum Beispiel große Experimentatoren. Man findet auch die schöne Geschichte, wie man einzelne Stellen von π berechnen kann, ohne alle vorderen zu kennen. Weiters wird der "Inverse Symbolic Calculator" beschrieben, wie auch Sloanes Enzyklopädie. Die ζ-Funktion und "multiple zeta values" dürfen auch nicht fehlen, sowie etliche definite Integrale. Lamberts W-Funktion, Polylogarithmen und weitere „spezielle" Funktionen werden besprochen, wie auch kombinatorische Summen; da darf auch der Name Doron Zeilberger nicht fehlen.

Solche erfreulichen Bücher sind hochwillkommen! Man sollte dieses Buch auch an begabte Gymnasiasten verschenken, insbesondere, wenn es um Preisverleihungen geht. Die Autoren haben Freude an Mathematik, und die Leser spüren es. Und für all diejenigen, denen das Wort *crucible* vielleicht im Augenblick nicht geläufig ist: Es bedeutet Schmelztiegel, und man sieht auf dem Titelblatt auch einen weißbärtigen Schmied und seinen jugendlichen Adepten an der Esse stehen und Zahlen in den Tiegel schaufeln.

H. Prodinger (Stellenbosch)

J. M. Borwein, E. M. Rocha, J. F. Rodrigues (eds.): Communicating Mathematics in the Digital Era. A. K. Peters, Wellesley, Massachusetts, 2008, xii+325 S. ISBN 978-1-56881-410-0 H/b \$ 49,–.

Dieses Buch ging aus einer ICM Satellitentagung "Communicating Mathematics in the Digital Era" hervor, welche in Portugal 2006 stattfand. Die Hauptvortragenden sind im Wesentlichen diejenigen, die nun für die einzelnen Kapitel verantwortlich zeichnen. Das Material wurde in 3 große Gruppen eingeteilt, nämlich "Electronic Publishing and Digital Libraries", "Technology Enhancements for Disseminating Mathematics", und "Educational and Cultural Frameworks".

Es würde zu weit führen, auf die einzelnen Kapitel im Detail einzugehen, die oft die Projekte einzelner Länder beschreiben (Tschechien, Spanien, Frankreich, . . .). Eine kanadische Initiative ist zum Beispiel das "Coast-to-Coast Seminar", welches eine regelmäßige Video-Konferenz ist, an der sich etliche Universitäten beteiligen.

Mathematische Journale und ganz allgemein die Publikmachung mathematischer Inhalte ist in einem Umbruch begriffen, den jeder aktive Mathematiker selbst beobachten kann. In dem vorliegenden Band zu schmökern und zu schnuppern ist recht aufschlussreich. Vielleicht motiviert es auch das eine oder andere Team, sich aktiv an diversen Projekten zu beteiligen.

Das Buch ist kein Mathematikbuch im eigentlichen Sinne, beleuchtet aber doch Themen, die uns alle interessieren. Es sollte in mathematischen Bibliotheken vorhanden sein.

H. Prodinger (Stellenbosch)

S. Grabarchuk, P. Grabarchuk, S. Grabarchuk, Jr: The Simple Book of Not-So-Simple Puzzles. A. K. Peters, Wellesley, Massachusetts, 2008, vii+105 S. ISBN 978-1-56881-418-6 P/b \$ 19,95.

This booklet contains quite a few puzzles – a hundred-and-eight to be exact – which can really be puzzling at times. Some of them may strengthen the reader's self-esteem. But I have to warn you: Some of the riddles may have the opposite effect. And there is another caveat for those of you who love the analytic approach to problems and who want to see the context and the theory behind the problem:

This booklet may not be the real thing for you. Yes, there is a solution to every one of the problems. However, this solution does not explain or analyse the problem. It comes out of the blue. And that's that. But certainly there are two sides to every thing: If you feel like cracking a couple of nuts and if you don't want to be annoyed by theory and background information, then go for it!

J. Lang (Graz)

K. Houston: How to Think Like a Mathematician. A Companion to Undergraduate Mathematics. Cambridge University Press, 2009, xi+265 S. ISBN 978-0-521-71978-0 P/b £ 18,99.

Der Text richtet sich an Einsteiger in ein naturwissenschaftliches Studium, insbesondere natürlich der Mathematik. Es geht dem Autor nicht darum, viel konkreten Mathematik-Stoff zu vermitteln, sondern im Zentrum stehen die Themen Aussagenlogik, logisches Denken und Beweisführung. Also ein Buch über die für den Studierenden wichtigsten *soft skills* (wenn man es so ausdrücken möchte, aber eigentlich sind es ja *hard* skills). Zitat aus der Einleitung: 'Unfortunately, they [the students] expect us to ask questions and for them to give the answers because that is the way they have been educated. This book aims to give them the questions they need to ask so they don't need me anymore.'

Die verschiedenen Arten der Beweisführung werden systematisch besprochen, wobei z.B. auch auf den Unterschied zwischen einem Beweis durch Kontraposition (logische Umkehrung) und einem Widerspruchsbeweis hingewiesen wird (was oft nicht so genau unterschieden wird und eine Quelle der Verwirrung darstellen kann). Vieles wird an elementaren Fällen genau ausgeführt (z.B. der Beweis der Aussage „aus n^2 gerade folgt n gerade“). Linguistische und logische Fallen bleiben nicht unerwähnt.

John von Neumann meinte: *In mathematics you don't understand things. You just get used to them.* Das zielt auf den Punkt, wo z.B. Inhalte und Formelsprache ineinander verschwimmen (ein populäres Missverständnis). Es ist immer wieder gut, sich das bewusst zu machen. Der entsprechende Abschnitt über 'True understanding' geht jedoch nicht weiter auf dieses Thema ein. Weitere Abschnitte widmen sich den oft vernachlässigten Themen: Wie formuliert man Beweise richtig, wie liest und versteht man Beweise, etc. Es gibt auch einen Abschnitt 'How to solve problems', ein Sammlung von Tipps, die sich von selbst verstehen sollten, es für Einsteiger aber oft nicht sind. Insgesamt eignet sich das Buch sehr gut als Begleiter für das Studium; es ist sehr übersichtlich gestaltet und leicht ‚querzulesen‘. Auch viele Übungsaufgaben sind enthalten.

Als Leser mit langer Erfahrung in der Lehre könnte man sich noch mehr wünschen, etwa Anleitungen zur eigenständigen Darstellung komplexerer Zusammenhänge (ich denke etwa an einen Seminarvortrag oder eine Bachelorarbeit). Aber das ist wohl Thema für ein eigenes Buch.

W. Auzinger (Wien)

D. Paul: PISA, Bach, Pythagoras. Ein vergnügliches Kabarett um Bildung, Musik und Mathematik. Mit Musik-CD. 2. Auflage. Vieweg Verlag, Wiesbaden, 2008, xvi+212 S. ISBN 978-3-8348-0441-9 H/b € 24,90.

Schon das *Vorwort*, *Technische Vorbemerkungen oder Große Fußnote zum Thema Fußnoten* und *Gebrauchsanweisung oder Die Packungsbeilage* geben einen Ausblick auf das was noch kommt. Das Buch ist in 13 unabhängige Kapitel uns zwei Anhänge unterteilt. Ich finde die Idee ganz großartig, Mathematik als Kabaratt Menschen schmackhaft zu machen. Allerdings habe ich es ganz allgemein als schwierig empfunden, Kabarett zu lesen und nicht einer Aufführung beizuwohnen. Da das Buch insgesamt als vergnügliches Kabarett rund um Bildung, Musik und Mathematik tituliert ist, liegt auch eine CD mit Musikbeipielen bei.

G. Schranz-Kirlinger (Wien)

R. Taschner: Numbers at Work. A Cultural Perspective. Translated by O. Binder and D. Sinclair-Jones. A. K. Peters, Wellesley, Massachusetts, 2007, xi+209 S. ISBN 978-1-56881-290-8 H/b $ 39,–.

Das Buch ist die englische Ausgabe von Rudolf Taschners „Der Zahlen gigantische Schatten“, das von der Fachwelt und von an Mathematik Interessierten mit großer Begeisterung aufgenommen wurde. Die sorgfältige und teure Ausstattung entspricht wie bei der deutschen Ausgabe dem hohen Niveau des Gebotenen. Es ist erfreulich und wird dem Stellenwert des Buchs gerecht, wenn es mit der Übersetzung nun auch einen weiteren Adressatenkreis erreichen wird als das die deutsche Originalausgabe konnte.

P. Hackl (Wien)

H. Wußing: 6000 Jahre Mathematik. Eine kulturgeschichtliche Zeitreise. Unter Mitwirkung von H.-W. Alten und H. Wesemüller-Kock. (Vom Zählstein zum Computer.) Springer, Berlin, Heidelberg, 2008.

Band 1: Von den Anfängen bis Leibniz und Newton. Mit 305 Abbildungen, davon 161 in Farbe. xiii+529 S. ISBN 978-3-540-77189-0 H/b € 29,95.

Band 2: Von Euler bis zur Gegenwart. Mit einem Ausblick von E. Zeidler. Mit 435 Abbildungen, davon 269 in Farbe. xvii+675 S. ISBN 978-3-540-77313-9 € 29,95.

Ein zweibändiges, sehr ausführliches Werk zur Geschichte und Entwicklung der Mathematik. Auch Biographien von den Personen, die Mathematik betrieben und lehrten, finden sich zahlreich in diesen Büchern. Sehr interessant ist die Darstellung: Mathematik wird hier eingebettet in die politschen und kulturellen Ereignisse der jeweiligen Epoche. Auch Gedanken zur Zukunft der Mathematik, also ein Ausblick in das 21. Jahrhundert, wird präsentiert. Erwähnenswert ist, dass von den 6000 Jahren Mathematik im ersten Band etwa 5700 abgedeckt sind. Das spiegelt die rasante Entwicklung dieser Wissenschaft in den letzten 300 Jahren wider.

Dem Autor ist es jedenfalls gelungen, die Fülle des Stoffs soweit wie möglich in den aufeinanderfolgenden Epochen jeweils nach Gebieten gegliedert darzustellen und parallel dazu die Entwicklung in einzelnen Ländern zu zeigen.

Ein in jeder Hinsicht, v.a. aber mathematisch und historisch, sehr interessantes und bereicherndes Werk.

G. Schranz-Kirlinger (Wien)

Algebra und Diskrete Mathematik

J. Beck: Combinatorial Games. Tic-Tac-Toe Theory. (Encyclopedia of Mathematics and Its Applications 114.) Cambridge University Press, 2008, xiv+732 S. ISBN 978-0-521-46100-9 H/b £ 85,–.

Die klassische Spieltheorie bei Zweipersonen-Nullsummenspielen ist vor allem daran interessiert, bei Spielen mit unvollständiger Information durch geeignete Randomisierung (gemischte Strategien) zu optimalem Verhalten für beide Spieler zu gelangen. Die mathematische Basis bildet dabei ein Minimax-Theorem von John von Neumann, das heute mittels „starker Dualität“ bei linearen Optimierungsaufgaben auch einen algorithmischen Zugang zur Lösung derartiger Spiele bietet.

Spiele mit „vollständiger Information“ sind unter diesem Gesichtspunkt weniger interessant, da hier Randomisierung nicht mehr notwendig ist, und bereits deterministisches Verhalten der Spieler zu Gleichgewichtspunkten führt. Allerdings ist die Ermittlung der optimalen Strategien bei halbwegs interessanten Spielen nicht möglich, weil der Spielbaum kombinatorisch „explodiert“; man denke etwa an Schach.

Die relativ junge Disziplin der kombinatorischen Spieltheorie widmet sich diesem Problem. Im Gegensatz zur Klasse der kombinatorischen Spiele, wo man relativ einfach Gewinnkonfigurationen erkennen und dann die Lösung auf einfachere Unterspiele reduzieren kann, werden im vorliegenden Werk Spiele betrachtet, die solche Reduktionen nicht ohne weiteres erlauben. Als Repräsentant werden verallgemeinerte Versionen von *Tic-Tac-Toe* betrachtet. Diesen Spielen ist gemeinsam, dass der Spielablauf relativ einfach zu beschreiben ist (Markieren von Feldern mit „×“ oder „○“; diese Markierungen können nicht mehr rückgängig gemacht werden. Es gibt wohldefinierte Gewinnkonfigurationen.)

Obwohl der Spielbaum bei solchen Spielen nicht zugänglich ist, so kann man die probabilistische Methode von Erdős adaptieren, und eine randomisierte Variante des Spiels betrachten, wobei beide Spieler ihre Entscheidungen zufällig treffen. Durch geeignete Derandomisierung lassen sich dann Rückschlüsse auf optimale

Strategien ziehen. Dazu ist es notwendig, spieltheoretische Momente des randomisierten Spiels zu ermitteln und zu analysieren.

Dies erfolgt auf etwa 700 Seiten in 4 Teilen. Das Buch ist sehr flüssig geschrieben, aber es stellt hohe Anforderungen an die Leser.

F. Rendl (Klagenfurt)

D. Eisenbud: The Geometry of Syzygies. A Second Course in Commutative Algebra and Algebraic Geometry. With 27 Figures. (Graduate Texts in Mathematics 229.) Springer, Berlin, Heidelberg, New York, 2005, xvi+243 S. ISBN 0-387-22215-4 H/b, ISBN 0-387-22232-4 P/b € 29,95.

Eine *Syzygie* einer endlichen Familie $(f_i)_{i \in I}$ von Polynomen ist eine endliche Familie $(g_i)_{i \in I}$ von Polynomen mit der Eigenschaft $\sum_{i \in I} g_i f_i = 0$. Dieses Wort kommt aus dem Griechischen und hat die Bedeutung von „Verbindung" oder „zusammenspannen". Eine endliche Familie von Polynomen (in n Variablen) erzeugt einerseits ein Ideal im Polynomring und definiert andererseits eine algebraische Varietät, die Menge der gemeinsamen Nullstellen in K^n (wobei K der Koeffizientenkörper der Polynome ist). Syzygien können daher sowohl aus dem Blickwinkel der (kommutativen) Algebra als auch aus dem der (algebraischen) Geometrie betrachtet werden.

Das vorliegende Buch beschäftigt sich mit der qualitativen geometrischen Theorie der Syzygien. Es beschreibt geometrische Eigenschaften von projektiven Varietäten, die in enger Verbindung zu ihren Syzygien stehen. Es ist aus Vorlesungen des Autors – einer der weltweit führenden Experten der kommutativen Algebra und der algebraischen Geometrie – in Berkeley, Brandeis und Paris hervorgegangen.

Die Kapitel des Buchs: Free Resolutions and Hilbert Functions. First Examples of Free Resolutions. Points in P^2. Castelnuovo-Mumford Regularity. The Regularity of Projective Curves. Linear Series and 1-Generic Matrices. Linear Complexes and the Linear Syzygy Theorem. Curves of High Degree. Clifford Index and Canonical Embedding. Besonders die letzten zwei Kapitel führen direkt in die aktuelle Forschung und zu offenen Fragen.

Es gibt zwei sehr kompakt geschriebene Anhänge: Der erste führt in die lokale Kohomologie ein, der zweite stellt für das Buch nötige Vorkenntnisse der kommutativen Algebra (die über das Standardwissen eines Algebraikers hinausgehen) zusammen.

Dieses Buch ist sehr elegant geschrieben und vermittelt viele interessante Ideen. In der Lehre könnte es gut für weiterführende Vorlesungen über algebraische Geometrie verwendet werden.

Franz Pauer (Innsbruck)

I. M. Isaacs: Finite Group Theory. (Graduate Studies in Mathematics, Vol. 92.) American Mathematical Society, Providence, Rhode Island, 2008, xi+350 S. ISBN 978-0-8218-4344-4 H/b $ 59,–.

This beautiful book introduces the reader to basic topics in finite group theory. Some knowledge in group theory is assumed (although collected in an appendix), and so the journey starts with the Sylow Theory, and proceeds via subnormality, extension theory, commutators, transfer theory to Frobenius actions and to the Thompson subgroup. Up to here, the author intends it as a textbook for a 1-semester course in advanced group theory. What follows, are some deepenings on permutation groups, subnormality and transfers. This book tries successfully to bring out the beauty of group theory, with many highligts which can hardly (if ever) found in a book, like Zenkov's theorem about the intersection of abelian subgroups.

Remarkably nice is the collection of exercises which, from the first pages on, offer insights which might be unknown to most readers, some of them being extremely useful. I decided not to give this book into my shelf, but to leave it permanently on my desk. It is hard to find a text which is as beautiful and useful as this one.

G. Pilz (Linz)

Zahlentheorie

J. P. Buhler, P. Stevenhagen (eds.): Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography. (Mathematical Sciences Research Institute Publications 44.) Cambridge University Press, 2008, x+652 S. ISBN 978-0-521-80854-5 H/b £ 50,–.

This volume contains 20 survey articles based on lectures of the one-semester program on algorithmic number theory given at MSRI, Berkeley, in 2000. The first two articles are introductions to this fascinating area:

1. H.W. Lenstra, Jr.: *Solving the Pell equation.* 2. J. Buhler, S. Wagon: *Basic algorithms in number theory.*

The next eight deal with classical problems from algorithmic number theory (factoring, primality, smooth numbers, lattices, elliptic curves, algebraic number theory, fast arithmetic algorithms):

3. C. Pomerance: *Smooth numbers and the quadratic sieve.* 4. P. Stevenhagen: *The number field sieve.* 5. R. Schoof: *Four primality testing algorithms.* 6. H.W. Lenstra, Jr.: *Lattices.* 7. B. Poonen: *Elliptic curves.* 8. P. Stevenhagen: *The arithmetic of number rings.* 9. A. Granville: *Smooth numbers: computational number theory and beyond.* 10. D.J. Bernstein: *Fast multiplication and its applications.*

The remaining ten articles are surveys from closely related areas (cryptography, Arakelov class groups, computational class field theory, zeta functions over finite fields, arithmetic geometry, modular forms):

11. C. Pomerance: *Elementary thoughts on discrete logarithms.* 12. O. Schirokauer: *The impact of the number field sieve on the discrete logarithm problem in finite fields.* 13. D.J. Bernstein: *Reducing lattice bases to find small-height values of univariate polynomials.* 14. R. Schoof: *Computing Arakelov class groups.* 15. H. Cohen, P. Stevenhagen: *Computational class field theory.* 16. D.J. Bernstein: *Protecting communications against forgery.* 17. D. Wang: *Algorithmic theory of zeta functions over finite fields.* 18. A.G.B. Lauder, D. Wang: *Counting points on varieties over finite fields of small characteristic.* 19. J. Top, N. Yui: *Congruent number problems and their variants.* 20. W.A. Stein: *An introduction to computing modular forms using modular symbols.*

A. Winterhof (Linz)

W. W. L. Chen, W. T. Gowers, H. Halberstam, W. M. Schmidt, R. C. Vaughan (eds.): Analytic Number Theory. Essays in Honour of K. Roth. Cambridge University Press, 2009, xviii+491 S. ISBN 978-0-521-51538-2 H/b £ 60,–.

This book contains the following 32 essays in honour of Klaus Roth: 1. R. Baker, G. Harman: *Numbers with a large prime factor II.* 2. W.D. Banks, I.E. Shparlinski: *Character sums with Beatty sequences.* 3. J. Beck et al.: *The Hales-Jewett number is exponential.* 4. V. Beresnevich et al.: *Classical metric Diophantine approximation revisited.* 5. J. Bourgain: *The sum-product phenomenon.* 6. T.D. Browning, D.R. Heath-Brown: *Integral points on cubic hypersurfaces.* 7. J. Brüdern: *Binary additive problems and the circle method, multiplicative sequences and convergent sieves.* 8. Y. Bugeaud: *On the convergents to algebraic numbers.* 9. B. Chazelle: *Complexity bounds via Roth's method of orthogonal functions.* 10. W. Chen, G. Travaglini: *Some of Roth's ideas in discrepancy theory.* 11. H.G. Diamond, H. Halberstam: *Congruences and ideals.* 12. P.D.T.A. Elliott: *Elementary geometry of Hilbert spaces applied to abelian groups.* 13. B. Green, T. Tao: *New bounds for Szemerédi's theorem II.* 14. N. Hebbinghaus et al.: *One-sided discrepancy of linear hyperplanes in finite vector spaces.* 15. H.A. Helfgott, A. Venkatesh: *How small must ill-distributed sets be?* 16. C. Hooley: *On the power-free values of polynomials in two variables.* 17. N.M. Katz: *On a question of Browning and Heath-Brown.* 18. S. Konyagin: *Good distribution of values of sparse polynomials modulo a prime.* 19. A. Lasjaunias: *Diophantine approximation and continued fractions in power series fields.* 20. M. Laurent: *On transfer inequalities in Diophantine approximation.* 21. H. Maier: *On exponential sums with multiplicative coefficients.* 22. D. Masser: *Multiplicative dependence of values of algebraic functions.* 23. B. de Mathan: *Linear forms in logarithms, and simultaneous Diophantine approximation.* 24. M.B. Nathanson: *The Caccetta-Häggkvist conjecture and additive number theory.* 25. E. Novak,

H. Woźniakowski: *L_2 discrepancy and multivariate integration.* 26. A. Sárközy, C.L. Stewart: *Irregularities of sequences relative to long arithmetic progressions.* 27. A. Schinzel: *The number of solutions of a linear homogeneous congruence II.* 28. W.M. Schmidt: *The Diophantine equation* $\alpha_1^{x_1} \dots \alpha_n^{x_n} = f(x_1, \dots, x_n)$. 29. D.S. Thakur: *Approximation exponents for function fields.* 30. R.C. Vaughan: *On generating functions in additive number theory I.* 31. M. Waldschmidt: *Words at transcendence.* 32. U. Zannier: *Roth's theorem, integral points and certain ramified covers of* P_1.

A. Winterhof (Linz)

W. A. Coppel: Number Theory. An Introduction to Mathematics: Part A and B. Springer, Berlin, Heidelberg, New York, 2006, Part A: xv+339+28 S. ISBN-10 0-387-29851-7, ISBN-13 978-0387-29851-1, H/b € 46,95, Part B: ix+326+27 S. ISBN-10 0-387-29853-3, ISBN-13 978-0387-29853-5, H/b € 46,95.

Eine Einführung in die Mathematik ist dieses Buch nicht wirklich. Dass es von A bis Z als Textbuch geeignet ist, daran zweifle ich auch. Eher ist es eine Reise durch die fundamentale mathematische Welt von W. Coppel. Die Grundidee besteht darin, ein Gefühl der Einheit und der Vielfalt der Mathematik beizubringen. Dazu eignet sich Zahlentheorie besonders gut, da allerlei algebraische Strukturen sowie reelle, komplexe, asymptotische, Fourier Analysis, dynamische Systeme und Wahrscheinlichkeitstheorie bei ihr unmittelbar bedeutsame Anwendungen finden. In diesem Sinne ist das Buch eine Einführung in die Mathematik durch die Zahlentheorie: die gewöhnlichen Strukturen werden eingeführt und sofort verwendet, um Ergebnisse zu bekommen. Coppel teilt die intellektuellen Prioritäten von Bourbaki. In manchen Kapitel hat er einen klassischen, eigenwillig altmodischen Standpunkt eingenommen. Er folgt Jacobi, wenn es sich um elliptische Funktionen handelt. Es gibt Anwendungen auf die Mechanik, aber keine auf die Kryptographie.

Die 13 Kapitel behandeln folgende Themen: (1) Konstruktion der verschiedenen Zahlenmengen, (2&3) Teilbarkeit, Kongruenzen, quadratische Reste und quadratische Körper, arithmetische Funktionen, (4) Kettenbrüche, diophantische Approximation, Pellsche Gleichung, (5) Hadamard-Matrizen, Designs, (6) Absolutbeträge, p-adische Zahlen, (7) Quadratische Formen, (8) Geometrie der Zahlen, Gitter, Kugelpackungen, (9& 10) Verteilung der Primzahlen, Formulierungen und Beweis des Primzahlsatzes, harmonische Analysis, (11) Gleichverteilung und Ergodentheorie – der elegante Beweis des Ergodensatzes von Keane wird gegeben, und der Satz von Van der Waerden wird ausführlich bewiesen (in einer Partition der ganzen rationalen Zahlen enthält ein Element der Partition arithmetische Teilfolgen beliebiger Länge), (12& 13) Elliptische Integrale und Funktionen mit Anwendungen auf arithmetische Funktionen; der Satz von Mordell wird unter der Voraussetzung, dass $E(\mathbb{Q})$ ein Element der Ordnung 2 besitzt, bewiesen.

Die Kapitel sind ähnlich aufgebaut. Zunächst wird die Theorie pädagogisch entwickelt, mit Beispielen oder einfachen Ergebnissen beginnend. In einem weiteren Abschnitt werden Verallgemeinerungen, Anwendungen, Verfeinerungen ohne Beweis erwähnt, historische und fachliche Anmerkungen hinzugefügt, und eine ausführliche Literaturliste angegeben. Die Beweise sind detailliert, lückenlos, gepflegt, sehr klar, oft elegant. Auch hundertmal gedruckte Beweise wie der des Primzahlsatzes durch die Methode von Wiener-Ikehara hat Coppel verarbeitet, leicht modifiziert und durchsichtig gemacht. Dennoch nimmt sich Coppel mehr Freiheit, wenn es sich um beweislose Ergänzungen handelt. Dann wendet er sich offenbar an einen fortgeschrittenen Leser. Zum Beispiel werden Quotienten der klassischen Gruppen erwähnt, bevor der Begriff einer Gruppe überhaupt eingeführt wird! Es gibt keine Übungen.

Die Kapitel sind nicht voneinander unabhängig. Da der Autor den Konnex zwischen verschiedenen mathematischen Themen deutlich herausstellen will, werden oft frühere Ergebnisse in einem neuen Rahmen verwendet.

Als Beispiel für den Stil gebe ich den Inhalt des siebten Kapitels genauer wieder: Thema ist die Theorie der quadratischen Formen. In der Einleitung wird angedeutet, das Hauptziel sei der Satz von Hasse-Minkowski. Es beginnt mit der algebraischen Theorie der quadratischen Formen über einem beliebigen Körper (äquivalente q.F., Existenz einer Basis, Klassifizierung über den reellen Zahlen und den endlichen Körpern). Dann wird das Hilbert-Symbol eingeführt – also $(a,b) = 1$ dann und nur dann, wenn die Gleichung $ax^2 + by^2 = 1$ Lösungen besitzt. Das Hilbert-Symbol über $\mathbb{Q}_p$ wird untersucht – die p-adischen Zahlen sind im vorigen Kapitel definiert worden. Die Tabelle der Hilbert-Symbole bilden Hadamard-Matrizen, welche im Kapitel 5 diskutiert wurden. Mithilfe der Kapitel 5 und 6 beweist Coppel den Satz von Hasse-Minkowski. Zuletzt gibt es verschiedene Anmerkungen über alternative Beweise, Geschichte, u.a. über obere Schranken für die Anzahl der oben studierten Gleichungen.

Als Dynamiker hat Coppel offensichtlich die Rolle der reellen Analysis betont, insbesondere die der Ergodentheorie. Die algebraische Zahlentheorie ist fast nicht vorhanden, und die probabilistische Zahlentheorie kommt überhaupt nicht vor. Wenn man das Buch als Ausdruck eines persönlichen Geschmacks versteht, ist solch ein Vorwurf bedeutungslos. Übrig bleibt ein schöner Text über klassische Zahlentheorie.

G. Barat (Marseille)

H. G. Diamond, H. Halberstam: A Higher-Dimensional Sieve Method. With Procedures for Computing Sieve Functions (W. F. Galway). (Cambridge tracts in mathematics 177.) Cambridge University Press, 2008, xxi+266 S. ISBN 978-0-521-89487-6 H/b £ 45,–.

The aim of this book is to present a new and general approach to higher-dimensional sieves. Two of the great specialists of the subject matter develop in a very readable way a hybrid of the Selberg and the Rosser-Iwaniec sieve to extend the existing theory to problems of sieve dimension higher than 1. A partial account (based on Selberg's method) can be found in Greaves (2001), "Sieves in Number Theory".

The main contribution of the present book is an extension to sifting dimension $\kappa > 1$ (also called sifting density) of a method of Jurkat and Richert for dimension 1 (which sees the Selberg sieve combined with infinitely many iterations of the Buchstab identity). The main analytic difficulty in the proof is to ensure the solvability of a certain coupled system of difference-differential equations satisfying given boundary conditions. The second part of the book is fully devoted to a detailed study of these equations. The numerical solution is obtained with the help of *Mathematica*, and a *Mathematica* package for sieve-theoretical calculations can be downloaded from the book's webpage (*http://www.math.uiuc.edu/SieveTheoryBook*).

The plot of the book follows closely the style of Halberstam & Richert, Sieve Methods, 1974: short chapters, good motivating background, aiming for a simple exposition and for striking applications (twin prime conjecture, prime g-tuples conjecture etc.).

Sieve theory is a rather sophisticated area within the realm of analytic number theory, and it takes a considerable effort (and amount of time) to learn the subtleties of the field. The present book is definitely of great interest to the intermediate-advanced sieve theorist. Beginners in sieve theory should first start with Nathanson (1996), "Additive Number Theory: The Classical Bases" or (no picnic!) work their way through the book of Greaves.

T. Stoll (Marseille)

H. M. Edwards: Higher Arithmetic. An Algorithmic Introduction to Number Theory. (Student Mathematical Library, Vol. 45.) American Mathematical Society, Providence, Rhode Island, 2008, xii+210 S. ISBN 978-0-8218-4439-7 P/b \$ 39,–.

Dieses interessante und ungewöhnliche Buch erarbeitet die ersten Kapitel der *disquisitiones arithmeticae* von C. F. Gauss. Ausgehend von der Diophantischen Gleichung $AX^2 + B = Y^2$ wird die Theorie der Kongruenzen, der Arithmetik von quadratischen Zahlringen und der binären quadratischen Formen entwickelt. Dabei ist der Autor jedoch bestrebt, keinerlei "set-theoretic abstractions and unrealizable constructions" zu verwenden, sondern alles auf "algorithms and computations" aufzubauen. Jeglichen Hinweis auf eine algebraische Struktur wird man in diesem Buch vergebens suchen. Zum Rechnen genügen die nichtnegativen ganzen Zahlen und später die "hypernumbers", die durch Hinzunahme des zusätzlichen Symbols $\sqrt{A}$ (A positiv und keine Quadratzahl) entstehen. Wie man unter Verzicht auf Algebra und auf negative Zahlen Kongruenzen in nicht faktoriellen Ringen einführt, kann der neugierige Leser auf Seite 81 des Buchs nachlesen. Geschlechtertheorie und die Komposition von binären quadratischen Formen wird natürlich auch à la Gauss behandelt. Ungewöhnlich ist auch, dass der Autor neue Bezeichnungen für etablierte Begriffe verwendet, wie z.B. "stable/pivotal modules" für „reduzierte/ambige" Ideale oder "signature" statt „Geschlechtscharakter".

Günter Lettl (Graz)

Geometrie, Topologie

W. Benz: Classical Geometries in Modern Contexts. Geometry of Real Inner Product Spaces. Second Edition. Birkhäuser Verlag, Basel, Boston, Berlin, 2007, xiii+277 S. ISBN 978-3-7643-8540-8 H/b EUR 79,90.

This book is the second edition of one of the standard textbooks on the geometry of real inner product spaces. It contains chapters on translation groups, on Euclidean and Hyperbolic geometry, on Möbius and Lie geometries, on Lorentz transformations, on δ-projective mappings and theorems of isomorphism. The precise and clear style of the presented matter enables the reader (with some basic knowledge) to obtain some profound insight into this field of geometry. Most of the chapters are devoted to dimension-free considerations. The last chapter on δ-projective mappings and isomorphism theorems is new in this second edition. The conditions for isometries between two different spaces are worked out in detail. The book can be recommended to students and teachers who want to get into the state of the art of this theory.

O. Röschel (Graz)

A. I. Bobenko, Yu. B. Suris: Discrete Differential Geometry. Integrable Structure. (Graduate Studies in Mathematics, Vol. 98.) American Mathematical Society, Providence, Rhode Island, 2008, xxiv+404 S. ISBN 978-0-8218-4700-8 H/b \$ 69,–.

Discrete differential geometry has its origin in the desire to discretize differential-geometric notions in an intelligent way and today contains a mature theory exhibiting the classical differential geometry of coordinate systems in surfaces as a special case. The authors have contributed significantly to this development, which in particular established links with integrable systems, and which recognized geometric consistency as the true background of integrability (which is otherwise only rather informally defined).

The contents of this book are the following: Chapter 1 repeats the classical results on surfaces and transformations. Chapters 2–4, *Discretization Principles* and *Special Classes of Surfaces* introduce the discrete theory by means of discrete integrable systems and their consistency. The next chapter on *Approximation* gives a sure foundation to the viewpoint of the smooth theory as a special case or limit case of the discrete one.

The conceptual core of the book is Chapter 6, *Consistency as integrability*, with its fundamental insight that 3D consistency of equations on 2D lattices is responsible for the usual properties of integrable systems, like Bäcklund transforms or zero curvature representations. Chapters 7 und 8 deal with discrete complex analysis and circle packings, while Chapter 9, *Foundations*, is a survey of that part of projective geometry needed elsewhere in the book.

The authors have succeeded in an impressive manner to collect and exhibit a branch of mathematical knowledge which was hitherto accessible only in single publications. At the same time this book contains new and unpublished results. The many exercises make this work very valuable for courses. It is heartily recommended.

J. Wallner (Graz)

T. tom Dieck: Algebraic Topology. (EMS Textbooks in Mathematics.) EMS, Zürich, 2008, xi+567 S. ISBN 978-3-03719-048-7 H/b € 58,–.

This book is a broad introduction to algebraic topology. Its first part deals with standard topics of algebraic topology, namely homotopy and homology theories. This includes basic studies of homotopy, fundamental groups, covering spaces, cell complexes, singular and cellular homology etc. and their interrelations. The second part of the book describes more advanced topics. In particular the author discusses bundles and their homotopy properties, and gives basic definitions and results on differential manifolds and their homology. Several chapters are devoted to dualities between homology and cohomology theories. In addition the reader gets a relatively complete overview on the theory of characteristic classes (Chern, Stiefel-Whiteney, Pontryagin classes). The book concludes with a few words about bordism (including the Pontryagin-Thom theorem).

The book is written in the modern terminology of category theory, especially in its first part. It contains many exercises and examples. Several theorems contain simplified proofs that have never appeared in the literature before.

O. Karpenkov (Graz)

A. Katok, V. Climenhaga: Lectures on Surfaces. (Almost) Everything You Wanted to Know about Them. (Student Mathematical Library, Vol. 46.) American Mathematical Society, Providence, Rhode Island, 2008, xv+286 S. ISBN 978-0-8218-4679-7 P/b $ 49,–.

This series of 36 lectures has evolved from courses at Penn State University. They lead the reader through a variety of areas: combinatorics, Riemannian geometry, real and complex differentiable structures, topology and many more. There is even a paragraph on hyperbolic planes, embedded in the chapter on Riemannian metrics. The emphasis is more on the topological rather than on the algebraic side. Of course it is not possible to completely cover so vast an area in a handy paperback. What the authors achieve, though, is pretty much amazing. They do not simply pile up things and ideas with some relevance in the realm of surfaces. Far from it: They lay the bricks carefully and do not forget the mortar.

In every lecture the authors describe and motivate the new definitions, explain the propositions and deliver the goods (i.e., proofs). The reader is never left behind. I must admit that in a book this broad I would not have expected such an amount of consistency and pedagogical verve.

The most appealing thing about this book is its determination. Many a facet of surfaces is covered (or at least touched upon) in this booklet. Sure, the geometry of surfaces is a prolific field, but after this read it seems a lot more so.

J. Lang (Graz)

L. Keen, N. Lakic: Hyperbolic Geometry from a Local Viewpoint. (London Mathematical Society Student Texts 68.) Cambridge University Press, 2007, x+271 S. ISBN 978-0-521-68224-4 P/b £ 23,99.

The main theme of this book is hyperbolic metrics in 'arbitrary' planar domains. As a preparation for this, many aspects of classical hyperbolic geometry are introduced first.

The authors start with Möbius geometry, the hyperbolic metric in the unit disk, and the different kinds of hyperbolic isometries there (Sections 1 and 2). Sections 3 and 4 deal with conformal mappings in general, and with conformal uniformization. Discrete groups of hyperbolic transformations, and especially Fuchsian groups are next. In particular Poincaré's theorem on generating groups via edge pairings in fundamental domains is shown.

Having completed this introductory material, the authors move to define the hyperbolic density in a planar domain X which has at least two boundary points. This is done by pushing forward the hyperbolic density in the unit disk H^2 with a universal covering map $\pi : H^2 \to X$. The length of a tangent vector $w = d\pi(v)$ attached to $q = \pi(p) \in X$ is computed by

$$\|w\|_{q\in X} = \|v\|_{p\in H^2} \big/ \|w\|_{\mathbb{R}^2}.$$

The infimum of densities generated by push forwards via a conformal mapping (of which π is an example) is the Kobayashi density.

The book proceeds with properties of these densities, the Caratheodory density, with Lipschitz and Bloch domains, and with the important and difficult task of estimating densities. Three chapters concern applications in connection with iterated systems of holomorphic functions and the limits of such systems.

Here new and interesting results are collected and presented for a target audience of graduate students and researchers, but the first half of the book is well accessible also for undergraduate students, and indeed everyone who is interested in an introduction to hyperbolic geometry.

J. Wallner (Graz)

S. G. Krantz, H. R. Parks: Geometric Integration Theory. (Cornerstones.) Birkhäuser, Boston, Basel, Berlin, 2008, ix+339 S. ISBN 978-0-8176-4676-9 H/b € 58,74.

Geometrische Maß- und Integrationstheorie ist eines der schönsten Gebiete der Mathematik. Sie ist ausgezeichnet durch natürliche Fragestellungen, z.B. das isoperimetrische Problem, und durch nichttriviale Antworten. Will man sich einlesen oder ein Resultat nachschlagen, so ist das umfangreiche Buch von Federer wenig hilfreich. Andere Bücher dieser Art gibt es kaum, wenn man von denen von Evans und Gariepy, Lin und Yang, Mattila und Simon absieht. Das vorliegende Buch kommt den zuerst genannten Bedürfnissen bestens nach. Die Kapitelüberschriften geben einen guten Eindruck der dargestellten Fülle des Stoffes: Die Carathéodorysche Konstruktion und niedrigdimensionale Maße, Invariante Maße und die Konstruktion des Haarschen Maßes, Überdeckungssätze und Differentiation von Integralen, die Flächenformel, die Coflächenformel und Poincarésche Ungleichungen, Differentialformen und der Satz von Stokes, Currents und Variationsrechnung, Regularität von maßminimierenden Currents. Einige Figuren unterstützen das Verständnis.

Den Autoren ist zu diesem gelungenen Werk zu gratulieren und viele Leser, die im Grenzgebiet von Geometrie und Analysis arbeiten, werden ihnen dankbar sein. Dem Buch ist eine weite Verbreitung zu wünschen.

P. M. Gruber (Wien)

M. Mukerji: Ornamental Origami. Exploring 3D Geometric Designs. A. K. Peters, Wellesley, Massachusetts, 2009, x+145 S. ISBN 978-1-56881-445-2 P/b $ 24,95.

The book is devoted to the exploration of polyhedral ornaments composed of origami pieces. It is no mathematical textbook as it presents tools, tips and techniques for folding origami parts which can be assembled to form spatial models. For a wide series of models the folding procedures are described in clear and understandable notation. The author presents examples for ornaments belonging to the polyhedral groups of E_3 – with spectacular results. It is astonishing what interesting structures can be achieved by “simple folding paper”.

The writer of this review has enjoyed the great variety of models generated according to this handbook. It was a nice and recreational time following the instructions during some evenings of paper folding. But the results have been worth it.

So the book can be recommended to all skilful persons interested in origami techniques and the world of polyhedral ornaments.

O. Röschel (Graz)

Reelle und Komplexe Analysis

D. M. Bressoud: A Radical Approach to Lebesgue's Theory of Integration. (MAA Textbooks.) Cambridge University Press, 2008, xiv+329 S. ISBN 978-0-521-71183-8 P/b £ 24,99*, ISBN 978-0-521-88474-7 H/b £ 60,–.

D. Bressoud ist der Autor des Vorgängerbandes "A Radical Approach to Real Analysis", und das hier vorliegende Lehrbuch ist in demselben Geist verfasst. 'Radical Approach' bezeichnet eine Darstellung, die an der historischen Entwicklung orientiert ist, ausgehend von der Riemannschen Definition des Integralbegriffs und seiner Kritik durch die Fachkollegen im 19. Jahrhundert. Am Anfang stehen die 'Five Big Questions': Konvergenz von Fourierreihen, Natur des Integralbegriffs, Gültigkeit des Hauptsatzes, Zusammenhang zwischen Stetigkeit und Differenzierbarkeit und gliedweise Integration von Funktionenreihen.

Der Text ist keine historische Abhandlung, ist aber eng an der Historie der Thematik im 19. und frühen 20. Jahrhundert orientiert. Die Problematik der nirgends dichten Teilmengen von $\mathbb{R}$ und die Verwirrung über den Hauptsatz der Differential- und Integralrechnung motivierten die Untersuchung der „Geometrie" der reellen Zahlen und die Aktivitäten hinsichtlich einer präzisen Fassung des Maßbegriffs durch Jordan, Borel bis hin zu Lebesgue. Nach der Einführung Lebesgue-messbarer Funktionen und des Lebesgue-Integrals werden die wesentlichen klassischen Sätze diskutiert, bis hin zum Satz über die dominierte Konvergenz als Kriterium für gliedweise Integration.

Das Kapitel über den Hauptsatz gipfelt in der definitiven Version nach Lebesgue für absolut stetige Integranden. Im abschließenden Teil über Fourierreihen finden sich die Resultate über die f.ü. Konvergenz von Césaro-Mitteln, und natürlich die Standardresultate für Funktionen aus L^2 (Vollständigkeit des trigonometrischen Fundamentalsystems, Satz von Riesz-Fischer).

Eine einschlägige Lehrveranstaltung an diesem Text zu orientieren, wäre der Gegenpol zu der oft gehandhabten axiomatischen Einführung von Lebesgue-Maß und Lebesgue-Integral. Dies wäre didaktisch sehr vertretbar, kostet aber wohl relativ viel Zeit. Das Buch ist eher als Quelle für zusätzliches Lehrmaterial und viele (Gegen)beispiele und Übungsaufgaben zu sehen. Es finden sich auch speziellere Resultate wie z.B. über die „fast-Stetigkeit" messbarer Funktionen, und die „fast gleichmäßige" Konvergenz von f.ü. konvergenten Folgen messbarer Funktionen (Satz von Egorov).

W. Auzinger (Wien)

O. Christensen: Frames and Bases. An Introductory Course. (Applied and Numerical Harmonic Analysis.) Birkhäuser, Boston, Basel, Berlin, 2008, xviii+313 S. ISBN 978-0-8176-4677-6 H/b € 42,69.

Frames sind eine Begriffsbildung aus der Banachraum-Theorie bzw. in konkreterer Form aus der harmonischen Analysis, die sehr eng verwandt ist mit Riesz-Basen, wavelets, etc. Die Theorie der Frames hat sich in den letzten Jahrzehnten zu einem substantiellen Gebäude entwickelt; es gibt viele tiefliegende Ergebnisse und Beispiele, offene Fragen, und auch Anwendungen.

In dem vorliegenden Werk wird eine Verbindung zwischen der abstrakten Theorie von Frames und konkreten Konstruktionen solcher sowie Anwendungen in der Signalverarbeitung, hergestellt. Dementsprechend ist das Buch zweigeteilt; in den Kapiteln 1–5 werden Basen und Frames in Banach- und Hilberträumen diskutiert, die anderen Kapitel 6–11 widmen sich konkreten Konstruktionen und Anwendungen.

Der in der Funktionalanalysis arbeitenden Wissenschafter wird im ersten Teil dieses Buchs wahrscheinlich nur eine Einführung sehen und dann zu dem wesentlich ausführlicheren Buch "An Introduction to Frames and Riesz Bases" des gleichen Autors weiterschreiten. Der Student oder der funktionalanalytisch nicht versierte Leser dagegen wird die schlanke und auf niedrigem Niveau ansetzende Darstellung begrüßen. Dementsprechend geeignet ist diese Buch auch zur Vorbereitung einer Vorlesung.

H. Woracek (Wien)

E. Freitag, R. Busam: Complex Analysis. (Universitext.) Springer, Berlin, Heidelberg, New York, 2005, x+547 S. ISBN 3-540-25724-1 P/b € 39,95.

Dieses Buch ist die englische Übersetzung der vierten Auflage des – von den Autoren in deutscher Sprache abgefassten – Bands „Funktionentheorie 1" (Springer, 2006). Da die früheren Auflagen dieses Werks schon verschiedentlich besprochen wurden (siehe etwa IMN Nr. 167 und IMN Nr. 190), darf eine Besprechung des vorliegenden Bands wohl eher kurz ausfallen:

Die vierte Auflage – und damit auch die englische Übersetzung – ist eine verbesserte und erweiterte Fassung dieses erfolgreichen Buches. Der Aufbau blieb unerverändert, einige neue Übungsbeispiele wurden hinzugefügt. Wie bisher ist es auch bei diesem Buch ein Vergnügen, darin zu lesen – es eignet sich bestens sowohl zum Selbststudium als auch als Vorlesungsunterlage.

Inzwischen ist bereits eine zweite Auflage des vorliegenden Bands erschienen (Springer, 2009).

P. Dörfler (Leoben)

J. B. Garnett, D. E. Marshall: Harmonic Measure. (New Mathematical Monographs 2.) Cambridge University Press, 2008, xv+571 S. ISBN 978-0-521-72060-1 P/b £ 30,00*, ISBN 978-0-521-47018-6 H/b £ 69,–.

Das vorliegende Werk ist eine moderne und umfassende Darstellung der Theorie des harmonischen Maßes in der komplexen Zahlenebene. Der Begriff des harmonischen Maßes hat eine lange Tradition und spielt schon in den Anfängen der Potentialtheorie und geometrischen Funktionentheorie eine wichtige Rolle. In den letzten Jahrzehnten hat sich dieses Gebiet wesentlich weiterentwickelt. Um nur einige Themen zu nennen, bei denen in letzter Zeit wesentliche Fortschritte erzielt wurden: das Verhältnis des harmonischen Maßes zum Hausdorffmaß, das *Bishop-Jones* $H^{\frac{1}{2}-\eta}$ *Theorem* oder einige Entwicklungen rund um die Brennan Conjecture. Dementsprechend beinhaltet das vorliegende Buch, neben all den klassischen Sätzen, auch einige Ergebnisse, welche hier zum ersten Mal in Buchform aufbereitet wurden.

Das Buch ist für jeden Wissenschafter oder fortgeschrittenen Studenten mit einer soliden Grundausbildung in reeller und komplexer Analysis zugänglich. Die notwendigen Grundlagen aus der Potentialtheorie und Hardy-Raum-Theorie werden in den ersten vier Kapiteln sowie einer Serie von Anhängen dargelegt. Am Ende jedes Kapitels findet man Beispiele, Aufgaben und Ausblicke. Die Präsentation ist wohlüberlegt, und angenehm zu lesen. Insgesamt hat dieses Buch sicher das Potential, ein Standardwerk zu werden. Zur Vorbereitung einer Vorlesung ist das Buch, aufgrund seines Umfangs, jedoch wahrscheinlich nur beschränkt geeignet.

H. Woracek (Wien)

N. V. Krylov: Lectures on Elliptic and Parabolic Equations in Sobolev Spaces. (Graduate Studies in Mathematics, Vol. 96.) American Mathematical Society, Providence, Rhode Island, 2008, xviii+357 S. ISBN 978-0-8218-4684-1 H/b $ 65,–.

Ziel des Buchs ist die Darstellung einer Lösungstheorie linearer, elliptischer und parabolischer Differentialgleichungen in Sobolewräumen W_p^m mittels a-priori-Ungleichungen. Dabei wird für $p = 2$ die Fouriertransformation und für $p \neq 2$ die Theorie der singulären Integraloperatoren in Gestalt der Maximalfunktion und des Satzes von Fefferman-Stein herangezogen. Diese Verwendung neuerer Hilfsmittel aus der Harmonischen Analysis gestattet es dem Autor, im 6. und 7. Kapitel eine Lösungstheorie für elliptische und parabolische Gleichungen mit VMO-Koeffizienten ("vanishing mean oscillation") darzustellen. Von klassischen Texten zu denselben Themen unterscheidet sich das Buch durch das Fehlen expliziter Lösungsformeln und der sogenannten Integralgleichungsmethode. Das Buch endet mit Kapiteln über Sobolewsche Einbettungssätze, Maximumprinzipien, Pseudodifferentialoperatoren und Räumen von Besselpotentialen.

N. Ortner (Innsbruck)

W. T. Shaw: Complex Analysis with *Mathematica*. CD updated for Mathematica 6. Cambridge University Press, 2008, xiii+571 S. ISBN 978-0-521-83626-5 H/b £ 45,–.

This book is an attempt to use *Mathematica* to illuminate the topic of complex analysis. It starts with solving quadric, cubic and quartic equations. The following chapters are devoted to complex iteration, especially to the Newton iteration in order to explain complex fractals, the Mandelbrot set and the concept of bifurcation using various visualizations with *Mathematica*. In the third part traditional complex analysis is presented, where *Mathematica* is again used to visualize complex functions or to evaluate contour integrals and residues. The novel features of the last part of the book include the use of *Mathematica* to visualize conformal mappings and their applications to potential flow, exploring numerical transform techniques, the Schwarz-Christoffel transformation and the theory of spinors and twistors. Each chapter ends with a collection of exercises, the enclosed CD contains electronic copies of all the chapters of the text, in the form of *Mathematica* notebooks.

F. Haslinger (Wien)

D. C. Ullrich: Complex Made Simple. (Graduate Studies in Mathematics, Vol. 97.) American Mathematical Society, Providence, Rhode Island, 2008, xi+489 S. ISBN 978-0-8218-4479-3 H/b $ 75,–.

Dies ist ein eher unkonventionelles und anspruchsvolles Lehrbuch für einen "one-year course at the beginning graduate level". Der Titel zielt nicht in Richtung „Anschauung" oder einer a priori-Motivation der wesentlichen Begriffe, sondern bezieht sich auf den langsamen und teilweise redundanten Zugang. So wird z.B. in Kapitel 2 der Cauchysche Integralsatz für einige Spezialfälle hergeleitet; der allgemeine Beweis folgt später, und verschiedene Versionen werden formuliert. Ob damit ein tieferes Verständnis erreicht wird, ist jedoch nicht unmittelbar einsichtig.

Einige Highlights: Möbius-Transformationen werden gleich bei ihrer Einführung charakterisiert als die Automorphismen der Riemannschen Zahlenkugel $\mathbb{C}_\infty$ (basierend auf der Tatsache, dass jede holomorphe Funktionen von $\mathbb{C}_\infty$ nach $\mathbb{C}_\infty$ rational ist). Im Teil über konforme Abbildung finden sich Beweise des Satzes von Carathéodory über die Fortsetzung konformer Abbildungen sowie der Beweis des Riemannschen Abbildungssatzes; ein eigener Abschnitt ist der Eulerschen der Produktdarstellung für $\sin z$ gewidmet. Die Sätze von Runge und Mittag-Leffler werden ausführlich behandelt. Viel weiteres Material ist in Übungsaufgaben verpackt.

Speziellere Kapitel im zweiten Teil widmen sich unter anderem dem Zusammenhang zwischen dem Dirichlet-Problem und der Brownschen Bewegung, der Gammafunktion, der Konvergenz von Potenzreihen (Sätze von Abel, Tauber), und dem

Beweis der Picardschen Sätze. Man findet auch etliche weniger bekannte Resultate, wie z.B. eine Version der Cauchyschen Integralformel für nichtholomorphe Funktionen oder den Beweis der Hausdorff-Young-Ungleichung aus der Fourieranalysis. Sehr schön zum nachlesen, wieder entdecken und neu entdecken.

W. Auzinger (Wien)

Angewandte und numerische Mathematik

L. D. Faddeev, O. A. Yakubovskiĭ: Lectures on Quantum Mechanics for Mathematics Students. (Student Mathematical Library, Vol. 47.) American Mathematical Society, Providence, Rhode Island, 2009, xii+234 S. ISBN 978-0-8218-4699-5 H/b \$ 39,–.

This book is based on a famous course originally developed by the first author and then continued by the second one. Before the present translation these notes were only available in Russian. They give a very readable introduction to the subject with only minimal mathematical prerequisites and are thus well suited for undergraduate students. In particular, the authors focus on ideas rather than full mathematical rigor. However, in contradistinction to most physics texts, the mathematical problems are not entirely ignored. The topics covered are classical – from basic concepts like the algebra of observables to concrete examples like the hydrogen atom and scattering theory. My single complaint is the lack of exercises. Otherwise I can only say that I wished it had existed at my time as a student.

G. Teschl (Wien)

A. Koop, H. Moock: Lineare Optimierung – eine anwendungsorientierte Einführung in Operations Research. Spektrum Akademischer Verlag, Heidelberg, 2008, x+270 S. ISBN 978-3-8274-1897-5 P/b € 24,95.

Hervorgegangen aus einer Fachhochschulvorlesung mit dem Titel *Operations Research*, bietet das Buch eine übersichtliche Einführung in die lineare und ganzzahlige Optimierung. Nach Vorstellung einiger Problemtypen und des Gauß- bzw. Gauß-Jordan-Algorithmus wird die Simplexmethode zur Lösung linearer Optimierungsprobleme erläutert. Daran schließt ein Kapitel über Innere-Punkte-Verfahren (Methode von Dikin) an. Transportprobleme werden mittels des dualen Simplexverfahrens (Transportalgorithmus) gelöst. Danach werden kurz parametrische und ganzzahlige lineare Programme besprochen.

Nach diesem theoretisch-algorithmischen Teil werden zwei Fallstudien aus der Praxis vorgestellt. Je ein Kapitel ist der Besprechung der *Excel*-Solver bzw. von C-Programmen für den Simplex-Algorithmus und für Transportprobleme gewidmet. Auf 50 Seiten werden dann Lösungen zu den Übungsaufgaben diskutiert.

Die Darstellung ist elementar, aber klar und gut verständlich. Daher eignet sich dieses Buch gut zur Begleitung in einführenden Vorlesungen und zum Selbststudium.

R. Burkard (Graz)

S. T. Rachev (ed.): Handbook of Computational and Numerical Methods in Finance. Birkhäuser, Boston, Basel, Berlin, 2004, VII+435 S. ISBN 0-8176-3219-0 H/b € 97,90.

Dieses Buch ist eine Sammlung von zwölf Arbeiten über numerische Methoden in der Finanzmathematik, u.a. Monte Carlo-Methoden, Finite Differenzen-Methoden, Stochastische Portfolio-Optimierung, genetische Algorithmen und neuronale Netze. Neben einigen eher spezifisch ausgerichteten Kapiteln sind darunter auch einige Überblicksartikel über Teilgebiete dieses Bereichs. Der Titel "Handbook" des Bandes ist etwas irreführend, aber einige Kapitel geben einen guten Einblick in das jeweilige Themengebiet. Besonders hervorzuheben sind der Survey über Malliavin Calculus und der Survey über Quantisierungs-Methoden.

Es folgt eine Liste der einzelnen Kapitel: 1. Skewness and Kurtosis Trades (O. Blaskowitz, K. Härdle, P. Schmidt), 2. Valuation of a credit spread put option: the stable Paretian model with copulas (D. D'Souza, K. Amir-Atefi, B. Ratcheva-Jotova), 3. GARCH-Type processes in modelling energy prices (I. Khindanova, Z. Atakhanova, S. Rachev), 4. Malliavin calculus in finance (A. Kohatsu-Higa, M. Montero), 5. Bootstrap unit root tests for heavy-tailed time series (P. Kokoszka, A. Parfionovas), 6. Optimal portfolio selection and risk management (S. Ortobelli, S. Rachev, I. Huber, A. Biglova), 7. Optimal quantization methods and applications to numerical problems in finance (G. Pagès, H. Pham, J. Printems), 8. Numerical methods for stable modelling in financial risk management (S. Stoyanov, B. Ratcheva-Jotova), 9. Modern heuristics for finance problems (F. Schlottermann, D. Seese), 10. On relation between expected regret and conditional value-at-risk (C. Testuri, S. Urysaev), 11. Estimation, adjustment and application of transition matrices in credit risk models (S. Trueck, E. Oezturkmen), 12. Numerical analysis of stochastic differential systems and its applications in finance (Z. Zheng).

H. Albrecher (Lausanne)

U. Schäfer: Das lineare Komplementaritätsproblem. Eine Einführung. (Springer-Lehrbuch.) Springer, Berlin, Heidelberg, 2008, x+268 S. ISBN 978-3-540-79734-0 P/b € 26,95.

Lineare Komplementaritätsprobleme $LCP(q,M)$ sind Verallgemeinerungen von linearen und quadratischen Optimierungsproblemen. Sind ein Vektor q und eine quadratische Matrix M gegeben, so sucht das Problem $LCP(q,M)$ zwei nichtnegative, zueinander orthogonale Vektoren w und z mit $w = q + Mz$. In dieser einführenden Darstellung behandelt Schäfer zunächst eingehend den Lemke-Algorithmus zur Lösung linearer Komplementaritätsprobleme, der aber nicht immer eine Lösung findet. Daher werden Klassen von Matrizen betrachtet, die Aussagen über die Anwendbarkeit des Lemke-Algorithmus ermöglichen. Als Anwendungen werden Zwei-Personen Spiele, freie Randwertprobleme und u.a. amerikanische Put-Optionen vorgestellt. Danach werden iterative Lösungsverfahren und Innere-Punkte-Methoden zur Lösung von $LCP(q,M)$ beschrieben. Ein Kapitel über Fehlerschranken beschließt das Buch.

Eine Reihe von Übungsaufgaben trägt zum Erlernen des Stoffs bei. Ein umfangreiches Literaturverzeichnis verweist auf weiterführende Arbeiten. Das Buch ist klar geschrieben und sehr ansprechend gestaltet. Es ist zu wünschen, dass diese erste deutschsprachige Darstellung linearer Komplementaritätsprobleme viele Freunde findet.

R. Burkard (Graz)

Wahrscheinlichkeitstheorie und Statistik

D. Applebaum: Probability and Information. An Integrated Approach. Second Edition. Cambridge University Press, 2008, xvi+273 S. ISBN 978-0-521-72788-4 P/b £ 25,99*, ISBN 978-0-521-89904-8 H/b £ 65,–.

Das Buch ist eine sehr elementare Einführung in die Wahrscheinlichkeitstheorie mit ein paar eingeschobenen Kapiteln über Informationstheorie, in denen die Grundbegriffe dieses Gebiets, Entropie, Information, Kanalkapazität, Codes mit variabler Wortlänge und die Entropie von Markoffketten, beschrieben werden. Auch der der Wahrscheinlichkeitstheorie gewidmete Teil enthält nur die wesentlichsten Begriffe und Ergebnisse: ein wenig Kombinatorik, Zufallsvariable, Erwartungswert, Varianz, einige spezielle Verteilungen, bedingte Wahrscheinlichkeit, schwaches Gesetz der großen Zahlen, klassischer Grenzverteilungssatz , „bewiesen“mithilfe von Momentenerzeugenden, und ein Kapitel über Markoffketten. Insofern unterscheidet es sich nur wenig von etlichen anderen Büchern, die zu diesem Thema auf elementarem Niveau geschrieben wurden, und auch der Zugang zu den einzelnen Konzepten ist eher konventionell. Meiner Meinung nach beschränkt sich der Leserkreis, an den sich dieses Buch wendet, auf Studierende mit geringem mathematischen Hintergrund, die sich schnell einen Überblick über Wahrscheinlichkeitstheorie mit ihren Zusammenhängen zur Informationstheorie verschaffen wollen.

N. Kusolitsch (Wien)

N. Henze: Stochastik für Einsteiger. Eine Einführung in die faszinierende Welt des Zufalls. 7., überarbeitete und erweiterte Auflage. Mit über 200 Übungsaufgaben und Lösungen. Vieweg Verlag, Wiesbaden, 2008, x+362 S. ISBN 978-3-8348-0423-5 P/b € 22,90.

Dieses Buch ist als Einführung in die Stochastik primär für Lehrerinnen und Lehrer, ihre Schüler, für Studierende des Lehramts, aber auch für Quereinsteiger aus Industrie und Wirtschaft konzipiert. Es legt großen Wert auf die Motivation der Begriffsbildungen und versucht anhand zahlreicher Beispiele und Paradoxien, für eine geeignete stochastische Denkweise zu sensibilisieren. Neben vielen historischen Bemerkungen enthält jedes der 32 Kapitel Lernziele und Lernzielkontrollen sowie Übungsaufgaben inklusive Lösungen.

Der bereits in einer Besprechung einer früheren Auflage (s. IMN 189) erwähnte und vom Autor bewusst gewählte häufige Wechsel zwischen wortreichem Prosastil und Satz-Beweis-Schema macht die Lektüre an manchen Stellen vielleicht etwas mühsam, insgesamt bietet das Buch aber einen guten ersten Einblick in zahlreiche Themen der Wahrscheinlichkeitstheorie und Statistik. Gegenüber der 6. Auflage wurden u.a. stetige Verteilungen und einige Standardverfahren der Statistik hinzugefügt.

H. Albrecher (Lausanne)

J. Kohlas, P.-A. Monney: Statistical Information, Assumption-Based Statistical Inference. (Sigma Series in Stochastics, Vol. 3.) Heldermann Verlag, Lemgo, 2008, xii+170 S. ISBN 978-3-88538-303-1 P/b € 32,–.

Statistische Information ist die Grundlage aller statistischen Verfahren. Der Begriff ist sehr allgemein und umfasst sowohl stochastische Modelle als auch a-priori-Information. Die Monografie versucht die Gemeinsamkeit von Bayesschen und anderen Verfahren mittels sogenannter funktionaler Modelle zu erfassen. Diese beschreiben wie Beobachtungen als Funktion von unbekannten Parametern und stochastischen Störungen erzeugt werden. Dies wird zuerst für diskrete Modelle und im zweiten Abschnitt für kontinuierliche Modelle dargestellt. Das ist an sich nicht neu, jedoch wird eine vereinheitlichende Modellbildung versucht und analysiert, welche Aussagen über den Parameter, bedingt durch Daten, gemacht werden können. Die Autoren argumentieren, dass das Plausibilitätsprinzip nicht haltbar ist und beschreiben die Integration jeglicher Art von a-priori-Information, nicht nur solcher in Form von Wahrscheinlichkeitsverteilungen. Es werden Beziehungen zu verschiedenen Ungewissheitstheorien aufgezeigt und anhand von speziellen statistischen Experimenten konkretisiert. Der Band ist für jene, die an der Theorie der Statistik interessiert sind, lesenswert.

R. Viertl (Wien)

Einführungen

T. Arens, F. Hettlich, C. Karpfinger, U. Kockelkorn, K. Lichtenegger, H. Stachel: Mathematik. Spektrum Akademischer Verlag, Heidelberg, 2008, 2009, xiv+1496 S. ISBN 978-3-8274-1758-9 H/b € 69,95.

Ein sehr umfassendes, solides Buch, groß und schwer auch im Äußeren. Eine ideale Lektüre, die griffbereit am Schreibtisch zur Verfügung stehen sollte. Insgesamt gibt es 6 Teile (Einführung und Grundlagen, Analysis einer reellen Variablen, Lineare Algebra, Analysis mehrerer reeller Variablen, Höhere Analysis, Wahrscheinlichkeitsrechnung und Statistik) und diese sind wieder in insgesamt 41 Kapitel unterteilt.

Trotz der 1.496 Seiten kann dieses Werk natürlich nicht alle Aspekte in jedem Bereich vollständig berücksichtigen, da ist die Mathematik zu umfassend. Aber es ist erstaunlich viel enthalten und ein sehr umfassenden Niveau gewählt worden. Ich denke, dieses Buch ist einerseits sehr gut geeignet für Studierende der Mathematik und technischer Studien, aber durchaus auch für aktiv in der Mathematik tätige Personen.

G. Schranz-Kirlinger (Wien)

T. Arens, F. Hettlich, C. Karpfinger, U. Kockelkorn, K. Lichtenegger, H. Stachel: Arbeitsbuch Mathematik. Aufgaben, Hinweise, Lösungen und Lösungswege zu Arens et al., Mathematik. Spektrum Akademischer Verlag, Heidelberg, 2009, vii+683 S. ISBN 978-3-8274-2123-4 P/b € 34,95.

Zahlreiche Beispiele, gegliedert in Kapitel, entsprechend dem zugehörigen Hauptwerk. Zur leichteren Handhabung wäre es allerdings nützlich gewesen auch im Arbeitsbuch jeweils die Überschriften der Kapitel anzugeben. Die Aufgaben sind unterteilt in Verständnisfragen, Rechenaufgaben und Anwendungsprobleme. Es gibt zu zahlreichen Beispielen Hinweise und danach teilweise recht ausführliche Lösungen, manchmal auch nur die Resultate. Die Aufgaben sind mit •, •• oder ••• je nach Schwierigkeitsgrad gekennzeichnet.

Insgesamt eine sehr gute Sammluung von nützlichen Beispielen aus nahezu allen Teilgebieten der Mathematik.

G. Schranz-Kirlinger (Wien)

T. Arens, F. Hettlich, C. Karpfinger, U. Kockelkorn, K. Lichtenegger, H. Stachel: Ergänzungen und Vertiefungen zu Arens et al., Mathematik. Spektrum Akademischer Verlag, Heidelberg, 2009, iv+242 S. ISBN 978-3-8274-2124-1 P/b € 19,95.

Zum Hintergrund: Das umfangreiche Werk von T. Arens et al., „Mathematik“, ist im Spektrum-Verlag im Jahr 2008 erschienen und bietet auf knapp 1.500 Seiten ein Kompendium der „gesamten“ (sic!) für Anwender relevanten Mathematik. Es hat einerseits den Charakter eines Lehrbuchs zu den Themen (Kapiteln) „Einführung und Grundlagen“, „Analysis einer reellen Variablen“, „Lineare Algebra“, „Analysis mehrerer reeller Variablen“, „Höhere Analysis“ sowie „Wahrscheinlichkeitsrechnung und Statistik“. Aufgrund seines inhaltlichen Umfanges und der extrem übersichtlich aufbereiteten Darstellung eignet es sich auch hervorragend als Begleiter, zum Nachlesen und Nachschlagen. Auf der Website *http://www.matheweb.de* finden sich Zusatzmaterialien zu den einzelnen Kapiteln, Lösungen zu den Übungsaufgaben, etc.

Der hier vorliegende Ergänzungsband enthält Bonusmaterial zu einzelnen Kapiteln, das auch im *PDF*-Format online abgerufen werden kann. Inhaltliche Schwerpunkte finden sich in den Bereichen Lineare Algebra, Vektoranalysis, Funktionalanalysis und insbesondere der Statistik. Die Art der Darstellung folgt dem bewährten Muster des Hauptbands.

W. Auzinger (Wien)

H. Pruscha, D. Rost: Mathematik für Naturwissenschaftler. Methoden, Anwendungen, Programmcodes. (Springer-Lehrbuch.) Springer, Berlin, Heidelberg, 2008, xii+337 S. ISBN 978-3-540-79736-4 P/b € 24,95.

Es war Absicht der Autoren, eine kompakte einbändige Darstellung zu verfassen, die den wichtigsten Stoff für die angesprochene Zielgruppe enthält. Die einzelnen Kapitel widmen sich den Themen Rechnen mit Zahlen, Folgen und Reihen, Funktionen, ein- und mehrdimensionale Differentialrechnung, eindimensionale Integration, komplexe Zahlen, Fourierreihen, Vektor- und Matrizenrechnung, mehrdimensionale Differentialrechnung, bis hin zur Wahrscheinlichkeitsrechnung und Statistik. Es handelt sich jeweils um relevanten „Kernstoff“, der sinnvoll und pragmatisch ausgewählt ist.

Als vorlesungsbegleitende Unterlage und zum Selbststudium ist das Buch sicherlich gut geeignet. Naturgemäß fallen viele relevante Themen under den Tisch, wie etwa mehrdimensionale Integration, Vektoranalysis, Normalformen für Matrizen, etc. Differentialgleichungen werden nur kurz angesprochen.

Als begleitendes Material enthält das Buch etliche kurze Programmcodes in Maple und R, Lösungen zu den Übungsaufgaben sind im *pdf*-Format verfügbar unter *http://www.math.lmu.de/∼mfn/*.

W. Auzinger (Wien)

C. W. Turtur: Prüfungstrainer Mathematik. Klausur- und Übungsaufgaben mit vollständigen Musterlösungen. 2., überarbeitete und erweiterte Auflage. Teubner Verlag, Wiesbaden, 2008, 600 S. ISBN 978-3-8351-0211-8 P/b € 29,90.

Zu all den folgenden Themen finden sind in diesem Buch zahlreiche gelöste Beispiele: Mengenlehre, Elementarmathematik, Aussagenlogik, Geometrie und Vektorrechnung, Lineare Algebra, Differentialrechnung, Integralrechnung, Komplexe Zahlen, Funktionen mehrerer Variablen und Vektoranalysis, Wahrscheinlichkeitsrechnung und Statistik, Folgen und Reihen, Gewöhnliche Differentialgleichungen, Funktionaltransformationen.

Eine sehr nützliche und ansprechende Sammlung für Studierende, aber auch für Lehrende.

G. Schranz-Kirlinger (Wien)

Nachrichten der Österreichischen Mathematischen Gesellschaft

Bezug von Jahresbericht und Semesterberichten der DMV durch ÖMG-Mitglieder

Durch eine Vereinbarung mit der Deutschen Mathematikervereinigung und den entsprechenden Verlagen ist es möglich, den Mitgliedern der Österreichischen Mathematischen Gesellschaft sowohl den *Jahresbericht der Deutschen Mathematikervereinigung* als auch die *Mathematischen Semesterberichte* zu einem günstigen Preis anzubieten. Die Preise pro Jahr und Zeitschrift sind € 23,50 (2010) € 24,– (2011) € 24,50 (2012) € 25,– (2013).

Falls Sie eine oder beide dieser Zeitschriften beziehen möchten, werden Sie gebeten, gemeinsam mit Ihrem Mitgliedsbeitrag für die ÖMG den entsprechenden Betrag einzuzahlen und den Zahlungszweck auf dem vorgedruckten Erlagschein durch Ankreuzen anzugeben. Der Versand erfolgt direkt durch den Verlag.

Die Aktion des automatischen Bezugs der *Mitteilungen der Deutschen Mathematikervereinigung* für Mitglieder im Inland wird fortgeführt.

Brief des Vorsitzenden

Sehr geehrte Damen und Herren!

Nunmehr geht meine Amtszeit als Vorsitzender der Österreichischen Mathematischen Gesellschaft zu Ende. In dieser spannenden Zeit ist viel Erfreuliches geschehen. Ich denke hier nur an die Erfolge von österreichischen Mathematikern bei Berufungsverfahren im Ausland oder bei der Einwerbung großer Drittmittelprojekte beim FWF und anderer Förderinstitutionen bzw. bei der Vergabe von START- und Wittgensteinpreisen. In meiner Amtszeit hat die ÖMG auch zwei Kongresse veranstaltet, nämlich 2007 gemeinsam mit den slowakischen Kollegen und 2009 in Graz gemeinsam mit der Deutschen Mathematikervereinigung. Insbesondere der große Grazer Kongress hat die Vielfalt und Leistungsfähigkeit der österreichischen Mathematik eindrucksvoll unter Beweis gestellt und ich möchte allen Teilnehmerinnen und Teilnehmern für ihr Engagement danken. Natürlich gibt es auch schwierige Problemzonen im Bereich der Mathematik, die noch einer Lösung harren. Insbesondere möchte ich hier das Thema „Mathematik an höheren

Schulen“ bzw. „Zentralmatura“ ansprechen. Hier wird auch in Zukunft noch viel Argumentationsarbeit nötig sein und ich hoffe, dass sich die Österreichische Mathematische Gesellschaft wie bisher oder noch stärker in diesen Prozess einbringt. Man sollte nie aus den Augen verlieren, dass der Stellenwert der Mathematik auch von seiner Positionierung als Unterrichtsfach an den Höheren Schulen abhängt. Darüber hinaus muss die ÖMG auch andere Aspekte der Mathematik vertreten, nämlich einerseits stets auf ihre Bedeutung als Werkzeug für Natur-, Ingenieur- und Wirtschaftswissenschaften hinweisen (Mathematik kann sogar als Schlüsseltechnologie in diesem Zusammenhang gesehen werden), aber gleichzeitig auch betonen, dass die Mathematik ein wesentlicher Bestandteil unseres Kulturguts ist. Ich gehe davon aus, dass alle diese Aspekte der Mathematik auch vom zukünftigen Vorstand vertreten werden und bin sehr optimistisch, dass auf die österreichische Mathematik eine positive Weiterentwicklung zukommt. Allen Kolleginnen und Kollegen, mit denen ich im Rahmen der ÖMG in den letzten Jahren zusammenarbeiten konnte, möchte ich auf diesem Wege meinen ausdrücklichen Dank aussprechen.

Robert Tichy (Vorsitzender der ÖMG)

Protokoll der Generalversammlung der ÖMG

Zeit: Dienstag, 22. September 2009, 18:30–20:15

Ort: Hörsaal BE01, TU Graz, Steyrergasse 30

Tagesordnung:

1. Feststellung der Beschlussfähigkeit
2. Berichte des Vorsitzenden und weiterer Vorstandsmitglieder, insbesondere des Kassiers
3. Berichte aus den Landessektionen
4. Bericht der Rechnungsprüfer und gegebenenfalls Entlastung des Vorstandes
5. Neuwahl des Vorstandes
6. Verleihung des Förderungspreises, der Studien- und Schülerpreise und einer Ehrenmitgliedschaft
7. Allfälliges

TOP 1: Tichy begrüßt die Anwesenden (ca. 35) und stellt die Beschlussfähigkeit fest.

TOP 2: Mitgliederentwicklung: In diesem Jahr gab es erfreulicherweise ca. 25 Neueintritte. Acht Mitglieder sind ausgeschieden, vier davon durch Ableben; ihrer wird kurz gedacht.

Tichy berichtet von Gesprächen im Zuge der Tagung mit Ministerialrat Weselka und Lokalpolitikern bezüglich der Lehramtsausbildung im UF Mathematik. Insbesondere stehen viele Pensionierungen im Schulbereich bevor, ein möglicher Lehrermangel ist absehbar.

Schlöglmann scheidet aufgrund seiner Pensionierung als Vorsitzender der Didaktikkommission aus und zieht ein Resümee. Momentan gibt es zwei heiße Themen im Schulbereich: die Restrukturierung der Lehrerausbildung (Zuständigkeit Pädagogische Hochschulen versus Universitäten) und die zentrale Matura, die 2014 an den AHS und 2015 an den BHS starten soll. Schlöglmann beklagt das rasche Tempo, in dem die Reformen durchgeführt werden sollen. Erfahrungen aus anderen Ländern sind nur schwer umlegbar, da Österreich im Gegensatz ein hochdifferenziertes Oberstufensystem hat.

Tichy dankt Schlöglmann für seine langjährige Arbeit und berichtet, dass Prof. Humenberger (Univ. Wien) zu seinem Nachfolger gewählt wurde. Zusätzlich sollen folgende Personen in die Didaktikkommission aufgenommen werden: Dr. Anita Dorfmayr (Univ. Wien), Prof. Werner Peschek (Univ. Klagenfurt), Min.Rat Mag. Dr. Peter Schüller, Mag. Dr. Stefan Siller, Landesschulinspektor Mag. Helmut Zeiler. Die Generalversamlung stimmt diesen Änderungen zu.

Tichy berichtet von einem gemeinsamen Mittagessen der Vorstände der ÖMG und der DMV. Der nächste gemeinsame Kongress findet 2013 in Innsbruck statt. Bezüglich des Versands der DMV-Mitteilungen an ÖMG-Mitglieder wurde für die kommenden 3 Jahre ein Fixpreis von € 3.000 für die ÖMG vereinbart. Weiters macht die DMV das Angebot, den Jahresbericht der DMV um € 23 pro Exemplar für ÖMG-Mitglieder verfügbar zu machen. Die Generalversammlung beschließt, das Angebot anzunehmen und es in den IMN zu bewerben.

Larcher präsentiert die Finanzentwicklung der ÖMG im Jahr 2008.

TOP 3: Innsbruck: Ostermann berichtet über Öffentlichkeitsarbeit an Volksschulen und Volkshochschulen und über eine Sommerschule für Schülerinnen und Schüler, die gemeinsam mit der Universität Wien organisiert wurde. Die Studierendenzahlen stagnieren.

Salzburg: Hellekalek berichtet, dass sich das Institut momentan im Umbruch befindet. Es war eine Professur für Stochastik ausgeschrieben. Nach der Absage des Listenersten wird nun mit dem zweiten verhandelt. Demnächst wird eine Professur für diskrete Mathematik ausgeschrieben.

Klagenfurt: Kautschitsch berichtet von einer Veranstaltung für SchülerInnen (Talentecamp) und Einzelvorträgen. Auch in Klagenfurt gibt es in den nächsten Jahren einige Pensionierungen und Neuausschreibungen.

Linz: Larcher berichtet von einer „Projektwoche angewandte Mathematik“ und dem Johannes-Kepler-Symposium.

Graz: Woess dankt dem Vorsitzenden des Organisationskomitees (Heuberger) der

Tagung in Graz für seinen Einsatz und berichtet von aktuellen und bevorstehenden Professorenbesetzungen an der MU Leoben, Univ. Graz und TU Graz.

TOP 4: Feichtinger berichtet, dass bei der Rechnungsprüfung keine Unregelmäßigkeiten festgestellt wurden und beantragt die Entlastung des Vorstandes. Dem Antrag wird zugestimmt.

TOP 6: Ehrenmitgliedschaft: Tichy berichtet, dass gemäß dem neuen Prozedere bezüglich der Verleihung der Ehrenmitgliedschaft sowohl Beirat als auch Vorstand einstimmig der Verleihung der Ehrenmitgliedschaft an Prof. Peter M. Gruber zugestimmt haben. Es sollen damit sowohl seine wissenschaftlichen Leistungen als auch sein Engagement für die ÖMG gewürdigt werden.

Die Schülerpreise werden am Freitag im Rahmen der ÖMG/DMV-Tagung vergeben: Es gab 27 Einreichungen von Fachbereichsarbeiten. Sieben Arbeiten wurden ausgewählt und am Freitag vorgestellt und prämiert.

Die heurigen Studienpreise gehen an Mag. Katrin Grunert für ihre Diplomarbeit "Long-time asymptotics for the KdV Equation" bei Gerald Teschl (Univ. Wien) und an Dr. Christoph Aistleitner für seine Dissertation "Investigations in Metric Discrepancy Theory" bei István Berkes (TU Graz).

Der Förderungspreis ergeht an Alois Panholzer (TU Wien). M. Drmota hält eine Laudatio.

TOP 5: Es wird vorgeschlagen, M. Drmota zum Vorsitzenden zu wählen. Die Abstimmung erfolgt geheim und fällt einstimmig zugunsten Drmotas aus. Die Wahl des restlichen Vorstandes erfolgt per Akklamation.

Stellvertretender Vorsitzender: Oberguggenberger
Schriftführer: Lamel
Stellvertretender Schriftführer: Ostermann
Kassier: Larcher
Stellvertretender Kassier: Kirschenhofer
Herausgeber IMN: Wallner
Beauftragte für Frauenförderung: Schranz-Kirlinger
Beauftragter für Öffentlichkeitsarbeit: Teschl

TOP 7: Tichy dankt für die konstruktive Zusammenarbeit.

Vorsitz: R. Tichy Schriftführerin: I. Fischer

Laudatio auf Peter Gruber anlässlich der Verleihung der Ehrenmitgliedschaft

Peter Gruber wurde im Jahre 1941 in Klagenfurt geboren. Nach seiner Schulausbildung in Kärnten inskribierte er an der Universität Wien und promovierte dort im Hauptfach Mathematik mit einer Dissertation zur Geometrie der Zahlen (Betreuer: N. Hofreiter) im Jahr 1964. Anschließend war er Assistent am Institut von W. Nöbauer an der TU Wien, wo er sich auch im Jahr 1970 habilitierte. Im Jahr 1971 wurde Peter Gruber zum Ordinarius an der Universität Linz ernannt und im Jahr 1976 schließlich als Nachfolger von Hans Hornich an die TU Wien zurückberufen. Für sein bisheriges Wirken erhielt Peter Gruber zahlreiche in- und ausländische Auszeichnungen, etwa die Ehrendoktorate der Universitäten Siegen und Turin. Im Jahr 1985 wurde er zum Ehrenmitglied der Akademie von Modena gewählt, im Jahr 1991 zum wirklichen Mitglied der österreichischen Akademie der Wissenschaften.

Peter Gruber ist nun seit über 30 Jahren äußerst erfolgreich an der TU Wien tätig. Er hat eine international weithin sichtbare Schule im Bereich der Konvexgeometrie aufgebaut und dieses Gebiet selbst durch mehr als 100 wissenschaftliche Arbeiten bereichert. Dabei ist sein Interesse vielfältig: Frühe Arbeiten beschäftigen sich etwa mit Geometrie der Zahlen oder mit geometrischen Charakterisierungen von Ellipsoiden, später interessierten ihn topologische Bezüge (wie z.B. Metriken im Raum der konvexen Körper oder Bairesche Sätze). Auch Approximationsfragen im Zusammenhang mit konvexen Körpern waren ihm ein Anliegen. Niemals hat er sich für „leichte“ Probleme interessiert, sondern er hat sich stets den gerade anstehenden „schweren“ Fragestellungen in seinem Arbeitsgebiet zugewandt. Beeindruckend sind auch die Bücher, die Peter Gruber publiziert hat. Hier sind besonders *Geometry of Numbers* (gemeinsam mit Lekkerkerker), und das kürzlich erschienene Werk *Convex and Discrete Geometry* zu erwähnen. Erstgenanntes ist inzwischen zu einem Standardwerk geworden. Letzteres wird sicherlich ein solches werden, und man findet eine ausführliche Würdigung und Besprechung in diesem IMN-Heft durch Rolf Schneider. Es war Peter Gruber auch stets ein Anliegen, sein Arbeitsgebiet und die Mathematik im Allgemeinen durch die Organisation von Kolloquien, Tagungen und Konferenzen zu fördern. Regelmäßig veranstaltete er „Minikolloquien“ zur Konvexgeometrie, die unter der Schirmherrschaft der ÖMG standen und sein Arbeitsgebiet nachhaltig beeinflusst haben. Es gelang ihm auch immer wieder, sehr prominente Mathematiker nach Österreich einzulanden, ich denke hier etwa an F. Hirzebruch, P. Erdős, R. Remmert, J. Dieudonné, L. Ahlfors, H. Zassenhaus u.a. Besonders gefördert hat Peter Gruber die österreichische Mathematik als ÖMG-Vorsitzender in den Jahren 1978–1982.

Daher ist es mir eine besondere Freude, dass Vorstand, Beirat und Generalversammlung der ÖMG einhellig beschlossen haben, die Ehrenmitgliedschaft an Peter Gruber zu verleihen.

R. Tichy (Graz)

Laudatio auf Alois Panholzer, Förderungspreisträger der Österreichischen Mathematischen Gesellschaft 2009

Es freut mich sehr, dass ich hier die Laudatio für den diesjährigen Förderungspreisträger Alois Panholzer halten kann. Ich kenne ihn schon seit über 12 Jahren, wir arbeiten seit vielen Jahren gemeinsam an der TU Wien und unsere Arbeitsgebiete sind sehr eng verwandt.

Ich möchte einleitend kurz auf seine Biographie eingehen. Alois Panholzer wurde 1971 in Linz geboren und wuchs in St. Martin im Mühlkreis auf, wo er Volks- und Hauptschule absolvierte. Daraufhin besuchte er die Chemie-HTL in Wels und begann 1991 das Studium der Technischen Mathematik an der TU Wien, das er 1995 mit dem Diplom und 1997 mit seiner von Helmut Prodinger betreuten Dissertation „Untersuchungen zur durchschnittlichen Gestalt gewisser Baumfamilien. Mit besonderer Berücksichtigung von Anwendungen in der Informatik“ mit Auszeichnung abschloss. Seine Dissertation wurde übrigens 1998 mit dem Dissertationspreis der ÖMG ausgezeichnet.

Anschließend begann sein beruflicher Werdegang als Projektassistent in einem von Helmut Prodinger geleiteten FWF-Projekt. Von 1999–2000 war er Vertragsassistent an der Universität Innsbruck. Ab März 2000 arbeitete er dann als Universitätsassistent an der TU Wien, wo er sich im Jahr 2002 für das Fach „Diskrete Mathematik“ habilitierte und seither dort als außerordentlicher Univ.prof. wirkt, mehrfach unterbrochen durch längere Forschungsaufenthalte in fast allen Erdteile.

Neben dieser intensiven wissenschaftlichen Arbeit widmet er so viel Zeit wie möglich seiner Familie und seiner nicht-wissenschaftlichen Leidenschaft, dem Bergsteigen – einer nicht selten anzutreffenden Eigenschaft des Homo Mathematicus Austriacus.

Nun möchte ich ein wenig auf seine wissenschaftlichen Leistungen eingehen. Sein Arbeitsgebiet lässt sich als „Mathematische Analyse von Algorithmen und Datenstrukturen“ charakterisieren, wobei hier eine sehr feine Analyse angestrebt wird, die weit über eine O-Aufwandsabschätzung hinausgeht. Er wurde hier wesentlich durch seinen früheren Dissertationsbetreuer Helmut Prodinger und die Schule von Philippe Flajolet beeinflusst. Sein spezielles Interesse ist es, Verteilungseigenschaften von gewissen Parametern – wie z.B. der Aufwand eines Algorithmus – unter Zugrundelegung eines geeigneten Wahrscheinlichkeitsmodells asymptotisch zu charakterisieren. Dabei werden Methoden der Kombinatorik, der asymptotischen Analysis und der Wahrscheinlichkeitstheorie miteinander verknüpft.

Ich möchte zur Illustration pars pro toto auf eine für mich beeindruckende Arbeit näher eingehen, nämlich auf die fast 50seitige Arbeit “Multiple Quickselect”, die 2003 in der Zeitschrift *Theoretical Computer Science* erschienen ist. Sie beschäftigt sich mit der erwarteten Anzahl von Vergleichen in gewissen Quickselect-Varianten. Es wird gezeigt, dass dieser Erwartungswert immer asymptotisch proportional zur Anzahl n der vorhandenen Daten ist. Das ist zwar nicht überraschend, aber die Schwierigkeit liegt darin, die Proprotionalitätskonstante in einer entsprechenden Form explizit anzugeben. Dies gelingt Alois Panholzer in einer bemerkenswerten Kombination von Methoden. Zunächst wird das Problem mittels erzeugender Funktionen in eine inhomogene Differentialgleichung Eulerschen Typs übersetzt. Anschließend gelingt es, mithilfe deren Lösung die gesuchten Koeffizienten prinzipiell asymptotisch abzulesen. Mit hohem Geschick im Umgang mit der Umformung kombinatorischer Summen, u.a. mit Identitäten für Schurfunktionen und Stirlingzahlen und mit Einsatz des Zeilbergerschen Algorithmus, gelingt es schließlich, eine handhabbare Formel explizit anzugeben.

Insgesamt hat Alois Panholzer etwa 50 wissenschaftliche Arbeiten publiziert. Die Wahl der Zeitschriften spiegelt seine wissenschaftlichen Interessen und seine wissenschaftliche Breite wider. Darunter finden sich neben kombinatorischen Zeitschriften wie *Journal of Combinatorial Theory*, *SIAM Journal on Discrete Mathematics*, *Discrete Applied Mathematics*, *European Journal of Combinatorics*, *Annals of Combinatorics*, Zeitschriften, die der Informatik zuzuordnen sind, wie *Algorithmica*, *Theoretical Computer Science*, *Journal of Algorithms*, *Journal of Automata, Languages and Combinatorics*, *Discrete Mathematics and Theoretical Computer Science*, wahrscheinlichkeitstheoretische Zeitschriften wie *The Annals of Applied Probability*, *Random Structures and Algorithms*, *Combinatorics, Probability and Computing*, aber auch allgemeinere Zeitschriften wie *Advances in Applied Mathematics* und *Quaestiones Mathematicae*. Zahlreiche referierte Tagungsbeiträge ergänzen dieses Bild.

Alois Panholzer hat bereits einige Forschungsprojekte eingeworben; derzeit ist er Projektleiter im Nationalen Forschungsnetzwerk des FWF, „Analytische Kombinatorik und Probabilistische Zahlentheorie", er leitet ein bilaterales Projekt mit der UPC Barcelona und ist an einem EU-Projekt beteiligt.

Ich hoffe, ich habe durch meine Ausführungen einen kleinen Einblick in die Arbeit von Alois Panholzer geben können. Allein aus der großen Anzahl seiner Arbeiten erkennt man seinen außerordentlichen Fleiß. Dieser ist aber gepaart mit einem guten Geschmack für interessante Probleme, die er mit großem Geschick und vielseitigen Techniken zu lösen weiß. Er arbeitet – nicht nur im wissenschaftlichen Bereich – äußerst gewissenhaft, verlässlich und konzentriert. Als Institutsvorstand gesprochen: So einen Mitarbeiter kann man sich nur wünschen. Es zeichnet ihn darüber hinaus aus, dass er seine Leistungen und Kenntnisse bescheiden verbirgt als sie zeitgeistgemäß zu vermarkten. Umso mehr freut es mich, dass er diesjähriger Preisträger der ÖMG ist.

Lieber Alois! Ich gratuliere dir ganz herzlich zu diesem Preis und wünsche dir weiterhin alles Gute und viel Erfolg!

M. Drmota (TU Wien)

Schülerpreis für herausragende Fachbereichsarbeiten in Mathematik oder Darstellender Geometrie

Dieses Jahr wurde der Schülerpreis der ÖMG, der einige Jahre nicht ausgeschrieben wurde, auf Initiative von Landesschulinspektor Mag. Wolfgang Wurm wiederbelebt und die Ausschreibung vom Bundesministerium für Unterricht, Kunst und Kultur mit einem Bekanntgabeerlass unterstützt.

Insgesamt wurden 27 Fachbereichsarbeiten aus ganz Österreich eingereicht. Eine von der ÖMG eingesetzte Jury hat sechs dieser Arbeiten ausgewählt, deren Verfasser eingeladen wurden, ihre Arbeit am 25. September 2009 im Rahmen des *Tags für Lehrerinnen und Lehrer* beim ÖMG+DMV-Kongress in Graz in einer Kurzpräsentation vorzustellen:

- *Alexander Bors*, Erzherzog-Johann BORG Bad Aussee: Die Funktion, die ins Komplexe ging. (Betreuer: Mag. Harald Gerstgrasser).
- *Melanie Graf*, Gymnasium und Realgymnasium Wien 12: Mandelbrotmenge oder die Mathematik hinter dem Apfelmännchen (Betreuerin: Mag. Heidemarie Warnung).
- *Michael Kalcher*, BRG Graz Petersgasse: Kryptographie – eine Annäherung (Betreuerin: Mag. Johann Knaß).
- *David Nadlinger*, Bundesrealgymnasium Linz: Mathematische Grundlagen der 3D-Graphik. (Betreuer: Mag. Herbert Lenz).
- *Katharia Ölsböck*, Bundesgymnasium und Bundesrealgymnasium Tulln: Einführung in die Fuzzy-Logic (Betreuerin: Dr. Anita Dorfmayr).
- *Juraj Raic*, BRG Graz Petersgasse: Pfadgenerierung eines omnidirektionalen Roboters mit Swedish Wheels mittels Freiformkurventechnik (Betreuer: Mag. Rudolf Neuwirt).

Abbildung 1: Die Schülerpreisträger des Jahres 2009: Alexander Bors, David Nadlinger, Katharina Ölsböck, Michael Kalcher, Melanie Graf, Juraj Raic. Foto: H. Bors.

Die durchwegs gelungenen Präsentationen wurden von der Jury (Michael Drmota, Christian Schmeiser, Wolfgang Wurm, Rudolf Zoufal) beurteilt und es wurde entschieden, drei Kategorien von Preisen vergeben: Alexander Bors und David Nadlinger erhielten einen 1. Preis, Katharina Ölsböck und Michael Kalcher einen 2. Preis und Melanie Graf und Juraj Raic einen 3. Preis.

Hervorzuheben und äußerst erfreulich ist der Umstand, dass nicht nur die Schülerpreise der ausgezeichneten Arbeiten, sondern durchwegs alle eingereichten Schülerarbeiten von bemerkenswert hoher Qualität waren. Die ÖMG wird diesen Preis in den kommenden Jahren sicher wieder ausschreiben.

Michael Drmota (TU Wien, Vorsitzender der Schülerpreisjury)

Neue Mitglieder

Michael Vertneg, DI. – Striag.15, 1140 Wien, Österreich. geb. 1959. 1979 bis 1984 Studium Technische Mathematik, TU Wien, 1984 bis 2003 Steuerberater (1988), Wirtschaftsprüfer (1992) und Geschäftsführer (1996) bei Auditor Treuhand GmbH. Seit 2002 Partner und Geschäftsführer bei Deloitte Österreich. email *mvertneg@deloitte.at*.

Daniel Perz, – Berlinerring 24, 8047 Graz, Österreich. Schüler. geb. 1992. Schüler des BG/BRG Lichtenfelsgasse, 2006 Sieger des Anfängerwettbewerbs Steiermark, 2009 Preisträger des Bundeswettbewerbs. email *dape0506@hotmail.com*.

Ausschreibung der ÖMG-Schülerpreise 2010

Die Österreichische Mathematische Gesellschaft zeichnet herausragende Fachbereichsarbeiten in Mathematik oder Darstellender Geometrie mit Preisen aus.

Diese Arbeiten müssen bis Ende Mai 2010 in der ÖMG (Univ.Prof. Dr. Michael Drmota, Technische Universität Wien, Wiedner Hauptstraße 8–10/104, 1040 Wien) einlangen und werden von einer Jury begutachtet.

Die Verfasserinnen und Verfasser jener Arbeiten, die im Zuge dieser Begutachtung in die engere Wahl kommen, werden zu einem Kurzvortrag eingeladen, in dem sie ihre Arbeit präsentieren. Diese Präsentation, zu der auch die betreuenden Lehrerinnen und Lehrer eingeladen sind, wird voraussichtlich im September 2010 stattfinden. Ort und Termin werden noch bekannt gegeben. Anschließend erfolgt im Rahmen einer Feier die Preisverleihung.

Die ÖMG bittet alle ihre Mitglieder und die Leserinnen und Leser der IMN, potentielle Interessenten von dieser Einladung zu informieren und Schulen zur Teilnahme zu ermuntern.

Robert F. Tichy (Vorsitzender der ÖMG)

Adresse für Einsendungen:
Univ.Prof. Dr. Michael Drmota
Technische Universität Wien
Wiedner Hauptstraße 8–10/104
1040 Wien

Ausschreibung der ÖMG-Studienpreise 2010

Die Österreichische Mathematische Gesellschaft vergibt auch 2010 wieder zwei Studienpreise. Die Preisträger sollen junge Mathematikerinnen und Mathematiker sein, die in den Jahren 2008 oder 2009 eine Diplomarbeit bzw. eine Dissertation eingereicht haben.

Voraussetzung für den Studienpreis für Diplomarbeiten ist ein Abschluss eines Magister- oder Diplomstudiums an einer österreichischen Universität. Voraussetzung für den Studienpreis für Dissertationen ist entweder der Abschluss des Doktoratsstudiums an einer österreichischen Universität oder, im Falle eines Doktoratsstudiums an einer ausländischen Universität, das Vorliegen eines abgeschlossenen Magister- oder Diplomstudiums an einer österreichischen Universität. Die Nominierung muss durch einen zum Zeitpunkt der Nominierung in Österreich an einer Universität oder Forschungseinrichtung beschäftigten Mathematiker bzw. Mathematikerin erfolgen.

Der Vorschlag muss bis spätestens 15. März 2010 beim Vorsitzenden der ÖMG einlangen und folgende Unterlagen enthalten:

1. Ein Exemplar der als besonders hoch qualifiziert bewerteten mathematischen Diplomarbeit bzw. Dissertation;
2. zwei begründete Bewertungen dieser Diplomarbeit bzw. Dissertation;
3. einen Lebenslauf des Kandidaten bzw. der Kandidatin einschließlich kurzer Beschreibung des Studienablaufs.

Aus den eingereichten Vorschlägen werden durch eine vom Vorstand der ÖMG eingesetzte Begutachtungskommission die Preisträger ermittelt. Jeder ÖMG-Studienpreis ist mit 500 € dotiert. Jeder Preisträger erhält eine Urkunde.

Sollte der Preisträger oder die Preisträgerin noch nicht Mitglied der ÖMG sein, so wird sie (er) auf Wunsch in die ÖMG aufgenommen und vom Mitgliedsbeitrag für das erste Jahr befreit.

Robert F. Tichy (Vorsitzender der ÖMG)

Adresse für Einsendungen:
Univ.Prof. Dr. Michael Drmota
Technische Universität Wien
Wiedner Hauptstraße 8–10/104
1040 Wien

Ausschreibung des ÖMG-Förderungspreises 2010

Die Österreichische Mathematische Gesellschaft vergibt auch 2010 wieder ihren jährlichen Förderungspreis. Infrage kommen junge Mathematiker oder Mathematikerinnen, die in überdurchschnittlichem Maße durch ihre mathematische Forschung hervorgetreten sind. Ein wesentlicher Teil der Arbeiten muss in Österreich erbracht worden sein.

Die Nominierung muss durch einen zum Zeitpunkt der Nominierung in Österreich an einer Universität oder Forschungseinrichtung beschäftigten habilitierten Mathematiker bzw. Mathematikerin erfolgen.

Der Vorschlag muss bis spätestens 15. März 2010 beim Vorsitzenden der ÖMG einlangen und folgende Unterlagen enthalten:

1. Beschreibung und Wertung der wissenschaftlichen Leistung;
2. Publikationsliste;
3. wissenschaftlicher Lebenslauf.

Aus den eingereichten Vorschlägen wählt eine Begutachtungskommission den Preisträger oder die Preisträgerin aus. Der Preis ist mit 1.000 € und einer Ehrenmedaille dotiert. Außerdem wird der Preisträger oder die Preisträgerin eingeladen, beim nächsten ÖMG-Kongress in einem Vortrag über die erzielten Forschungsergebnisse zu berichten.

Sollte der Preisträger oder die Preisträgerin noch nicht Mitglied der ÖMG sein, so wird er oder sie auf Wunsch in die ÖMG aufgenommen und vom Mitgliedsbeitrag für das erste Jahr befreit.

Robert F. Tichy (Vorsitzender der ÖMG)

Adresse für Einsendungen:
Univ.Prof. Dr. Michael Drmota
Technische Universität Wien
Wiedner Hauptstraße 8–10/104
1040 Wien