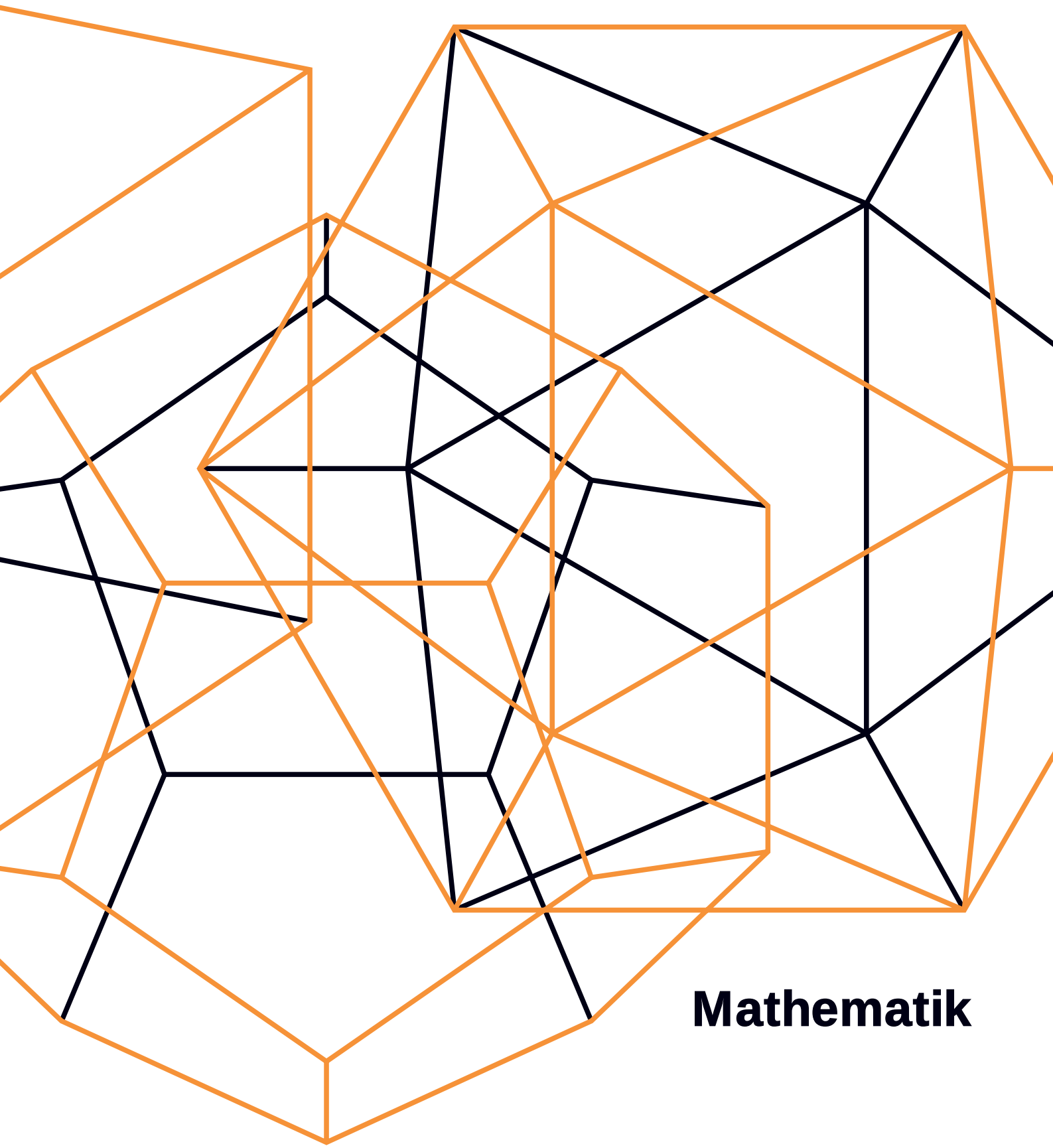
UNI NOVA

Wissenschaftsmagazin der Universität Basel 87 Juni 2000



Mathematik

Bisher erschienene uni nova-Ausgaben mit Themenschwerpunkten (einzelne Ausgaben sind noch erhältlich)

uni nova 68/93 April
Die Bibliothek

uni nova 69/93 November
Erdwissenschaften/Mikroskopie

uni nova 70/94 Februar
Kultur-/Geisteswissenschaften

uni nova 71/94 Juni
Internationalisierung des Rechts

uni nova 72/94 November
Nanowissenschaften – Nanotechnologie

uni nova 73/95 März
Strukturen in Raum und Zeit

uni nova 74/95 Juni
Altern

uni nova 75/96 Februar
Pflanzenvielfalt – Pflanzenschutz

uni nova 76/96 Juni
Frauen und Männer

uni nova 77/96 November
Angewandte Ökonomie

uni nova 78/97 Februar
Astronomie

uni nova 79/80 Mai 1997
Adolf Portmann – Zum 100. Geburtstag

uni nova 81 April 1998
Molekulare Biologie – Molekulare Medizin

uni nova 82 September 1998
Geographie

uni nova 83 Dezember 1998
Wissenschaft Theologie

uni nova 84 April 1999
Region Basel – Ein Thema für die Wissenschaft

uni nova 85 Juli 1999
Afrika in Basel – Basel in Afrika

uni nova 86 November 1999
Altertumswissenschaften

uni nova 87 Juni 2000
Mathematik

Impressum

uni nova,
Wissenschaftsmagazin der Universität Basel
herausgegeben von der Stelle für Öffentlichkeitsarbeit
Redaktion:
Ulla Fringeli, Beat Münch
Korrektorin:
Karin Müller
Gestaltung:
Saumer & Zürcher, Graphic Design, Basel
Fotolithos: M^{C} HighEnd, Basel
Druck: Kreis Druck AG, Basel
uni nova wird gedruckt auf Papier aus 50% Recyclingfasern und 50% Zellstoff.

Adresse: uni nova, Postfach, 4003 Basel
Telefon: 061 267 30 15, Telefax: 061 267 30 13
Internet: http:/www.unibas.ch/

Liebe Leserin, lieber Leser

Mathematik ist eine Sprache, die es erlaubt, über hochgradig komplexe Sachverhalte aus verschiedensten Bereichen menschlichen Forschens effizient zu sprechen. Wird der Verständlichkeit zuliebe die mathematische durch die Umgangssprache ersetzt, so lässt sich wohl einiges über die Sachverhalte und über die mathematische Denkweise sagen, aber der Kern der Sache geht verloren. Diese Tatsache erklärt die Scheu der Mathematik, sich als Disziplin vor einem allgemeinen Publikum zu präsentieren. Gleichzeitig empfindet man das Fehlen der Mathematik in der öffentlichen Diskussion als Mangel. Auch unter den Mathematikerinnen und Mathematikern wird ein zunehmendes Interesse spürbar, ihre Wissenschaft einem aufgeschlossenen Publikum begreifbar zu machen.

Um etwas über Mathematik mitteilen zu können, haben die Autorinnen und Autoren des Mathematischen Instituts unserer Universität für diese Ausgabe der uni nova Themen teils aus der Geschichte, teils aus den Anwendungsbereichen der Mathematik ausgewählt. So zeigt sich, dass die Mathematik mit einem Bein in der Kulturgeschichte verankert ist und mit dem andern Bein im Alltagsleben steht. Diese Auswahl soll den Zugang und das Verständnis erleichtern. Die aktuellen Forschungstätigkeiten des Instituts zu präsentieren, ist hier nicht das Hauptanliegen, sie treten dabei nur bedingt in Erscheinung.

Die Planung dieser Ausgabe fiel zusammen mit der Proklamierung des Jahres 2000 als «World Mathematical Year» durch die International Mathematical Union und die UNESCO. In zahlreichen Veranstaltungen und Konferenzen stellt sich die Mathematik als aktuelle Wissenschaft und Bestandteil des weltweiten Kulturgutes vor.

Die Tatsache, dass an der Basler Universität dieses Jahr der Ostrowski-Preis verliehen wird, und die Beachtung des 300. Geburtstages von Daniel Bernoulli durch Vorträge und eine Ausstellung im Kollegienhaus der Universität, unterstützen ebenfalls die Bemühungen, Mathematik einem breiteren interessierten Publikum zugänglich zu machen (so erschien der Katalog zur Ausstellung «300 Jahre Daniel Bernoulli» in Form einer Gratis-Zeitung.).

Die Basler Mathematikerinnen und Mathematiker schrieben ihre Beiträge für eine interessierte Leserschaft, um ihr einen Einblick in die Mathematik zu geben und somit dem Vorurteil «Mathematik verstehe ich nicht» entgegenzutreten.

Die Redaktion dankt vor allem Professor Hans-Christoph Im Hof für seine Beratung und seinen grossen Einsatz beim Entstehen dieser Ausgabe.

Für die Redaktion
Ulla Fringeli

Inhalt

Achilles und die Schildkröte: Ein Dialog über Kreise und Kugeln, Elektrostatik und Kapillarflächen

Wolfgang Reichel

Dies ist der Versuch, die Ergebnisse einer mathematischen Doktorarbeit auszugsweise einem interessierten, aber fachlich nicht geschulten Publikum zugänglich zu machen. Dass dies nicht leicht ist, merkt jeder, der einen solchen Versuch unternimmt.

Im Folgenden lassen wir den griechischen Helden Achilles und eine mit ihm befreundete Schildkröte einen Dialog führen. Die Idee, Achilles, den Schnellfüssigsten der Sterblichen, und die Schildkröte, die Schwerfälligste der Schwerfälligen, sprechen zu lassen, geht auf Douglas R. Hofstadter zurück. In seinem 1979 erschienenen Buch *Gödel, Escher, Bach – ein endloses geflochtenes Band* führt er diese Dialoge zur Perfektion. Hofstadter seinerseits wurde von Lewis Carrolls *What the Tortoise said to Achilles* aus dem Jahr 1895 inspiriert. Den Wettkampf zwischen Achilles und der Schildkröte schuf Zeno von Elea, ein griechischer Erfinder von Paradoxen aus dem 5. Jahrhundert v. Chr. Zeno lässt die beiden einen Wettkampf über eine festgelegte Strecke von, sagen wir, der Länge eines Stadions austragen. Als grossmütiger Held gewährt Achilles der Schildkröte einen Vorsprung von zwanzig Schritten. Nach dem Startsignal ersprintet Achilles in wenigen Sekunden die Zwanzig-Schritt-Marke, den Startpunkt der Schildkröte. Diese kroch inzwischen einen Schritt vorwärts, und auch diesen Schritt durcheilt Achilles im Bruchteil einer Sekunde. Dort angekommen ist ihm die Schildkröte allerdings wieder ein winziges Stückchen voraus. Führt man Zenos gedankliche Einteilung der Aufholjagd weiter, so erhält man eine unendliche Folge von Zeitschritten, zu denen Achilles den Ort erreicht, den die Schildkröte beim vorherigen Zeitschritt gerade verlassen hat. Für Zeno von Elea stand damit fest, dass entgegen aller Erfahrung Achilles die Schildkröte nie einholen wird, und er schloss daraus, dass Bewegung reine Illusion ist. Zeno wusste nicht, dass die Summe dieser unendlich vielen Zeitschritte endlich ist und Achilles deshalb – wie erwartet – die Schildkröte in endlicher Zeit einholt.

Treten wir also ein wenig zur Seite und beobachten Achilles und die mit ihm befreundete Schildkröte auf dem Nachhauseweg am Ende eines langen Wettkampftages. Darüber, dass beide auf dem Gebiet der angewandten Mathematik sehr bewandert sind und über Kenntnisse aus der fernen Zukunft verfügen, machen wir uns an dieser Stelle keine Gedanken. Achilles beginnt den Dialog mit den Lieblingsgegenständen griechischer Geometrie:

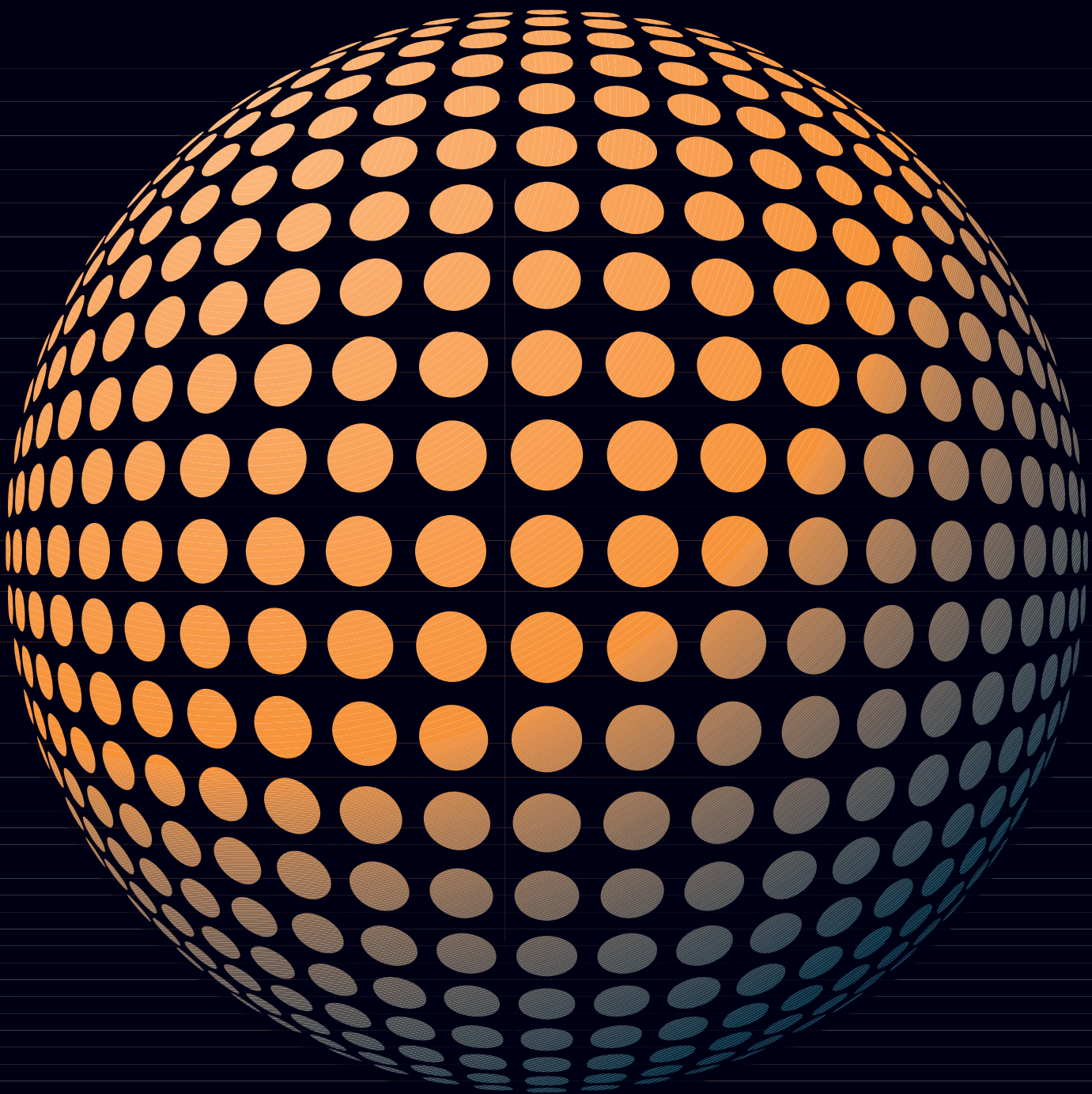
Achilles: Aufs Neue ist mir klar geworden, dass die von uns Griechen so verehrte Form des Kreises und der Kugel die erhabenste und vollkommenste unter allen geometrischen Formen ist.

Schildkröte: Ich bin gespannt, Neues zu erfahren.

A: Stell dir einmal vor, die metallische Oberfläche einer hohlen Kugel ist mit einer bestimmten elektrischen Ladungsmenge aufgeladen worden. Die elementaren Ladungen, die Elektronen, sind auf der Kugeloberfläche frei beweglich. Sie stossen sich auch gegenseitig ab. Deswegen versuchen sie, so weit wie möglich voneinander entfernt zu sein, um gemeinsam einen Zustand kleinster gespeicherter Energie einzunehmen. Da sie aber die Kugeloberfläche nicht verlassen können, verteilen sie sich völlig gleichmässig auf der Kugeloberfläche. Damit hält jedes Elektron den grösstmöglichen Abstand zu allen benachbarten Elektronen. Idealisiert betrachtet, und das fällt uns Griechen leicht, ist an jedem Punkt der Oberfläche die Ladungsdichte die gleiche. Ist das nicht eine wunderbare Eigenschaft der Kugel?

S: Ja, das ist sehr schön. Aber ehrlich gesagt beeindruckt mich das kaum, denn wieso soll nur die Kugel diese schöne Eigenschaft haben und nicht auch andere Körper?

A: Ich verstehe nicht, worauf du mit deiner Frage hinaus willst.



S: Könnte es denn nicht sein, dass sich die Ladungen, die man auf irgendeine andere metallische Oberfläche gebracht hat, ebenfalls so gleichmässig verteilen, dass die Ladungsdichte überall die gleiche ist? Dann wäre die Kugel gar nichts Besonderes und ihr Griechen müsstet euch fragen, warum sie euch so viel bedeutet.

A: Beim Zeus – wie soll denn so etwas möglich sein! Und wie um alles in der Welt würde ein solch eigenartiger Körper denn aussehen? Wenn man die Kugel nur ein wenig verformt, so können doch die Ladungen nicht mehr völlig gleichmässig verteilt sein, oder?

S: Nun, mein lieber Freund, das sind Mutmassungen, aber kein Beweis. Dennoch kann ich dich und die griechische Welt beruhigen. Unter allen Körpern mit glatter Oberfläche ist tatsächlich die Kugel der einzige Körper, der diese gleichmässige Verteilungseigenschaft besitzt.

A: Ich wusste es doch. Auf Kugeln kann man sich verlassen. Sie haben einfach die schönsten und perfektesten Symmetrien, die man sich vorstellen kann. Du solltest einmal den Beitrag *Symmetrie in Schulalltag und Theorie* in dieser uni nova-Ausgabe lesen.

S: Oh – da sei aber mal vorsichtig, lieber Achilles. Du magst zwar Kugeln mühelos meterweit durch die Luft schleudern können …

A: Nicht nur Kugeln, auch Speere und den Diskus. Und Rennen, Hoch- und Weitspringen sind meine weiteren Stärken.

S: Ja, ja – und trotzdem holst du mich nie ein. Spass bei Seite. Als wissenschaftlich denkender Mensch müsste dir klar sein, dass es durchaus vernünftig ist zu fragen, ob nicht auch andere Körper die gleichmässige Verteilungseigenschaft haben. Kurzum – man muss der Sache auf den Grund gehen und beweisen, dass eben nur Kugeln diese Eigenschaft zukommt. Tatsächlich wird im Jahre 1995 einem Mathematiker – nennen wir ihn Symmetrikos – in seiner an den Universitäten Karlsruhe und Basel angefertigten Doktorarbeit dieser Beweis gelingen. In seiner Arbeit wird er sich mit der Untersuchung überbestimmter Randwertaufgaben beschäftigen.

A: Überbestimmter was?

S: Randwertaufgaben. Dies sind Aufgaben, bei denen man Lösungen von Gleichungen sucht, die ein Naturgesetz ausdrücken.

A: Schon Pythagoras wusste: «Alles ist Zahl».

S: Ihr Griechen habt eben immer das erste Wort. Zurück zu den Randwertaufgaben. Mehr darüber kannst du in dem Beitrag *Die Mathematik als moderne Weltsprache: Am Beispiel der Differenzialgleichungen* in dieser uni nova-Ausgabe erfahren. Meistens reichen diese Gleichungen allerdings nicht aus, um einen physikalischen Zustand zu beschreiben. Deshalb fordert man zusätzlich, dass die Lösungen – in unserem Fall das elektrische Potential der Ladungsverteilung – auf der Oberfläche des betrachteten Körpers bestimmte vorgegebene Werte annehmen. Die Oberfläche eines Körpers bezeichnet man im mathematischen Jargon gerne auch als Rand – und daher kommt der Name Randwertaufgabe.

A: Und was ist daran überbestimmt?

S: Auf der Oberfläche eines Körpers verteilen sich elektrische Ladungen nach dem Prinzip der «kleinsten Energie» (vielleicht möchtest du mehr zu diesem Minimalitätsprinzip in dem Artikel *Die Variationsrechnung und ihre Basler Ursprünge* in dieser uni nova-Ausgabe lesen). Nach den physikalischen Gesetzen der Elektrostatik bedeutet dies, dass das zugehörige Potential auf der Körperoberfläche überall denselben Wert annehmen muss. Hätte nämlich das Potential an zwei verschiedenen Punkten der Oberfläche unterschiedliche Werte, so würde ein Strom fliessen und die Potentialdifferenz wieder ausgleichen.

A: Ich folge dir …

S: Versuche, dir nun einmal einen Körper mit der gleichmässigen Verteilungseigenschaft vorzustellen. Ausser der Konstanz des Potentials auf der Oberfläche fordern wir gleichzeitig, dass die Ladungsdichte in jedem Punkt der Oberfläche dieselbe ist. Damit haben wir dem Potential zu viel zugemutet. Im Allgemeinen kann es beide Forderungen nicht erfüllen – ausser natürlich für den Fall, dass unser Körper eine Kugel ist. Gerade der Umstand, dass wir im Allgemeinen zu viel fordern – das Problem also überbestimmen –, lässt sich nutzen, um zu beweisen, dass unser Körper eine Kugel sein muss.

A: Ich bin beeindruckt.

S: Dazu hast du allen Grund. Und du kannst auch ein bisschen stolz auf euch Griechen sein, denn genau betrachtet haben die griechischen Mathematiker ein wenig zu diesem Ergebnis beigetragen.

A: Wie ist das denn möglich?

S: Mathematik ist eine Wissenschaft, in der ein Ergebnis auf dem anderen aufbaut. Jede Generation von Mathematikern verwendet Ergebnisse der vorherigen. Denn die Erkenntnisse gelten für alle Zeiten und an allen Orten, weil sie aus logischen Schlussfolgerungen bestehen. Wenn man die Regeln der Logik versteht und anerkennt, kann man zu jeder Zeit auch einen vielleicht vor Jahrhunderten oder Jahrtausenden gefundenen Beweis nachvollziehen.

A: Und was haben die griechischen Mathematiker nun mit unserem Symmetrikos zu tun?

S: Wie gesagt, er wird im Jahr 1995 einen Beweis für unser Ladungsproblem geben. Und er wird zahlreiche Ideen anderer Mathematiker verwenden. Etwa eine Idee aus dem Jahr 1971 von James Serrin aus den Vereinigten Staaten von Amerika. Und dieser wird wiederum Ideen eines russischen Mathematikers namens Alexander Danilowitsch Alexandroff aus dem Jahr 1962 verwendet haben.

A: Ich sehe immer noch nicht, an welcher Stelle wir Griechen ins Spiel kommen.

S: Serrin und Alexandroff werden bedeutende Arbeiten über geometrische Fragestellungen verfassen. Und in der Geometrie seid ihr Griechen ja bekanntlich grosse Meister. Man bedenke nur den Beitrag *Die wahre Geometrie oder denkbare Geometrien* in dieser uni nova-Ausgabe.

A: Eben. Und grosse Sportler sind wir auch. Man bedenke nur die olympischen Spiele, den Marathon …

Die Konversation gleitet auf andere Bahnen. Ein Weilchen später machen die beiden eine Pause und erfrischen sich an einem Brunnen, wobei sie den Dialog über Kreise und Kugeln wieder aufnehmen:

A: Lass mich auf unser Kugelproblem zurückkommen. Gibt es denn noch andere schöne Eigenschaften, die ausschliesslich Kugeln und Kreisen zukommen?

S: Oh ja – dutzende. Zum Beispiel die isoperimetrische Eigenschaft: Unter allen Körpern gleichen Volumens hat die Kugel die kleinste Oberfläche.

A: Donnerwetter.

S: Oder diese: Unter allen glatten Körpern haben nur Kugeln überall auf ihrer Oberfläche konstante mittlere Krümmung. Dies wird übrigens der vorher erwähnte russische Mathematiker Alexandroff beweisen und dabei ganz nebenbei eine schöne, nach ihm benannte allgemeine Methode entwickeln.

A: Gib es auch Charakterisierungen von Kreisen?

S: Sicher – zum Beispiel die folgende: Unter allen eingespannten Membranen mit gleicher Grundfläche erzeugt genau die kreisförmige Membran den tiefsten Grundton. Aber es gibt noch weitere Charakterisierungen von Kreisen, die wiederum mit den überbestimmten Randwertaufgaben zu tun haben. Ich will dir eine davon zeigen. Dazu giessen wir Wasser in dieses Becken.

Glücklicherweise befindet sich ein grosses Waschbecken beim Rastplatz.

S: (zieht eine Kapillare aus ihrem Gepäck) Wir nehmen nun dieses Glasröhrchen mit kreisförmigem Querschnitt …

A: Mit ähnlich dünnen Strohhalmen trinken die eleganten Damen und Herren in Athen ihre kühlen Getränke.

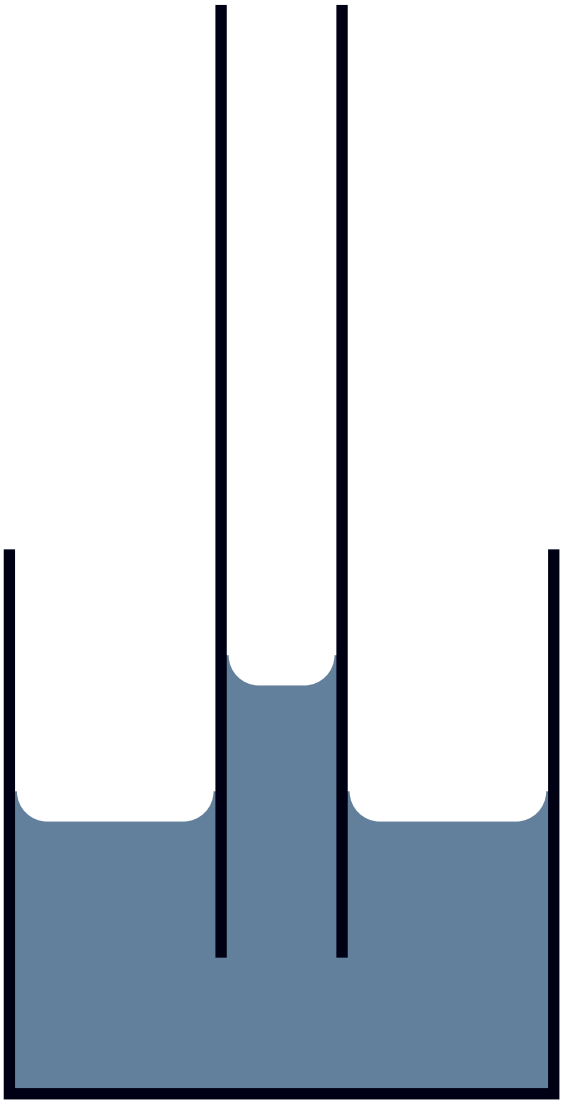
S: Genau – allerdings ist unser Röhrchen aus Glas. Dieses Röhrchen tauchen wir jetzt etwa bis zur Hälfte senkrecht in das Wasser dieses Beckens. Was siehst du?

A: Nichts Besonderes.

S: Du musst schon genauer hinsehen.

A: Nun, der Wasserspiegel im Röhrchen scheint etwas höher zu sein als der im Becken.

S: Richtig. Und an der Wand des Röhrchens ist er wiederum höher als in der Mitte des Röhrchens, richtig?



A: Ja. Es ist, als ob die Wasseroberfläche im Röhrchen zum Rande hin hochgebogen ist. Warum wohl?

S: In späteren Jahrhunderten wird man dies den Kapillaritätseffekt nennen und ihn damit erklären, dass die molekularen Kräfte zwischen den Atomen eines Wassermoleküls und den Atomen des Glases grösser sind als zwischen den Atomen zweier Wassermoleküle. Daher «reisst» die Glaswand das Wasser am Rande hoch, und aufgrund der Oberflächenspannung des Wassers folgt der Wasserspiegel in der Mitte des Röhrchens etwas nach. Wenn man spekuliert, wie dieser Effekt von der Krümmung der Glaswand abhängen könnte, so wird man vermuten, dass – grob gesagt – das Wasser dort am höchsten steigt, wo die Krümmung der Glaswand am stärksten ist. Und nun denk daran, dass unser Röhrchen einen kreisförmigen, das heisst also einen Querschnitt mit konstanter Krümmung hat.

A: Ah – ich weiss. Man kann es gut erkennen. Überall am Rande ist das Wasser gleich hoch gestiegen. Hab ich Recht?

S: Vollkommen. Wieder eine dieser schönen Eigenschaften des Kreises. Und nun ...

A: Lass mich raten. Du möchtest wissen, ob auch Röhrchen mit anderen, nicht kreisförmigen Querschnitten diese Eigenschaft haben können?

S: So ist es. Und genau wie vorhin beim Ladungsproblem ist die Antwort: Nein. Nur bei Röhrchen mit kreisförmigem Querschnitt tritt dieses Phänomen auf.

A: Fantastisch – wer wird das entdecken?

S: Das lässt sich nicht genau sagen. Ich glaube, dass es alle Forscher, die sich mit diesen Kapillarflächen beschäftigen, wohl ahnen. Einen mathematischen Beweis, dass es so sein muss, wird allerdings erst der bereits genannte James Serrin im Jahr 1971 liefern.

A: Es scheint, dass der Symmetrikos dem neuesten Stand der Forschung etwas hinterherhinkt?

S: Dafür wird ihm aber etwas Verwandtes gelingen. Stell dir vor, wir tauchen anstelle eines Röhrchens einen massiven Glasstab senkrecht in das Becken. Nun kann kein Wasser in den Stab hinein, denn er ist ja massiv. Aber an der Aussenwand des Stabes tritt wieder der Kapillaritätseffekt auf – allerdings ist er weniger stark ausgeprägt und man kann ihn nicht so schön beobachten. Wir müssen auch sicherstellen, dass unser Becken so gross ist, dass nicht der Kapillaritätseffekt zwischen dem Wasser und der Wand des Beckens unser Experiment beeinflusst. Hat unser Stab nun kreisförmigen Querschnitt …

A: … so steigt das Wasser überall an der Aussenwand des Stabes gleich hoch.

S: Und diese Eigenschaft kommt wieder nur ausschliesslich dem Glasstab mit Kreisquerschnitt zu. Wie du dir bestimmt denken kannst, haben das äussere Kapillaritätsproblem und das Ladungsproblem eine Gemeinsamkeit. Unserem Symmetrikos wird es gelingen, beide Probleme so abstrakt zu formulieren, dass diese Gemeinsamkeiten zu Tage treten. Dazu ist die Mathematik als «Sprache» bestens geeignet. Rein mathematisch gesehen, sind die beiden Probleme nur Spezialfälle einer ganzen Klasse von allgemeineren überbestimmten Randwertaufgaben. Eine der erstaunlichsten Errungenschaften der mathematischen Denkweise ist, mit einem einzigen Beweis eine Vielzahl von Problemen auf einmal zu lösen.

Der gemeinsame Weg von Achilles und der Schildkröte neigt sich dem Ende zu.

A: Wir sind beinahe zu Hause. Ich möchte Dir noch eine Frage stellen. Gibt es denn auch technische Anwendungen für diese Charakterisierungen von Kreisen und Kugeln?

S: Das ist ja nun eine ganz und gar ungriechische Frage, die man in der Zukunft bei der Vergabe von Forschungsmitteln immer häufiger den Mathematikern stellen wird. Aber sie ist berechtigt – so schön auch der erkenntnistheoretische Wert der Forschung sein mag. Um die Frage zu beantworten, lass uns das Ladungsproblem und das Kapillaritätsproblem unter dem Aspekt betrachten, dass sie den zugrunde liegenden Körper eindeutig charakterisieren. Und damit beschreiten wir ein weites Feld der Mathematik, das noch in den Kinderschuhen steckt. Dazu gehört, dass es zum Beispiel wünschenswert wäre, auch andere einfache geometrische Gebilde wie Ellipsen, Rechtecke, Ellipsoide und Quader so charakterisieren zu können wie Kreise und Kugeln. Diese Fragestellungen treten oft in der folgenden Form auf: Lässt sich eine geometrische Form dadurch rekonstruieren, dass man die durch den Körper durchgehenden oder von ihm reflektierten elektromagnetischen oder akustischen Wellen misst? Dieses Prinzip der Tomographie werden sich am Ende des zwanzigsten Jahrhunderts die Ärzte zunutze machen, um ihren Patienten in den Bauch zu schauen und ihnen ihre Organe, ihren Herzschlag und ihre ungeborenen Kinder sichtbar zu machen.

A: Das klingt phantastischer als das Orakel von Delphi!

S: Kein schlechter Vergleich, lieber Freund. Tatsächlich wird die Mathematik leider sehr oft die Aura des unerreichbaren, geheimnisumwitterten Kultes an sich haben.

A: Lass mich zusammenfassen: Die Ergebnisse und Methoden der mathematischen Gegenwartsforschung legen also die Grundlagen für die Anwendungen der Zukunft. So wie die griechischen Geometer die Grundlage für Alexandroff sind, der wiederum Serrin inspirieren wird, welcher seinerseits die Ideen unseres Symmetrikos auslösen wird.

S: Und da eine gute Idee im Laufe der Zeit von mehreren Forschern aufgegriffen wird, gewinnt dieses Prinzip nach zweieinhalb Jahrtausenden eine beachtliche Dynamik.

A: Liebe Schildkröte – ich bin beeindruckt. Wer hätte gedacht, wie stark die Mathematik einst unser Weltbild gestalten wird.

S: Die Mathematik produziert selten schnelle, gewinnträchtige Erfolge. Die Ergebnisse entstehen langsam und so gut wie nie im Licht des öffentlichen Interesses. Aber sie bestehen für die Ewigkeit.

Gekürzte und bearbeitete Fassung einer Arbeit, die 1997 mit dem Klaus-Tschira-Preis für verständliche Wissenschaft an der Universität Karlsruhe ausgezeichnet wurde.

Dr. Wolfgang Reichel ist seit 1998 Assistent am Mathematischen Institut.
Er arbeitet auf dem Gebiet der partiellen Differenzialgleichungen.

Die Mathematik als moderne Weltsprache: Am Beispiel der Differenzialgleichungen

Catherine Bandle

Es ist für Natur- und Geisteswissenschaftler einfach zu erklären, womit sie sich beschäftigen. Die einen untersuchen die Materie und die andern die Schöpfungen des menschlichen Geistes. Viel schwieriger zu beantworten ist diese Frage für einen Mathematiker oder eine Mathematikerin. Die Mathematik befasst sich mit Strukturen *in abstracto*, unabhängig von der Dinglichkeit ihrer Objekte. Physiker, Populationsbiologen, Ökonomen können die gleiche Mathematik benützen. Im Alltag wird sie meistens nur indirekt über ihre Anwendungen wahrgenommen. Unser Kreditkartenwesen, die CD und die Computertomographie wären ohne hoch entwickelte Rechenverfahren unmöglich.

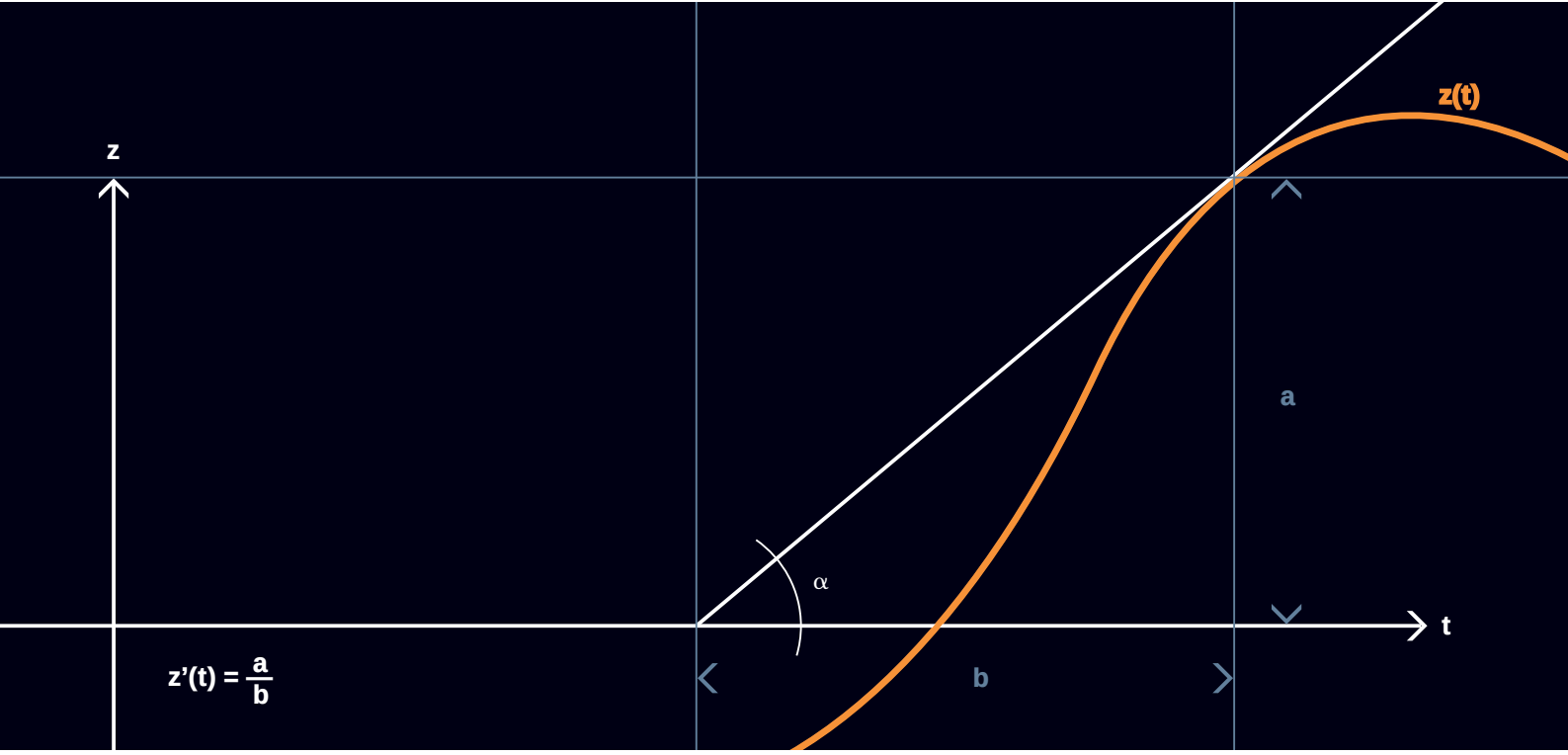
Die Mathematisierung der Wissenschaften ist eines der Merkmale unserer Zeit. Viele WissenschaftlerInnen kennen und gebrauchen die Mathematik in erster Linie als Sprache. Für *Galileo Galilei* (1564–1642) war sie «das Alphabet, mit dessen Hilfe Gott die Welt geschaffen hat». Sie ist in der Lage, Informationen zu komprimieren und ihre Komplexität zu reduzieren. Der Wandel im Verhältnis zwischen Mathematik und Anwendungen geht einher mit der rasanten Entwicklung der Computertechnik. Anstelle kostspieliger Experimente tritt das mathematische Modell, häufig in Form von Differenzialgleichungen.

Ursprünge

Das Studium der Differenzialgleichungen geht auf das 17. Jahrhundert zurück, die Zeit in der die Infinitesimalrechnung und die Newtonsche Mechanik erfunden wurden. Mit dem Begriff der Funktion, das heisst einer Vorschrift, die vorgegebenen Variablen eine Zahl zuordnet (in vielen Fällen durch eine Kurve veranschaulicht) und ihrer Ableitung (Steigung der Kurve) wurde es möglich, die Geschwindigkeit und die Beschleunigung einer Masse, sowie zeitliche Wachstumsraten von Bevölkerungsdichten oder Vermögenswerten zu formulieren.

Das Trägheitsgesetz «*Kraft = Masse · Beschleunigung*» kann als Gleichung $mz''(t) = K(t,z(t),z'(t))$ geschrieben werden, wobei m die Masse, $z(t)$ die Bahn zur Zeit t, $z'(t)$ die Beschleunigung des Körpers darstellen. Wenn in den Gleichungen Ableitungen vorkommen, spricht man von *Differenzialgleichungen*.

Als in der Folgezeit die Physik einfacher deformierbarer Körper untersucht wurde, war man gezwungen, Funktionen mehrerer Variablen einzuführen. Die Temperatur beispielsweise ist eine Funktion der Zeit und des Ortes. Gleichungen, die Funktionen mehrerer Variablen und Ableitungen nach all diesen Variablen enthalten, nennt man *partielle Differenzialgleichungen*.



Entwicklung im 20. Jahrhundert

Die ersten partiellen Differenzialgleichungen finden sich in den Arbeiten von Euler (1734). 1746 leitete d'Alembert die Gleichung der schwingenden Saite her, die heute noch benützt wird.

In seiner prophetischen Arbeit «Sur les équations aux dérivées partielles de la physique mathématique» (1890) stellt *H. Poincaré* eine Liste von partiellen Differenzialgleichungen auf, die er sowohl für die Entwicklung der Theorie der Differenzialgleichungen und für das Verständnis der mathematischen Modelle als auch für die Analysis (Theorie der Funktionen) für wichtig hielt. Die Liste umfasste klassische Gleichungen aus der Elektro-, Thermo-, Hydrodynamik und der Optik. Poincaré stellte fest, dass sie trotz unterschiedlichster Herkunft Ähnlichkeiten besitzen («un air de famille») und dass sie deshalb auch gemeinsame Eigenschaften haben sollten. Obwohl sie nur annäherungsweise reale Vorgänge darstellten und ihre physikalische Herleitung zum Teil unsorgfältig war, verlangte er, dass sie mathematisch mit derselben Genauigkeit und Strenge behandelt werden, wie dies seit 1870 unter dem Einfluss der Weierstrass'schen Schule in andern Bereichen der Mathematik üblich war.

Diese Haltung hat sich bis heute bewährt. Sogar Goethe, der in der Regel ein etwas gebrochenes Verhältnis zur Mathematik hatte, lobte sie: «Diese Bedächtigkeit, nur das Nächste ans Nächste zu reihen, oder vielmehr, das Nächste aus dem Nächsten zu folgern, haben wir von den Mathematikern zu lernen, und selbst da, wo wir uns keiner Rechnung bedienen, müssen wir immer so zu Werke gehen, als wenn wir dem strengsten Geometer Rechenschaft zu geben schuldig wären.»

Unter den 23 Problemen, die Hilbert im Jahre 1900 am Internationalen Mathematiker-Kongress in Paris stellte, befassten sich zwei mit partiellen Differenzialgleichungen. Eines betraf die Glattheit und das andere die Existenz ihrer Lösungen. Hilbert interessierte sich vor allem für diejenigen Gleichungen, die von *Variationsproblemen* stammen. Damit wurde die Agenda des 20. Jahrhunderts festgelegt. IhreAuswirkungen erstreckten sich von der Analysis bis zur Geometrie. Dank der Entwicklung der Funktionalanalysis wurde es möglich, Theorien zu entwickeln, mit denen die Hilbertschen Fragen für grosse Klassen von partiellen Differenzialgleichungen beantwortet werden konnten.

Typisch für das Studium der Differenzialgleichungen ist, dass es sich im Spannungsfeld zwischen den Forderungen der Anwender, die möglichst schnell konkrete Lösungen haben möchten, und den MathematikerInnen, die gerne und oft lieber nach den inneren Zusammenhängen forschen, befindet. Diese Herausforderung war für seine Entwicklung förderlich.

In den letzten Jahren begann sich das Selbstverständnis der Mathematik wieder zu wandeln. Es spielen zunehmend konstruktive Gesichtspunkte eine Rolle. Anforderungen von aussen sind: gute Modelle und zuverlässige Aussagen über ihr qualitatives und quantitatives Verhalten.

Reaktions-Diffusionsgleichungen

Ein typisches Beispiel einer partiellen Differenzialgleichung ist die Wärmeleitungs- oder Reaktions-Diffusionsgleichung. Sie beschreibt das *Erhaltungsprinzip* einer physikalischen Grösse.

$u_t(x,t) = \Delta u(x,t) + f(x,t,u(x,t),\nabla u(x,t))$

In Worten bedeutet diese Gleichung:

Reaktion = Diffusion + Quellterm

Ob die Grösse $u(x,t)$ die Temperatur eines Körpers am Ort x und zur Zeit t oder eine Bevölkerungsdichte darstellt, ist irrelevant. Wichtig ist nur, dass sie demselben Gesetz genügt, nämlich: Die Produktionsrate pro Zeiteinheit setzt sich aus den Teilchen, die in den Ort x diffundieren, und solchen, die von einer Quelle erzeugt werden, zusammen. Die Quellergiebigkeit f ist in der Regel neben dem Ort und der Zeit auch von der jeweiligen Temperatur und von der Konvektion abhängig. Dies ist vor allem bei chemischen Reaktionen der Fall. Die präzise Form der Funktion f hängt vom Modell ab und lässt einen grossen Spielraum an Möglichkeiten zu.

Welche Probleme stellen sich in diesem Zusammenhang an die Mathematik?

Sie lassen sich grob in drei Klassen aufteilen:

– Diagnostik
– Voraussage
– Kontrolle

a) Hat die Gleichung eine Lösung? Unter welchen zusätzlichen Vorgaben, wie zum Beispiel Kenntnis des Anfangsstadiums, ist sie eindeutig? Die Antwort ist insofern schwierig, als die Lösungen nicht explizit, sondern nur näherungsweise berechnet werden können. Es zeigt sich, dass bei vorgegebener Temperatur auf dem Rand des Gefässes die Lösung für jede Anfangstemperatur eindeutig bestimmt ist. Diese Aussage beruht auf dem Minimumprinzip, welches für alle Körper unabhängig von ihrer Geometrie gültig ist. Es besagt, dass bei einer positiven Quelle (Heizung) das Minimum am Anfang des Prozesses oder auf dem Rand des Körpers angenommen wird. Dies entspricht unseren Erfahrungen. Der kühlste Ort in einem geheizten Zimmer ist an der Wand oder in dem Zeitpunkt, in dem man das Zimmer betritt. Eine feinere Analyse zeigt ferner, dass die Ausbreitungsgeschwindigkeit unendlich gross ist, eine Eigenschaft, die unserer Intuition widerspricht. Aussagen dieser Allgemeinheit lassen sich weder durch Experimente noch durch Berechnung von Spezialfällen gewinnen, sondern können nur auf Grund theoretischer Überlegungen hergeleitet werden.

b) Die nummerische Berechnung der Lösung bei Vorgabe der Anfangs- und Randbedingungen erfordert ausgeklügelte Verfahren. Wegen der Komplexität des Problems müssen alle Symmetrien der Lösungen berücksichtigt werden, um die Anzahl der Unbekannten und damit die Anzahl der Rechnungen auf ein Minimum zu reduzieren. Denn jeder Rechenschritt ist mit einem Fehler behaftet, der leicht ausser Kontrolle geraten kann. Bei der quantitativen Auswertung kommen die Computer zum Einsatz. Die Organisation der Rechnung hat sich zu einer eigenständigen Wissenschaft, dem *wissenschaftlichen Rechnen*, entwickelt.

c) Die nummerischen Lösungen sind für die Praxis unbrauchbar, wenn sie nicht mit Fehlerabschätzungen verbunden sind. Für die MathematikerInnen stellt sich die nicht triviale Aufgabe, diese mit der unbekannten genauen Lösung zu vergleichen. Dazu sind raffinierte Techniken entwickelt worden, die analytische und geometrische Überlegungen einbeziehen. Ein weiterer wichtiger Aspekt ist die Stabilität, die sicherstellt, dass kleine Änderungen der vorgegebenen Daten nur kleine Störungen der Lösungen hervorrufen.

Zweck der Mathematik

Wie bereits erwähnt, besteht ein mathematisches Modell aus einer Anzahl mathematischer Gleichungen, welche Beziehungen zwischen einzelnen Grössen beschreiben. Es kann sich dabei um physikalische, biologische, soziale oder psychologische Grössen handeln.

Was bezweckt man mit einem solchen Modell?

Es sind zunächst ganz praktische Gründe.

– *Berechnung der Zukunft.*
Die Lösungen von Differenzialgleichungen hängen von Parametern ab, die in der Regel durch die Daten zu Beginn eines Prozesses festgelegt werden. Die Mathematik liefert Methoden, um den späteren Verlauf zu berechnen. Paradebeispiele dafür sind Wettervorhersagen, Satellitenbahnen, Voraussagen von Mond- und Sonnenfinsternissen, welche in früheren Zeiten den Mathematikern hohes Ansehen verliehen haben. Heute wird eifrig nach einer Formel gesucht, mit der sich die Entwicklung der Finanzmärkte vorausbestimmen lässt. Dieser Aspekt hat Robert Musil besonders beeindruckt, wenn er sagt: «Man kann die Mathematik eine geistige Idealapparatur nennen mit dem Zweck, alle möglichen Fälle prinzipiell vorzudenken. Das ist Triumph der geistigen Organisation.»

– *Verzicht auf Experimente.*
Falls sich die Mechanismen eines Prozesses mathematisch beschreiben lassen, kann sein Verlauf berechnet werden. Wenn die Rechnungen zuverlässig sind, kann auf Experimente verzichtet werden. Dies spielt beispielsweise bei der Bestimmung der maximalen Belastbarkeit einer Brücke eine wichtige Rolle.

Es sind auch Überlegungen theoretischer Art, die zur Mathematisierung vieler Wissenschaften führen.

– *Besseres Verständnis für die Ursachen eines Prozesses.*
Ein mathematisches Modell ist nur dann möglich, wenn die Mechanismen, die für den Ablauf eines Prozesses verantwortlich sind, bekannt sind. Die abstrakte Theorie der Differenzialgleichungen kann dazu dienen, diese Mechanismen aufzuspüren. Obwohl die klassischen Gleichungen der mathematischen Physik wie zum Beispiel die Maxwellgleichungen nur Approximationen der Wirklichkeit sind, verdanken wir ihnen die Elektrodynamik und die spezielle Relativitätstheorie.

– *Gewinnung neuer mathematischer Erkenntnisse.*
Ein grosser Teil der modernen Analysis hat seine Wurzeln in der Theorie der Differenzialgleichungen. Die Frage, ob eine Lösung existiert, auch wenn sie nicht explizit angegeben werden kann, führte zur Entwicklung der Funktionalanalysis, einer der tiefgründigsten Theorien des 20. Jahrhunderts.

Fazit

Zur Erfassung der komplexen Strukturen der heutigen Wissenschaften hat sich die Mathematik als äusserst effizient erwiesen. Ihre Methode beruht in erster Linie darauf, komplizierte Sachverhalte auf einfachere zurückzuführen. Sie ist das geistige Instrument, mit dem abstrakte Strukturen wahrgenommen werden. Begriffliche Klarheit und logische Konsistenz – keine andere Wissenschaft verkörpert diese Merkmale so vollkommen wie die Mathematik. Die Differenzialgleichungen gehören zu den Gebieten, in denen die Anwendbarkeit der Mathematik am deutlichsten sichtbar wird. Ihre Sprache ist interdisziplinär und verbindet WissenschaftlerInnen der verschiedensten Sparten.

Prof. Dr. sc.math. Catherine Bandle ist Extraordinaria für Mathematik am Mathematischen Institut der Universität Basel.

Demokratie mathematisch beleuchtet

Yuri F. Bilu und Christine U. Liebendörfer

Marie-Jean-Antoine-Nicolas de Caritat, Marquis de Condorcet (1743 – 1794), war Philosoph, Mathematiker und ein blühender Verfechter der Demokratie und der Menschenrechte. Da er jünger war als die anderen grösseren französischen Aufklärer, erlebte er die Französische Revolution mit und nahm sogar aktiv daran teil. Er setzte sich dafür ein, das Leben des Königs zu verschonen, was dazu führte, dass er während der Schreckensherrschaft der Jakobiner eingesperrt und vermutlich im Gefängnis umgebracht wurde.

Das von Condorcet um 1785 veröffentlichte *Essai sur l'application de l'analyse à la Probabilité des décisions rendues à la pluralité des voix* (im folgenden Essai genannt) hat einen besonderen Stellenwert in der Geschichte der Wahrscheinlichkeitstheorie. Als Beispiel seines dort gezeigten Scharfsinns mag das folgende *Condorcet Paradox* dienen: Es ist möglich, dass eine Mehrheit die Wahl *A* der Wahl *B* vorzieht, eine Mehrheit die Wahl *B* der Wahl *C* vorzieht und dennoch eine Mehrheit die Wahl *C* der Wahl *A* vorzieht. (Ein Mathematiker würde sagen, dass «die Mehrheit zieht vor» nicht transitiv ist.) Wir wollen dieses angebliche Paradox an einem Beispiel illustrieren. Corinne, Monika und Stephan mögen Hamburger, Pizza und Rösti, mit den folgenden Ordnungen von Vorzügen der drei Wahlen: HPR für Corinne, PRH für Monika und RHP für Stephan. Dann werden Corinne und Stephan wohl eher Hamburger essen anstatt in die Pizzeria zu gehen, während Corinne und Monika lieber Pizza essen und Rösti-Lokale meiden. Falls Monika und Stephan sich zum Essen verabreden, werden sie eher ein traditionelles Rösti-Lokal aufsuchen, als dass sie Hamburger im Fast-Food-Lokal zu sich nehmen.

Das «Condorcet Jury Theorem»

In seinem *Essai* vertritt Condorcet die Meinung, dass die Mehrheit einer Gruppe von qualifizierten Wählern, die zwischen zwei Dingen wählen können, wahrscheinlich die richtige Wahl treffen würde. Ausserdem geht er davon aus, dass sich diese Wahrscheinlichkeit mit zunehmender Anzahl von Wählern bis zur vollständigen Sicherheit erhöhen würde.

Condorcet hat diese Aussage eigentlich nicht explizit formuliert, vielmehr hat er sie mit mehreren «hypothetischen Situationen» untermauert. Erst einige Zeit später hat der britische Soziologe D. Black dieses Thema wieder aufgegriffen und obige Bemerkung in seinem Buch *The theory of Committees and Elections* (Cambridge, 1958) niedergeschrieben.

Das *Condorcet Jury Theorem* (dessen Name von Black stammt und das wir im Folgenden mit CJT abkürzen werden) ist kein einzelnes Theorem, sondern eine Reihe von mathematischen Voraussetzungen, die die Richtigkeit von Condorcets Aussagen implizieren.

Für einen individuellen Wähler *v* bezeichnen wir mit *p(v)* seine *Kompetenz*, das heisst die Wahrscheinlichkeit, dass *v* die richtige Wahl trifft. Folglich ist *p(v)* eine Zahl zwischen 0 und 1. Falls *p(v)* grösser als 0.5 ist, dann ist es wahrscheinlicher, dass *v* die richtige Wahl trifft. Ist *p(v)* kleiner als 0.5, dann ist die falsche Wahl wahrscheinlicher.

In seiner einfachsten Form lautet das CJT wie folgt:

Theorem 1. Nehmen wir an, dass alle Mitglieder einer Gruppe von Wählern dieselbe Kompetenz $p>0.5$ haben und, im üblichen statistischen Sinne, unabhängig voneinander wählen. Dann treffen die Wähler wahrscheinlich die richtige Entscheidung und diese Wahrscheinlichkeit steigt mit der Anzahl der Wähler bis zur vollständigen Sicherheit.

Allerdings sind die Voraussetzungen hier zu stark, denn es ist einerseits unrealistisch, dass alle Wähler dieselbe Kompetenz haben und andererseits unabhängig voneinander entscheiden. Man könnte zum Beispiel annehmen, dass Mitglieder einer Familie oder derselben politischen Partei ähnlich entscheiden. Oder man denke an einen Populisten mit hohem Einfluss auf andere Wähler.

Der Fall von abhängigen Wählern wurde von vielen Forschern untersucht. Im Folgenden werden wir stets annehmen, dass alle Wähler unabhängig voneinander sind, was (mindestens ungefähr) für die meisten Situationen des wirklichen Lebens zutrifft.

«Stay away from fair coins»

Gegeben sei also eine Gruppe von Wählern, die im Allgemeinen verschiedene Kompetenzen haben. Da wir die Voraussetzungen in Theorem 1 abschwächen wollen, stellt sich die folgende Frage:

Genügt es (für die Gültigkeit des CJT) anzunehmen, dass die Kompetenz jedes Wählers 0.5 übersteigt?

Die Antwort ist «nein», wie uns Jacob Paroush, Wirtschaftsprofessor an der Bar Ilan Universität in Israel, lehrt, denn unter diesen Voraussetzungen steigt die Wahrscheinlichkeit der richtigen Entscheidung nicht mit der Anzahl der Wähler. Um dies einzusehen, betrachten wir eine Gruppe von Wählern, deren Kompetenz genau 0.5 ist; das heisst, für jeden Wähler ist die richtige oder falsche Entscheidung gleich wahrscheinlich. Ihre Wahl ist dann ebenfalls mit gleicher Wahrscheinlichkeit richtig oder falsch. Mathematisch gesprochen ist die Wahrscheinlichkeit P, dass die Mehrheit der Wähler die richtige Entscheidung trifft, genau 0.5.

Nun verändern wir die Kompetenzen der Wähler, so dass sie leicht höher liegen als 0.5. Damit steigt auch die Wahrscheinlichkeit P leicht über 0.5 an. Sind die Veränderungen der Kompetenzen klein genug, dann wird auch die Veränderung für P ganz klein sein (in der mathematischen Sprache heisst dies, dass P stets von den Kompetenzen der Wähler abhängt). Zum Beispiel wäre P für eine geeignete Veränderung der Kompetenzen gleich 0.501, was bedeuten würde, dass die Mehrheit beinahe gleich wahrscheinlich richtig oder falsch entscheidet, und dies unabhängig von der Anzahl der Wähler.

In seinem Artikel *Stay away from fair coins* [Soc. Choice Welfare 15 (1998), 15 – 20] gibt Paroush Beispiele an, die dieses Phänomen illustrieren. Das folgende wurde angeregt durch eine gemeinsame Arbeit von Paroush und Daniel Berend, Professor der Mathematik an der Ben-Gurion Universität (Israel). Seien $v_1,\ldots,v_n$ eine Gruppe von Wählern mit wie folgt definierten Kompetenzen: $p(v_1) = 1/2 + 1/2$, $p(v_2) = 1/2 + 1/4$, $p(v_3) = 1/2 + 1/6$, $p(v_4) = 1/2 + 1/8$ und so weiter. Unter Verwendung von Methoden der modernen Wahrscheinlichkeitstheorie (zentraler Grenzwertsatz) zeigen Berend und Paroush, dass für grosse n die Wahrscheinlichkeit P nahe bei 0.5 liegt, was bedeutet, dass für dieses Beispiel das CJT falsch ist.

Paroush nennt Individuen mit Kompetenz 0.5 *fair coins* und wir wollen diesen Abschnitt mit einem langen, aber interessanten Zitat seines Artikels schliessen.

«...their [fair coins'] votes are meaningless, they only introduce noise to any social choice and therefore they are inessential in the decision making process. The importance of staying away from fair coins is a reasonable explanation of the restrictions imposed by democratic countries on the permission to participate in the social choice activity that we do observe. It is evident that several groups of individuals who are considered fair coins or irrational in the sense that they make their choice at random, such as youngsters below a certain age or individuals who are hospitalized in lunatic asylums are not allowed to vote.

Most of the members of primitive tribes are not essential in the decision making process because they are almost close to fair coins. In these tribes decisions are not taken by a simple majority rule in a democratic way but are made by a committee of the elders. Because of their life experience, only the elders are considered individuals who stay away from 1/2. No one knows if the survival of these tribes would have been guaranteed with any alternative decision making process. Finally, note that the subject discussed here may also be a relevant argument in the endless debates if whether or not workers should take part in management decisions or students should participate in academic committees.»

Die durchschnittliche Kompetenz

Wir definieren die durchschnittliche Kompetenz einer Gruppe als die Summe der Kompetenzen aller Wähler, dividiert durch ihre Anzahl. Die folgende Aussage wurde von mehreren Forschern gleichzeitig gefunden.

Theorem 2. Sei p eine Zahl grösser als 0.5. Dann gilt das CJT für jede grössere Gruppe von unabhängigen Wählern mit durchschnittlicher Kompetenz grösser als p.

Demnach trifft eine grosse Gruppe von Wählern mit durchschnittlicher Kompetenz 0.501 sehr wahrscheinlich die richtige Entscheidung. Dieses Theorem ist viel nützlicher als Theorem 1. Zum einen ist die Voraussetzung viel schwächer, und zum anderen ist es viel einfacher, die durchschnittliche Kompetenz einer Gruppe als die individuelle Kompetenz jedes einzelnen Wählers zu bestimmen. Es ist jedoch möglich, dass eine Wählergruppe viele «fair coins» enthält, womit sich ihre durchschnittliche Kompetenz sehr stark 0.5 annähert. Kann man Theorem 2 auf solche Gruppen anwenden? «Ja», lautet die Antwort von Berend und Paroush. Im Weiteren soll eine Wählergruppe vernünftig heissen, wenn mindestens 1% der Mitglieder eine Kompetenz zwischen 0.001 und 0.999 haben. (Es ist in der Tat höchst unvernünftig zu glauben, dass 99% der Wähler entweder «sehr klug» oder «sehr dumm» sind.)

Theorem 3. Das CJT gilt für vernünftige Gruppen von n Wählern mit durchschnittlicher Kompetenz grösser als $\frac{1}{2} + \frac{1}{\sqrt[3]{n}}$.

Folglich kann einer grossen Gruppe von Wählern mit einer durchschnittlichen Kompetenz, die sich mit steigender Anzahl Wähler «langsam» 0.5 nähert, vertraut werden. Die letzte Bedingung ist recht subtil: Berend und Paroush zeigen, dass $\sqrt[3]{n}$ nicht einmal durch $\sqrt{n}$ ersetzt werden kann.

Entscheidungsregeln

Trotz der alarmierenden Beispiele aus dem zweiten Abschnitt können wir also der Mehrheit der Wähler vertrauen; mindestens dann, wenn die Anzahl der Wähler gross genug ist. Gleichwohl können wir uns nun folgende Frage stellen:

Ist der Mehrheitsentscheid die beste Vorgehensweise, oder gibt es eine effizientere Möglichkeit, eine Entscheidung zu treffen?

Sei wie oben $v_1, \ldots, v_n$ eine Gruppe von Wählern, die eine *ja/nein*-Wahl treffen müssen. Eine *Wahl* ist eine Folge von n Termen, wobei jeder Term entweder *ja* oder *nein* ist. Das heisst, jeder Term entspricht der Entscheidung eines einzelnen Wählers aus der Gruppe. Eine *Entscheidungsregel* ist die Zuordnung eines endgültigen *Wahlergebnisses ja* oder *nein* zu jeder Wahl gemäss einer Regel. Zum Beispiel kann das Wahlergebnis dem entsprechen, was die Mehrheit der Wähler entschieden hat; diese Regel heisst *Mehrheitsregel*. In allen Fällen, in denen die Anzahl n der Wähler ungerade ist, liefert sie ein eindeutiges Wahlergebnis. Wir können uns auch vorstellen, dass einer der Wähler (sagen wir v_1) viel kompetenter ist als die anderen und wir das Wahlergebnis allein aufgrund seiner Meinung treffen und alle anderen Meinungen ignorieren. Dies ist die *Expertenregel*.

Eine wichtige Klasse von vernünftigen Entscheidungsregeln sind die *gewichteten Mehrheitsregeln*, das heisst, wir ordnen den Wählern «Gewichte» $w_1,\ldots,w_n$ zu. Diese Gewichte können beliebige nicht negative Zahlen sein. (Manchmal sind auch negative Gewichte erlaubt.) Für jede Wahl wird das Wahlergebnis wie folgt bestimmt: Ist die Summe der Gewichte der Wähler, die *ja* gestimmt haben, grösser als die Summe der Gewichte der Wähler, die *nein* gestimmt haben, dann ist das Wahlergebnis *ja*. Im umgekehrten Fall ist das Wahlergebnis *nein*. Hier ergibt sich stets ein eindeutiges Wahlergebnis, falls für alle möglichen Festlegungen der ±-Vorzeichen die Summe $\pm w_1 \pm \ldots \pm w_n$ nicht null ist. Die Mehrheitsregel und die Expertenregel (mit v_1 als «Experte») sind Spezialfälle der gewichteten Mehrheitsregeln, nämlich mit den Gewichten (1,…,1) respektive (1,0…,0). Man beachte, dass verschiedene Gewichte dieselbe Regel definieren können. Zum Beispiel kann die Mehrheitsregel für drei Wähler auch durch die (4,3,2)-gewichtete Mehrheitsregel beschrieben werden. Hingegen kann nicht jede vernünftige Entscheidungsregel durch eine gewichtete Mehrheitsregel definiert werden. Seien zum Beispiel 15 Wähler in 3 Komitees mit je 5 Wählern unterteilt. Jedes Komitee entscheidet gemäss der Mehrheitsregel, und das Wahlergebnis entspricht der Mehrheit der Komiteewahlen. Diese Vorschrift ist sinnvoll (sie widerspiegelt beispielsweise die Präsidentenwahlen in den USA), kann aber nicht als gewichtete Mehrheitsregel dargestellt werden.

Ein anderes Beispiel einer nicht gewichteten Regel ist die *qualifizierte Mehrheitsregel*, deren Wahlergebnis *nein* ist, es sei denn, mindestens zwei Drittel der Wähler stimmen *ja*. (Diese Regel wird beispielsweise im Rahmen eines «Impeachment»-Verfahrens im Senat der USA angewandt, um den Präsidenten des Amtes zu entheben.) Zur Veranschaulichung schreiben wir alle möglichen gewichteten Mehrheitsregeln für 4 oder weniger Wähler nieder. Da die Wähler $v_1,\ldots,v_n$ immer so umnummeriert werden können, dass für ihre Gewichte $w_1 \geq \ldots \geq w_n$ gilt, genügt es, alle möglichen Regeln mit nicht aufsteigenden Folgen von Gewichten aufzuzählen. Für die «Menge» eines einzigen Wählers gibt es nur eine Regel, welche Experten- und Mehrheitsregel zugleich ist. Auch für zwei Wähler gibt es nur eine Regel, die Expertenregel (1,0). Für drei Wähler gibt es die Expertenregel (1,0,0) und die Mehrheitsregel (1,1,1). Drei mögliche Regeln gibt es für vier Wähler: erstens die Expertenregel (1,0,0,0); zweitens die Regel (1,1,1,0), die bedeutet, dass v_1, v_2 und v_3 durch Mehrheit entscheiden und die Wahl von v_4 ignorieren; drittens die Regel (2,1,1,1), bei der v_1 gewinnt, sobald mindestens einer der anderen seine Meinung teilt, aber verliert, wenn alle anderen gegen ihn sind. Das Aufzählen aller gewichteten Regeln für 5 Wähler sei als gute Übung dem Leser überlassen (es gibt 7 verschiedene Regeln).

Expertenregel gegen Mehrheitsregel

Wir kehren nun wieder zur Fragestellung des vorhergehenden Abschnittes zurück. Dabei wollen wir eine Entscheidungsregel für eine Menge $v_1,\ldots,v_n$ von Wählern *optimal* nennen, wenn sie mit höchster Wahrscheinlichkeit die «richtige» Entscheidung trifft. Sind die Kompetenzen $p_1,\ldots, p_n$ der Wähler bekannt, so ist die optimale Regel gegeben durch die gewichtete Mehrheitsregel mit den Gewichten $w_i = \ln \frac{p_i}{1-p_i}$. Um dies besser zu verstehen, betrachte man drei Beispiele. 1) Ist die Kompetenz p_i nahe bei 1, dann ist das zugehörige Gewicht eine grosse positive Zahl. Das ist ganz natürlich, denn die Meinung eines solchen Wählers sollte ein grosses Gewicht haben. 2) Ist p_i nahe bei 0, dann ist w_i eine sehr grosse *negative* Zahl. Auch dies ist gut verständlich, denn ein derartiger Wähler ist so unvernünftig, dass diejenige Meinung, die seiner eigenen widerspricht, möglichst viel Gewicht tragen sollte. 3) Ist die Kompetenz $p_i = 1/2$, dann ist $w_i = 0$. Dies bedeutet, dass die Meinung einer «fair coin» schlichtweg missachtet werden sollte.

Natürlich sind im Allgemeinen die Kompetenzen unbekannt. Ausserdem wäre ein guter Test, der die Kompetenz eines Individuums feststellen könnte, höchstwahrscheinlich nicht finanzierbar und sogar illegal. Daher ist es wichtig, ein «Mass der Effizienz» einer Entscheidungsregel für Wähler mit unbekannter Kompetenz festzulegen. Anhand dieses Masses können wir dann die effizienteste der Regeln herausfinden. Nun wird als *Effizienz* einer Entscheidungsregel die Wahrscheinlichkeit definiert, mit der diese Regel für eine zufällig ausgewählte Menge von Wählern optimal ist.

Ein Statistiker würde sagen, dass das Wort «zufällig» nur dann einen Sinn hat, wenn eine Verteilung der Zufallsobjekte, in unserem Fall sind das die Kompetenzen der Wähler, festgelegt wird. Deshalb werden wir annehmen, dass die Kompetenzen im Intervall [0.5,1] gleich verteilt sind. Das bedeutet, dass alle Kompetenzen grösser oder gleich 0.5 sind und dass die Anzahl der Wähler mit einer Kompetenz zwischen α und β proportional zur Differenz $\beta-\alpha$ ist. Mit anderen Worten, 20% der Wähler haben eine Kompetenz zwischen 0.6 und 0.7, 40% der Wähler haben eine Kompetenz zwischen 0.8 und 1, und so weiter.

Für eine kleine Anzahl von Wählern vergleichen Jacob Paroush und Shmuel Nitzan (auch von der Bar Ilan Universität) mittels der heuristischen *Monte-Carlo-Methode* die Effizienz der Expertenregel mit der der Mehrheitsregel (und noch weiteren). Erstaunlicherweise konnte festgestellt werden, dass die Expertenregel viel effizienter ist als die Mehrheitsregel. Für drei Wähler hat beispielsweise die Expertenregel eine Effizienz von 68%, während die der Mehrheitsregel nur 32% beträgt. Diese Untersuchung wurde von Daniel Berend und Jørgen Harmse, einem Mathematiker der Universität von Texas in Austin, fortgesetzt. Mit Methoden der modernen Mathematik konnten Berend und Harmse die heuristischen Berechnungen von Nitzan und Paroush bestätigen und für eine grosse Anzahl Wähler die überwältigend hohe Effizienz der Expertenregel gegenüber der Mehrheitsregel zeigen. Zum Beispiel ist für 99 Wähler die Expertenregel mindestens 10^{95}-mal effizienter als die Mehrheitsregel! (Bemerkenswert ist dabei, dass die Arbeit von Berend und Harmse die Eigenschaften der ζ-*Funktion* nutzt. Diese Funktion ist ein zentrales Objekt der reinen Mathematik, der man lange Zeit jegliche «praktische» Bedeutung absprach.)

Nun könnte man annehmen, dass das Phänomen der Effizienz der Expertenregel von der vorausgesetzten Gleichverteilung der Kompetenzen abhängt, die nun wiederum keine gute Beschreibung des realen Lebens ist. Aber Berends Doktorandin Luba Sapir untersuchte die Effizienz für viele verschiedene Arten von Verteilungen, und die Expertenregel erwies sich hartnäckig als viel effizienter als die Mehrheitsregel.

Schlussbemerkungen

In einer demokratischen Gesellschaft ist ein Komitee aus fünf Mitgliedern, welches die (2,1,1,1,0)-gewichtete Mehrheitsregel anwendet, kaum vorstellbar. Genau diese ist aber gemäss Nitzan und Paroush die effizienteste Regel für fünf Wähler. Die Expertenregel kommt an zweiter Stelle, und die Mehrheitsregel liegt an siebter und letzter Stelle. Bedeutet dies, dass die Diktatur (der Expertenregel entsprechend) die bessere Art einer sozialen Ordnung darstellt als die Demokratie? Natürlich nicht, denn die vielseitigen menschlichen Eigenschaften der Wähler oder Experten werden von unserem Modell nicht berücksichtigt. Die Diktatur mag wohl sehr effizient sein, sie sorgt aber kaum für Stabilität. Zu sehr hängt sie von Gesinnungsschwankungen einer einzelnen Person ab. Man denke zum Beispiel an Frankreich unter Louis XIV. Die Erfahrung zeigt, dass eine gut eingespielte Demokratie (wie in der Schweiz oder in England) die stabilsten politischen Verhältnisse garantiert. Die beste Lösung besteht wahrscheinlich in einer ausgewogenen Mischung zwischen Demokratie und Diktatur. In der Tat enthält jede Demokratie auch autoritäre Strukturen (beispielsweise in der Armee oder während Notzuständen), und fast jeder Diktator stützt sich auch auf demokratische Entscheide.

Die detaillierte Analyse der verschiedenen Arten von sozialen Ordnungen gehört jedoch ins Gebiet der Soziologie und nicht der Mathematik. Deshalb lassen wir es hiermit bewenden.

Wir möchten uns bei Daniel Berend, Wolfgang Reichel und Thomas J. Zehrt für wertvolle Bemerkungen und Vorschläge bedanken.

Dr. Yuri Bilu ist seit 1998 Assistent am Mathematischen Institut. Sein Arbeitsgebiet ist die Zahlentheorie.

Christine Liebendörfer hat in Basel das Mathematikdiplom erworben. Sie ist Assistentin und dissertiert über ein Thema aus der Zahlentheorie.

Die wahre Geometrie oder denkbare Geometrien

Hans-Christoph Im Hof

Praktische geometrische Kenntnisse sind in der Geschichte der Menschheit schon früh anzutreffen:

– Nach dem Hochwasser sieht alles anders aus. Das neu zu verteilende Land muss neu vermessen werden. Das ist Geometrie im strengen Sinne des Wortes.
– Die Planung komplizierter Bauwerke erfordert Techniken der räumlichen Geometrie.
– Wer übers Meer fährt oder den Himmel beobachtet und zu ordnen versucht, was er sieht, bedient sich der sphärischen Geometrie.

Etwas Neues begegnet uns vom 6. Jahrhundert v. Chr. an in der griechischen Kultur. Die Geometrie wird – wie auch die Arithmetik – zu einem Gegenstand des Nachdenkens. Des Nachdenkens würdig ist sie nicht als ein Sammelsurium nützlicher geometrischer Techniken, sondern als ein nach den Regeln der Logik errichtetes Gedankengebäude, in welchem eindeutige mathematische Aussagen als richtig gelten, wenn sie durch eine nachvollziehbare Kette von logischen Schlüssen bewiesen werden können.

Plato, Der Staat, VI.20

Du weisst, dass die Leute, die sich mit Geometrie
und Rechnungen und ähnlichen Dingen beschäftigen,
von bestimmten Voraussetzungen ausgehen. …
Von diesen Grundlagen aus leiten sie nun gleich das Weitere ab
und gelangen schliesslich folgerichtig zu dem,
worauf sie es mit ihrer Untersuchung abgesehen hatten. …
Und du weisst doch auch, dass sie die sichtbaren Gestalten zu Hilfe
nehmen und ihre Reden auf diese beziehen,
obschon eigentlich nicht sie den Gegenstand ihres Nachdenkens
bilden, sondern jene, von denen diese Abbilder sind. …
Die sichtbaren Gestalten selbst, die sie da modellieren und
zeichnen und wovon es auch wieder Schatten und Spiegelbilder im
Wasser gibt, die verwenden sie ihrerseits wieder als Bilder,
während sie jenes zu erblicken suchen, das man auf keine andere
Weise erblicken kann als mit dem vernünftigen Nachdenken.

Aristoteles, Zweite Analytik, I.10

Grundlagen eines jeden Gebietes nenne ich das, dessen Sein
und Zutreffen man nicht beweisen kann. Was die obersten und die
daraus abgeleiteten Begriffe bedeuten, wird also vorausgesetzt;
dass es so etwas gibt, muss bei den obersten Begriffen
ebenfalls vorausgesetzt, bei den andern bewiesen werden.
Die Beweismittel in den beweisenden Wissenschaften sind teils
ihnen eigentümlich, teils mehreren gemeinsam …
Eigentümlich ist zum Beispiel die Begriffsbestimmung einer Linie
oder einer Geraden, gemeinsam der Satz:
Gleiches von Gleichem abgezogen ergibt Gleiches.
Man kann auch sagen, eigentümlich seien die Gegenstände,
deren Sein vorausgesetzt werde und deren wesentliche Eigenschaften
die betreffende Wissenschaft untersuche,
zum Beispiel … für die Geometrie Punkte und Linien.
Hier setzt man voraus, dass sie sind und was sie sind.

Aus nichts lässt sich nichts folgern. Das Gebäude steht auf einem Fundament, auf einer Reihe von nicht bewiesenen, sondern als richtig postulierten Grundtatsachen. Ökonomie und guter Geschmack verlangen, die Liste der Postulate kurz zu halten. Was beweisbar ist, soll nicht postuliert werden.

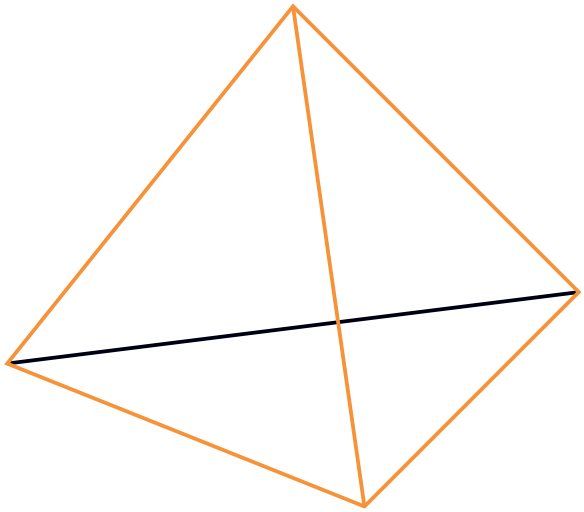
Aristoteles, Über den Himmel, III.4

Es ist offenbar, dass es weitaus besser ist, die Zahl der Grundtatsachen
endlich zu halten. Ja, sie sollten sogar so wenig wie möglich sein,
vorausgesetzt sie erlauben den Beweis derselben Resultate.
Darauf bestehen die Mathematiker.

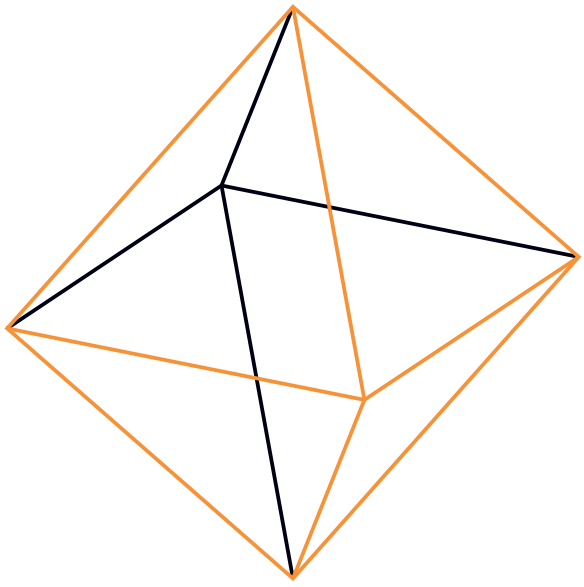
Die Elemente des Euklid

Das erste systematische Lehrbuch der Mathematik, das die Jahrtausende überlebt hat, sind die Elemente des Euklid. Hier wird eine Wissenschaft nach dem von Aristoteles aufgestellten Programm aufgebaut. Ausgehend von Postulaten werden Sätze bewiesen und daraus weitere Sätze und so weiter ad infinitum, praktisch so lange, wie sich innerhalb einer Theorie interessante offene Probleme finden lassen.

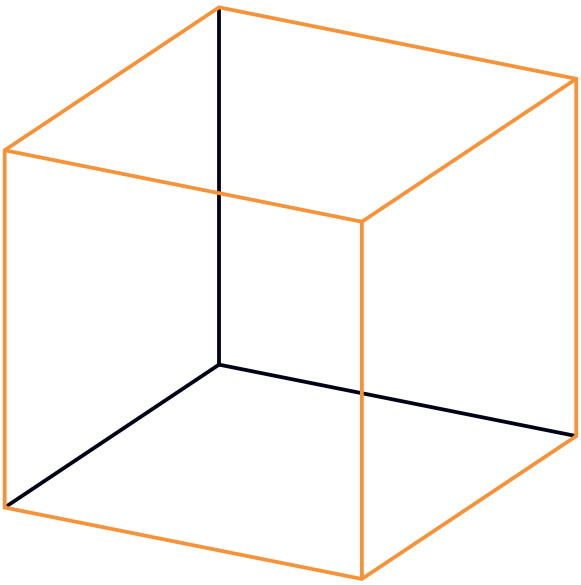
Die geometrischen Bücher der Elemente führen von der elementaren ebenen Geometrie bis zur Theorie der *Platonischen Körper* (Tetraeder, Oktaeder, Würfel, Ikosaeder und Dodekaeder). Die Platonischen Körper, unter allen von ebenen Flächen begrenzten räumlichen Gebilden diejenigen grösstmöglicher Symmetrie, finden wir im platonischen Dialog «Timaios» beschrieben. Sie sind dort zugeordnet den Elementen (Feuer, Luft, Erde, Wasser und – quinta essentia), welche sich nach Massgabe der geometrischen Möglichkeiten ineinander umwandeln können. Heute gehört die aus dem Studium von Symmetrien entwickelte Theorie der Symmetriegruppen zum Instrumentarium der Theoretischen Physik.



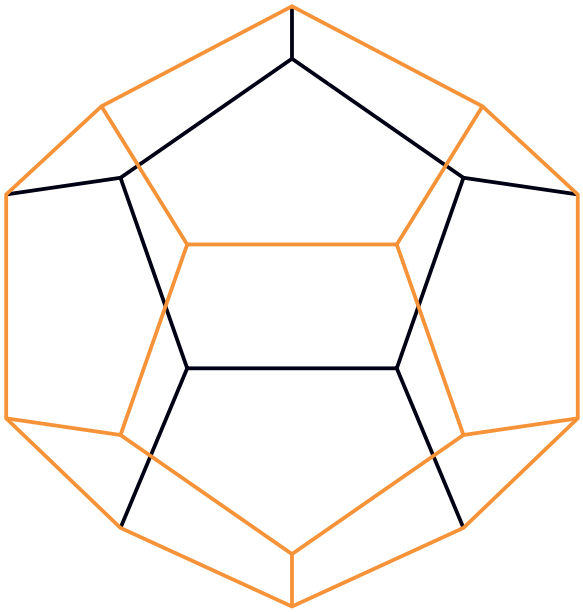
Tetraeder



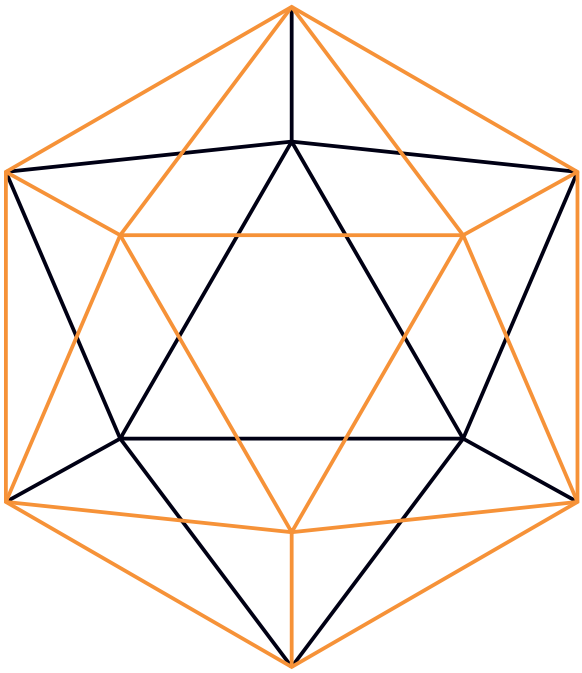
Oktaeder



Würfel

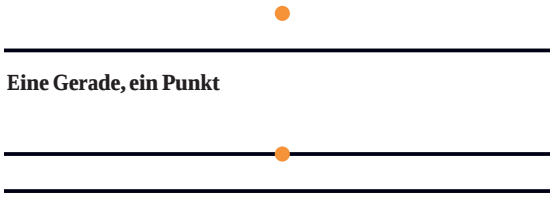


Dodekaeder



Ikosaeder

Abbildung 2:



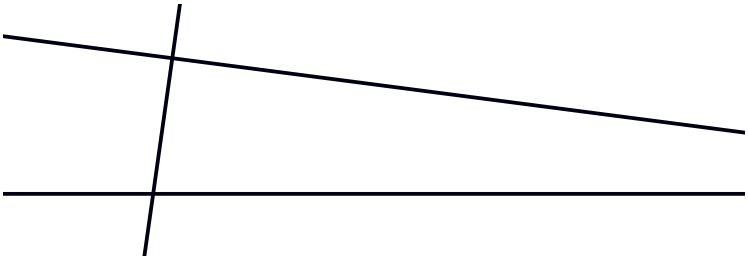
Eine Gerade, ein Punkt

… und die (dadurch eindeutig bestimmte?) Parallele

Die Parallelentheorie – ein Stein des Anstosses

Wir kehren zurück zur elementaren ebenen Geometrie. Ein wichtiger Satz bei Euklid besagt, dass es in einer Ebene zu einer Geraden und einem nicht auf ihr liegenden Punkt eine und nur eine Gerade gibt, die den Punkt enthält und zur gegebenen Geraden parallel ist. Diesen Satz beweist Euklid unter Verwendung des im Vergleich zu den andern Postulaten eher umständlich klingenden so genannten 5. Postulates.

Euklid, Die Elemente, 1. Buch, 5. Postulat
Es soll gefordert werden:
Wenn eine Gerade zwei Gerade trifft
und mit ihnen auf derselben Seite innere Winkel bildet,
die zusammen kleiner sind als zwei Rechte,
so sollen die beiden Geraden,
ins Unendliche verlängert,
schliesslich auf der Seite zusammentreffen,
auf der die Winkel liegen,
die zusammen kleiner sind als zwei Rechte.



Das 5. Postulat und mit ihm die ganze euklidische Parallelentheorie wurde sogleich zu einem Stein des Anstosses. Nicht dass die Schlüssigkeit der Beweise und damit die Richtigkeit der Sätze angezweifelt wurden – die euklidische Parallelentheorie steht auch durchaus im Einklang mit der Erfahrung –, der Vorwurf, der bereits von den frühesten Kommentatoren an Euklid gerichtet wurde, lautete: Das 5. Postulat sei ein beweisbarer Satz, es soll also nicht postuliert, es soll bewiesen werden.

Die Parallelentheorie – ein exemplarischer Stolperstein
In der Ersten Analytik von Aristoteles, II.16,
finden wir die Bemerkung:
«Den Lehrsatz in den Vordersätzen voraussetzen bedeutet, …
den Beweis schuldig bleiben, den man erbringen wollte. …
So verfahren die Mathematiker, die ihre Parallelenkonstruktion beweisen. Sie merken nicht, dass sie dabei Annahmen machen, die ihrerseits wieder zum Beweis die Parallelen voraussetzen.»
An welche Mathematiker dachte Aristoteles? Sicher nicht an Euklid, denn gerade dieser hat die Parallelentheorie nicht mittels Zirkelschlüssen aufgebaut. Wir müssen annehmen, dass es schon vor Euklid Versuche gab, die Geometrie auf ein solides Fundament zu stellen, dass aber diese Theorien mit logischen Fehlern behaftet waren. Aristoteles dienten solche Fehler als Anschauungsmaterial für Zirkelschlüsse.

Wer Beweisbarkeit behauptet, schuldet einen Beweis. Wird ein Beweis gefunden, ist die Sache erledigt. Solange kein Beweis bekannt ist (und solange auch die prinzipielle Unmöglichkeit eines solchen Beweises nicht nachgewiesen ist), bleibt offen, ob «nur» mangelnde Einsicht oder aber prinzipielle Unmöglichkeit das Finden des gesuchten Beweises verhindern.

Eine Geschichte von Irrtümern

Während zweier Jahrtausende haben unzählige Mathematiker der Antike, der islamischen Welt und des Abendlandes versucht, das 5. Postulat zu beweisen. Alle «Beweise» sind falsch: Sie enthalten entweder Fehlschlüsse oder aussermathematische Argumente (z.B. Rückgriffe auf die «Natur der Geraden») oder sie stützen sich auf ein anderes, meist mit dem fünften äquivalentes Postulat. Dies kann stillschweigend geschehen – dann ist der Beweis lückenhaft – oder es wird ausgesprochen. In diesem Falle ist der Beweis nicht wirklich falsch, er hält nur nicht, was er verspricht. Das 5. Postulat wird dann nicht aus den übrigen, sondern mit Hilfe eines neuen «fünften» Postulates bewiesen, und das Problem reduziert sich auf eine Frage des Geschmacks: nämlich auf die Frage, welche von zwei gleichwertigen Aussagen postuliert, welche bewiesen wird.

Gelehrte aus mehr als zwei Jahrtausenden, die sich mit der Parallelentheorie beschäftigt haben:

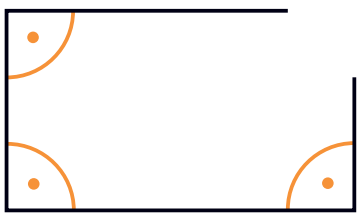
Aristoteles	4. Jh.	↑ vor Chr.
Euklid	4./3. Jh.	
Archimedes	3. Jh.	
Posidonius	2./1. Jh.	
Geminus	1. Jh.	
Ptolemäus	2. Jh.	↓ nach Chr.
Proclus	5. Jh.	
Aganis	6. Jh.	
Simplicius	6. Jh.	
Al-Gauhari	8./9. Jh.	
Tabit ibn Qurra	9. Jh.	
An-Nayrizi	9./10. Jh.	
Ibn al-Haytam	10./11. Jh.	
Umar al-Hayyam	11./12. Jh.	
Nasir ad-Din at-Tusi	13. Jh.	
Pietro Antonio Cataldi	16./17. Jh.	
Giovanni Alfonso Borelli	17. Jh.	
John Wallis	17. Jh.	
Girolamo Saccheri	17./18. Jh.	
Johann Heinrich Lambert	18. Jh.	
Adrien-Marie Legendre	18./19. Jh.	

Einige der Versuche, das 5. Postulat zu beweisen, lassen sich – mehr oder weniger – durch den folgenden Gedankengang beschreiben. Wir versuchen, ein Rechteck, das heisst ein Viereck mit vier rechten Winkeln zu konstruieren.

Wir beginnen mit einem rechten Winkel (a), fügen zwei weitere rechte Winkel hinzu (b) und fragen nach der Grösse des vierten Winkels (c). Nennen wir den vierten Winkel α. In der euklidischen Geometrie wird gezeigt – mit Hilfe des 5. Postulates –, dass α ein rechter Winkel ist. Könnte dies ohne Verwendung des 5. Postulates gezeigt werden, so würde daraus ein Beweis des 5. Postulates folgen.

Eine mögliche Strategie zum Nachweis, dass α ein rechter Winkel ist, besteht darin, die Annahme, dies sei nicht der Fall, ad absurdum zu führen. Ist α kein rechter Winkel, so ist es entweder kleiner oder grösser als 90°. Die Annahme, α sei grösser als 90°, lässt sich leicht zu einem Widerspruch führen, kann also verworfen werden. Die Annahme, α sei kleiner als 90°, lässt sich indessen nicht (ohne Trugschluss) ad absurdum führen.

a)



b)

c)

Die unerwartete Lösung

Erst zu Beginn des 19. Jahrhunderts wurde die Lösung gefunden: Neben der euklidischen existiert eine völlig gleichberechtigte nichteuklidische (die so genannte hyperbolische) Geometrie. In ihr gelten dieselben Postulate wie in der euklidischen, mit Ausnahme des fünften, von welchem die Negation gilt. Die beiden Geometrien widersprechen einander, jede ist aber in sich so stimmig (widerspruchsfrei) wie die andere. Somit ist es prinzipiell unmöglich, das 5. Postulat aus den übrigen zu beweisen.

Die Entdeckung einer zweiten Geometrie war eine wissenschaftliche Revolution. Es ging nun nicht mehr um die Beschreibung der einen wahren Geometrie, sondern um die Entdeckung und Erforschung «aller» denkbaren Geometrien.

Die Mathematik liefert nicht das Wahre, sondern das Denkbare: einen Katalog von Modellen. Im Alltagsleben hat sich das Modell der euklidischen Geometrie bewährt. Ob unsere Tische rechteckig oder nur beinahe rechteckig sind, ist irrelevant. Welche Geometrie hingegen für die Beschreibung des Universums die angemessenste ist, dies ist eine offene Frage. Sie liegt ausserhalb der Mathematik.

Die Entdecker der nichteuklidischen Geometrie

Carl Friedrich Gauss (1777 – 1855) teilt in verschiedenen Briefen mit, dass er sich seit 1792 mit den Grundlagen der Geometrie beschäftigt und sich der Existenz einer nichteuklidischen Geometrie vergewissert habe.

Janos Bolyai (1802 – 1860) kündigt im Jahre 1823 in einem Brief an seinen Vater Wolfgang Bolyai die Entdeckung einer neuen Geometrie an. Seine Theorie wird veröffentlicht im Appendix Scientiam Spatii absolute veram exhibens, einem Anhang zu einem Lehrbuch seines Vaters über Geometrie, Maros-Vasarhely, 1832.

Nikolai Ivanovich Lobachevskii (1792 – 1856) kündigt im Jahre 1826 in einem Vortrag an der Universität Kasan die Entdeckung einer neuen Geometrie an. Seine erste diesbezügliche Veröffentlichung erscheint auf Russisch im Kasaner Boten von 1829/30. Es folgen zahlreiche weitere Veröffentlichungen in Russisch, Deutsch und Französisch.

Einige charakteristische Eigenschaften der hyperbolischen Geometrie

Eigenschaften, die aus der Negation des 5. Postulates folgen, sind charakteristisch für die hyperbolische Geometrie. Zum Beispiel:

Die Summe der drei Winkel eines Dreiecks ist kleiner als 180°.

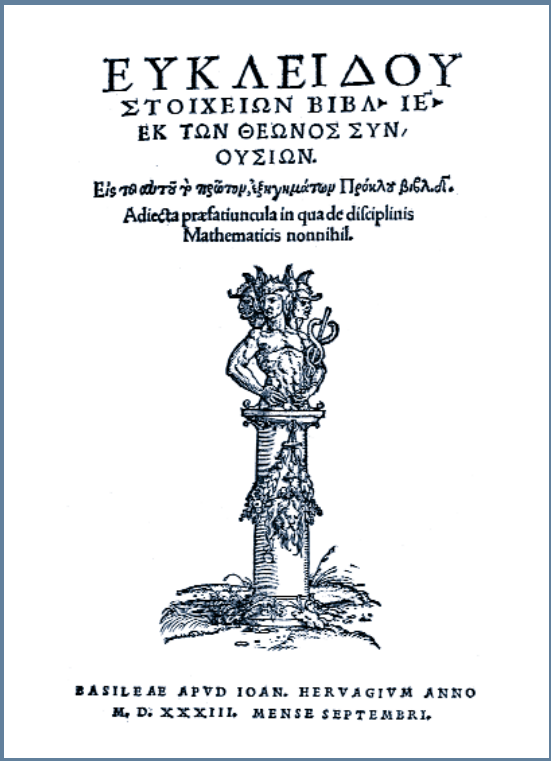
Die Winkel eines gleichseitigen Vierecks (eines Quadrats) sind kleiner als 90°. Sie sind umso kleiner, je grösser das Quadrat ist. Quadrate verschiedener Grösse sehen einander nicht ähnlich!

Parallele Gerade haben keinen konstanten Abstand voneinander. Sie laufen in einer Richtung zusammen, in der andern Richtung entfernen sie sich voneinander.

Zwei Gerade einer Ebene schneiden einander, sind zueinander parallel oder (und dies schliesst die ersten beiden Fälle aus) haben genau eine gemeinsame Senkrechte.

Versucht man, den dreidimensionalen Raum durch unendlich viele Exemplare ein und desselben Platonischen Körpers in vollkommen regelmässiger Weise auszufüllen, so kommt im euklidischen Raum nur der Würfel als «Pflasterstein» in Frage. Im hyperbolischen Raum sind alle fünf Platonischen Körper als Pflastersteine zugelassen. Während im euklidischen Fall die Grösse des Würfels ohne Belang ist, so ist die Grösse des entsprechenden Körpers im hyperbolischen Fall essentiell: Sie bestimmt den Winkel zwischen den Seitenflächen des Körpers.

Prof. Dr.phil. Hans-Christoph Im Hof
ist Ordinarius für Mathematik
am Mathematischen Institut der Universität Basel.



Die Überlieferung der «Elemente»

Die Elemente des Euklid gelten als das nach der Bibel am häufigsten edierte, kommentierte und in andere Sprachen übersetzte Werk. Im Abendland wurde der vollständige Text erst im 12. Jahrhundert durch Übersetzungen vom Arabischen ins Lateinische bekannt.

Die Abbildung zeigt das Titelblatt der ersten, aus *griechischen* Manuskripten edierten, *gedruckten* Ausgabe der Elemente des Euklid, erschienen 1533 in Basel.

Die Euler-Edition

Leonhard Euler (Basel 1707 – St. Petersburg 1783) war der bedeutendste und produktivste Mathematiker des 18. Jahrhunderts. Mehrere Versuche, Eulers immenses wissenschaftliches Werk in einer Gesamtausgabe zu veröffentlichen, sind am Umfang dieses Werks gescheitert.

Die heutige Euler-Edition geht auf einen Beschluss der Schweizerischen Naturforschenden Gesellschaft (heute: Schweizerische Akademie der Naturwissenschaften) aus dem Jahre 1909 zurück. Der erste Band der Edition erschien im Jahre 1911. Seither sind von den gedruckten Werken Eulers 67 Bände erschienen; drei Bände stehen noch aus. Seit 1967 wird auch der Briefwechsel Eulers bearbeitet. Von den geplanten zehn Bänden sind derzeit vier erschienen.

Die Herausgabe der wissenschaftlichen Manuskripte und Tagebücher Eulers wurde noch nicht in Angriff genommen.

www.leonhard-euler.ch

Die Bernoulli-Edition

Jacob (1654 – 1705), Johann (1667 – 1748) und Daniel (1700 – 1782) sind die hervorragendsten unter den Mathematikern und Physikern der Familie Bernoulli – aber nicht die einzigen: Insgesamt haben sich acht Mitglieder der Familie Bernoulli in der Mathematik und den Naturwissenschaften des 17. und 18. Jahrhunderts einen Namen geschaffen.

Die Bernoulli-Edition gibt die Gesammelten Werke und die wichtigsten Briefwechsel der Bernoulli und des ihnen nahe stehenden Jacob Hermann (1678 – 1733) heraus. Die Bernoulli-Edition wurde 1935 von Otto Spiess begründet, 1955 erschien der erste Band. (Otto Spiess war von 1908 bis 1944 Professor für Mathematik an der Universität Basel. Heute ist die Otto Spiess-Stiftung eine der Stützen der Edition.)

Gegenwärtig liegen 14 Bände vor; der gesamte Umfang der Edition wird zwischen 50 und 60 Bänden liegen.

www.ub.unibas.ch/spez/bernoull.htm

Reale Welt – Beobachtbare Welt

Ortwin Gerhard

Astronomische Bilder sind von beeindruckender Schönheit. Aber was bedeuten sie? Sie als Abbild von Naturphänomenen und Naturgesetzen quantitativ zu beschreiben und zu verstehen, benötigt physikalisches Verständnis und nicht selten mathematische Fertigkeiten. Ich möchte hier nur einen Aspekt herausgreifen, der auf einer Besonderheit der Astronomie beruht. Anders als in der Tomographie kann man nämlich ein bestimmtes astronomisches Objekt nur in einer einzigen Projektion beobachten.

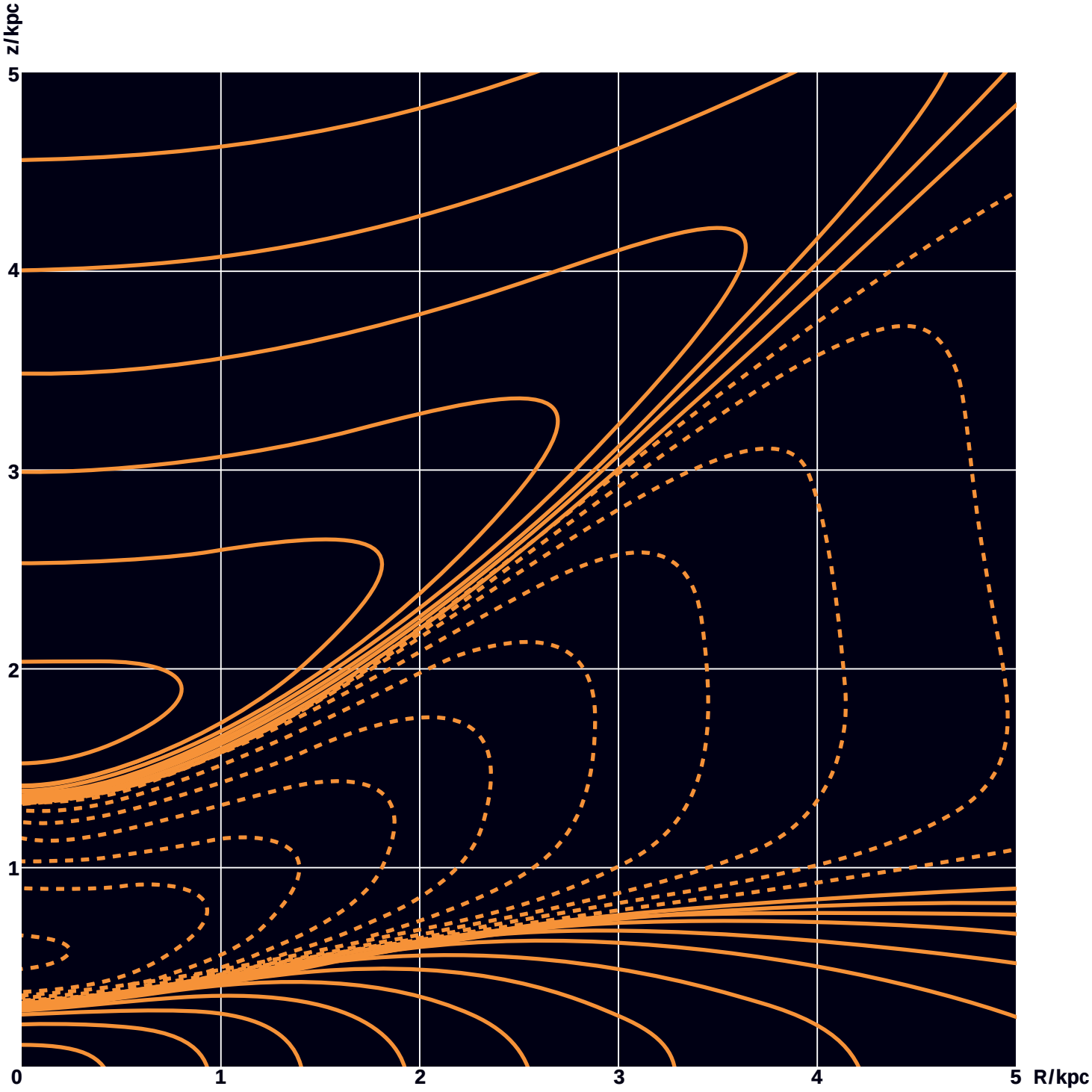
Nehmen wir eine elliptische Galaxie, eine Ansammlung von vielleicht 10^{11} Sternen, die ihren Namen daher hat, dass sie am Himmel als elliptische Lichtverteilung erscheint. Abweichungen von der Ellipsenform sind nur von der Grösse von etwa 1%. Elliptische Galaxien sind durchsichtig, das heisst, man sieht alle Sterne in der Projektion. Schon lange weiss man, dass eine Sternverteilung, die im dreidimensionalen Raum Ellipsoidform hat, in allen Projektionen elliptisch erscheint. Da alle elliptischen Galaxien elliptisch erscheinen, liegt der Schluss nahe, sie seien in Wirklichkeit Ellipsoide (ein statistisches Argument). Wenn da nicht die einprozentigen Abweichungen wären.

Wie eindeutig ist also die Deprojektion, das heisst die Rekonstruktion der dreidimensionalen räumlichen Verteilung? Natürlich im Allgemeinen überhaupt nicht, man kann ja immer Licht beliebig entlang jeder Sichtlinie hin- und herschieben, ohne dass sich das Bild ändert. «Beliebig» wäre aber nicht mit dem statistischen Argument verträglich. Wie aber dann? Nehmen wir an, wir hätten noch die zusätzliche Information, dass die Sternverteilung im Dreidimensionalen symmetrisch um eine Drehachse ist. Kann man sie dann eindeutig aus dem Bild deprojizieren? Ein einfaches mathematisches Argument sagt nein: Ein Teil der Lichtverteilung bleibt durch das Bild unbestimmt; mathematisch ausgedrückt fehlt die Information in einem Kegel (Konus) im so genannten Fourierraum der Lichtverteilung. Wenn aber Information fehlt, kann man aus dem Bild die dreidimensionale Verteilung nicht rekonstruieren. Mehr noch, durch Veränderung der Information in diesem Konus lässt sich die dreidimensionale Verteilung ändern, ohne dass man es im Bild sieht!

Die Abbildung zeigt eine so genannte Konusdichte. Addiert man eine solche Konusdichte zu einer normalen, überall positiven Sterndichteverteilung, so lässt sich eine andere positive Verteilung mit identischem Bild erzeugen. Das Erstaunliche an der in der Abbildung gezeigten Verteilung: sie ist in allen Projektionsrichtungen näher als 45 Grad zur z-Achse unsichtbar! Positive und negative Anteile addieren sich zu null, und zwar über das ganze Bild! Nur wenn man genügend weit von der Seite schaut, das heisst mit Winkel grösser als 45 Grad von der z-Achse, sieht man sie im Bild. (Für andere Winkel lassen sich ähnliche Konusdichten konstruieren.) Ohne das mathematische Argument wäre es sicher nicht so einfach gewesen, eine solche Verteilung zu konstruieren.

Die im Bild gezeigte Konusdichte enthält viel Licht nahe der äquatorialen (R-)Ebene. Dies entspricht einer rotationssymmetrischen, scheibenartigen Sternverteilung. Eine Sternscheibe ist auch oftmals die Erklärung für die beobachteten einprozentigen Abweichungen von der Ellipsenform. Die Abbildung zeigt, dass die Amplituden solcher Scheiben nur selten genau bestimmt werden können, wenn man nicht über zusätzliche Informationen verfügt, in diesem Fall Messungen von Sterngeschwindigkeiten.

Dieses Beispiel ist charakteristisch für eine Reihe astronomischer Probleme, bei denen eine beobachtete Grösse über einen Integraloperator mit der dreidimensionalen, realen Verteilung zusammenhängt. Letztere aus den Beobachtungsdaten zu bestimmen, ist ein so genanntes inverses Problem, für dessen Eigenschaften es mathematische Theorien gibt. Bei der Anwendung muss man noch berücksichtigen, dass die beobachteten Grössen nur innerhalb gewisser Unsicherheiten bekannt sind. In solchen Fällen löst man das inverse Problem im statistischen Sinn, was oft komplizierte nummerische Verfahren erfordert.



Eines unserer Forschungsprojekte hat zum Ziel, die Verteilung der mysteriösen dunklen Materie in elliptischen Galaxien aufzuklären und dadurch etwas über die Entstehung dieser Objekte im frühen Kosmos zu lernen. Auch dabei mussten Probleme umschifft werden, die aus der Tatsache herrühren, dass Sterngeschwindigkeiten nur projiziert beobachtbar sind. Einzelheiten siehe unter www.astro.unibas.ch/forschung/og/ellipse.shtml

Prof. Ph.D. Ortwin Gerhard ist Extraordinarius für Astronomie am Astronomischen Institut der Universität Basel.

Abbildung 1: Schnitt durch eine so genannte Konusdichte, die man sich rotationssymmetrisch um die z-Achse vorstellen muss. Die Skalierung der Achsen ist in kpc; 1 kpc entspricht ca. 3000 Lichtjahren oder 3 x 10^{21} cm. Durchgezogene und gepunktete Linien sind Linien konstanter positiver bzw. negativer Dichte. Für bestimmte Projektionsrichtungen ist diese Verteilung im Bild unsichtbar; siehe Text.

Öffentliche Geheimhaltung

Hanspeter Kraft

Die *Informationstheorie* beschäftigt sich mit der örtlichen und zeitlichen Übertragung von Information. Ein zentrales Teilgebiet ist die *Kryptographie*, welche sich mit der Sicherheit der Datenübertragung befasst, insbesondere also mit der Problematik der passiven Beeinträchtigung der Übermittlung durch Abhören und der aktiven Beeinflussung durch Fälschen. Bei all diesen Theorien spielt die Mathematik eine wichtige Rolle.

Geheimhaltung und Authentizität

Zwei grundsätzliche Fragen stehen im Vordergrund, nämlich die Frage der Geheimhaltung und die Frage der Authentizität:

– *Geheimhaltung*: Wie stellt der Sender sicher, dass nur der vorgesehene Empfänger die Nachricht lesen kann?
– *Authentizität*: Wie stellt der Empfänger sicher, dass die Nachricht vom angegebenen Sender stammt?

Diese Problematik ist keineswegs neu; sie hat die Geheimdienste aller Länder seit jeher beschäftigt. Mit der globalen Vernetzung und den beinahe unbeschränkten Möglichkeiten des Informationsaustausches, etwa per E-Mail oder über das Internet, hat diese Problematik jedoch völlig neue und ungeahnte Dimensionen angenommen.

Moderne Kryptographie

Was ist neu in der heutigen Situation, im Unterschied zur klassischen (meist militärischen) geheimen Nachrichtenübertragung?

– Die möglichen Gesprächspartner sind nicht zum Vorneherein schon festgelegt. Im Prinzip möchte jeder mit jedem sicher kommunizieren können.
– Die verwendeten Übertragungsmedien (elektrische Leitungen, Glasfaser, elektromagnetische Wellen, via Satellit) sind öffentlich, und die Netzwerke sind unüberschaubar. Der Benutzer muss damit rechnen, dass sie leicht abgehört werden können.

Die globale Verfügbarkeit von Information kommt also einher mit der wachsenden Unsicherheit, ob die erhaltene Information auch stimmt und vom angegebenen Absender stammt und ob umgekehrt die gesendete Information unverfälscht am richtigen Orte ankommt.

Man denke dabei etwa an die Benutzung von Kreditkarten bei Bankautomaten oder in Geschäften, an die Bestellung und Bezahlung von Waren über das Internet (E-Commerce), an die elektronische Börse, an den Schutz vor Kopien, an das Signieren von Verträgen über Netzwerke, an elektronische Abstimmungen und so weiter.

Sicherheit

Eine erste mögliche Massnahme zur Absicherung gegen Missbrauch ist das systematische Sammeln (und Speichern) von Informationen über die Vertragspartner (Kreditwürdigkeit!). Was dies tatsächlich bedeutet ist jedoch den meisten nicht bewusst:

– Ihre Kreditkartenfirma weiss genau, wann und wo Sie in den Ferien waren, was Ihr Hotel gekostet hat, in welchen Restaurants Sie essen gehen, wo Sie Ihre Kleider kaufen und wofür Sie wie viel Geld ausgeben.
– Damit der Betreiber Ihres Mobiltelefons genau abrechnen kann, macht er eine sorgfältige Aufzeichnung Ihrer Telefongespräche und kann damit problemlos Ihre dienstlichen Reiseaktivitäten rekonstruieren.
– Mit Kundenkarten der Form «Cumulus» speichern Firmen Ihr Kaufverhalten und benützen dies, um ihr Angebot (und die Preise) zu optimieren.
– Der Betreiber Ihres Kabelfernsehens kann problemlos feststellen, welche Sender und Programme Sie regelmässig anschauen.

Nimmt man alle diese Informationen zusammen, so kann man ein sehr detailliertes «Profil» von Ihnen erstellen, das Ihre Lebensgewohnheiten beinhaltet und Ihr Verhalten in bestimmten Situationen voraussagt. Von hier ist der Schritt zur unbemerkten Beeinflussung und Kontrolle nur noch ein kleiner!

Öffentliche Schlüssel

Es herrscht allgemein die Ansicht, dass diese Problematik in der Natur der Sache liegt, dass man sich also gegen Missbrauch nur absichern kann, wenn man bereit ist, gewisse Informationen über sich selbst preiszugeben.

Das Erstaunliche ist nun, dass diese Ansicht falsch ist. Die mathematische Theorie der «Public Keys» (d.h. der öffentlichen Schlüssel) ermöglicht einen sicheren Datenaustausch zwischen beliebigen Partnern, ohne dass die beiden sich kennen und persönliche Daten und Referenzen preisgeben müssen. Mehr noch, die Methode erlaubt auch die sichere und vertrauliche Verwendung von «digitalem Geld», das heisst die Bezahlung mit einer Art Kreditkarte, wobei das Kreditinstitut die Summe risikolos garantieren kann, ohne den Empfänger des Geldes zu kennen!

Es ist mir klar, dass das sehr unglaubwürdig tönt; es scheint dem gesunden Menschenverstand völlig zu widersprechen! Umso grossartiger ist die bahnbrechende Arbeit der beiden Mathematiker W. Diffie und M.E. Hellman aus dem Jahre 1976, in der die Idee des öffentlichen Schlüssels eingeführt und verschiedene Realisierungen dargestellt werden.

In den folgenden Abschnitten möchte ich diese geniale Idee an ein paar einfachen Beispielen vorstellen und erläutern. Zunächst müssen wir uns kurz über die Grundprinzipien der geheimen Nachrichtenübertragung unterhalten.

000101

Tafel I

Eine einfache Blockchiffer

Die Nachricht N sei als Folge von Ziffern gegeben, etwa

$$N = 13859834138728774128347712 3667.$$

Als Schlüssel verwenden wir die ersten 10 Stellen der Zahl

$$\pi = 3,141592653\ldots$$

(jede andere 10-stellige Zahl erfüllt den gleichen Zweck).

Der Algorithmus besteht darin, die obige Folge N in 10er-Blöcke einzuteilen und zu jedem Block den Schlüssel zu addieren, wobei die Addition ziffernweise erfolgt und die Überträge ignoriert werden, also 6 + 7 = 3 gesetzt wird:

Klartext: $N =$ 1385983413 '8728774128 '3477123667
Schlüssel: $S =$ 3141592653 '3141592653 '3141592653
Chiffrat: $N + S =$ 4426475066 '1869266771 '6518615210

Falls der Empfänger den Schlüssel S kennt, so kann er aus dem Chiffrat den Klartext N wieder herstellen, nämlich durch blockweise Subtraktion von

$$S = 3141592653,$$

wobei wiederum ziffernweise subtrahiert wird und gegebenenfalls 10 addiert wird, also 3 – 5 = –2 = 8 gesetzt wird:

Chiffrat: $C =$ 4426475066 '1869266771 '6518615210
Schlüssel: $S =$ 3141592653 '3141592653 '3141592653
Klartext: $C - S =$ 1385983413 '8728774128 '3477123667

Geheime Nachrichtenübertragung

Um Information vom Sender zum Empfänger zu transportieren, wird diese zunächst *digitalisiert*. Dies bedeutet, dass der Text oder das Bild (oder die akustischen Signale) mittels eines elektronischen Gerätes (z.B. eines Computers) und geeigneter Software in eine Bitfolge, d.h. in eine Folge 00101101010011000101010010 01 … von Nullen und Einsen verwandelt wird. Diese Folge wird portionenweise über das Netzwerk verschickt und vom Empfänger mit entsprechendem Gerät und Software in die ursprüngliche Information zurückverwandelt. Dazu ist es gar nicht nötig, im Detail zu wissen, mit welchen Geräten und welcher Software die Digitalisierung gemacht wurde: Für Experten ist es kein Problem, aus der Bitfolge die ursprüngliche Information wieder herzustellen.

Chiffrierung

Für die *geheime* Nachrichtenübertragung braucht man daher eine «Chiffrierung». Darunter versteht man ein Verfahren, welches die gegebene Bitfolge, den *Klartext*, in eine neue Bitfolge, das *Chiffrat*, verwandelt und dieses an den Empfänger verschickt. Diese Umwandlung erfolgt nach einem wohldefinierten (bekannten) Algorithmus unter Verwendung eines (geheimen) *Schlüssels*, welcher in der Praxis selbst eine Bitfolge von bestimmter Länge ist. Verfügt der Empfänger ebenfalls über diesen Schlüssel, so kann er den Klartext wieder herstellen und somit die Nachricht entziffern (siehe Tafel I).

Solche Verfahren werden durch integrierte Schaltungen (Chips) und spezielle Software geliefert. Ein bekannter Chiffrieralgorithmus ist der DES (= Data Encryption Standard); er ist in vielen Geräten fest eingebaut.

Es gibt heute absolut sichere Chiffrierverfahren, mit denen schnell und risikolos über öffentliche Leitungen geheime Nachrichten übertragen werden können. Hierzu müssen allerdings Sender und Empfänger über einen *gemeinsamen geheimen Schlüssel* verfügen.

Die zentralen Probleme bei der geheimen Nachrichtenübertragung liegen nicht beim Chiffrierverfahren, sondern beim *Schlüsselaustausch* und bei der *Schlüsselverwaltung*.

Öffentlicher Schlüsselaustausch

Eine unglaubliche Geschichte

Stellen Sie sich nun folgende Situation vor. In einem grossen Raum sitzen viele Leute, alle mit einem Laptop und geeigneter Software ausgerüstet und alle auf dem gleichen Wissensstand. Nun möchte ein beliebiges Paar im Raum, etwa Alice und Bob, einen geheimen Schlüssel austauschen. Die beiden kennen sich nicht und haben bisher nie miteinander geredet.

Nun beginnen die beiden einen öffentlichen Dialog, der von allen Anwesenden mitgehört wird. Am Schluss haben Alice und Bob einen gemeinsamen geheimen Schlüssel, etwa eine 200-stellige Zahl, und keiner der Anwesenden hat die geringste Chance, diesen Schlüssel herauszufinden!

Wenn man dies zum ersten Mal hört, dann glaubt man das nicht. Im Gegenteil, es ist doch offensichtlich, dass dies nicht gehen kann, denn die Unterhaltung ist ja öffentlich, und deshalb sind alle Leute auch nach der Diskussion auf dem gleichen Kenntnisstand. Dass dies trotzdem möglich ist, beruht auf der schon oben angedeuteten genialen Idee der beiden Mathematiker Diffie und Hellman, die ich nun erläutern möchte. Dazu sind ein paar einfache «mathematische» Vorbereitungen nötig.

Mathematische Grundlagen

Die Grundlage für diese Methode ist das *Rechnen modulo N*, wobei *N* eine positive, meist sehr grosse Zahl ist (siehe Tafel II). Beim obigen Beispiel eines Chiffrierverfahrens haben wir z.B. die Ziffern modulo 10 addiert, d.h. wir haben mit nur einer Stelle gerechnet und alle Vielfachen von 10 ignoriert.

Das Rechnen modulo *N* eignet sich besonders für den Umgang mit grossen Zahlen. Andernfalls läuft man Gefahr, besonders beim Multiplizieren und Potenzieren, dass die Zahlen zu gross werden und nicht mehr gespeichert werden können. Im Folgenden ist das *Potenzieren modulo N* von entscheidender Bedeutung, also das Berechnen von Potenzen der Form $a^n = a\,a\,a\,a\,\ldots\,a \mod N$. Dabei wird die Zahl *a* sukzessive mit sich selber multipliziert, und zwar *n*-mal.

Tatsache 1:
Ein heutiger Laptop kann sehr schnell modulo *N* potenzieren, das heisst Zahlen der Form $a^n = a\,a\,a\,a\,\ldots\,a \pmod N$ ausrechnen. Für 1000-stellige Zahlen *a*, *n* und *N* dauert dies nur wenige Millisekunden.

Dies ist keineswegs offensichtlich. Würde man nämlich die Zahlen sukzessive miteinander multiplizieren, so müsste man *n* Multiplikationen von grossen Zahlen durchführen, und dies würde bei 1000-stelligen Zahlen selbst auf den schnellsten heutigen Rechnern etwa 10^{100} Jahre dauern! Dass dies so viel rascher geht, beruht auf einer sehr intelligenten Methode des Potenzierens, bei der die Anzahl der notwendigen Multiplikationen nur etwa der Stellenanzahl des Exponenten entspricht (siehe Tafel III).

Man beachte: 10^{100} ist eine Eins mit 100 Nullen!

Tafel II

Das Rechnen modulo *N*

Das Rechnen mit ganzen Zahlen modulo *N* besteht darin, dass man nach dem Ausführen der Rechenoperation vom Ergebnis so oft mal *N* subtrahiert (oder addiert, falls das Ergebnis negativ ist), bis man eine Zahl zwischen 0 und *N* erreicht.
$5 + 8 = 3 \pmod{10}$; $7 \cdot 8 = 1 \pmod{11}$
$3^3 = 1 \pmod{13}$, $(-11) \cdot 9 = 1 \pmod{100}$
Ist $N = 10^n$, das heisst eine 1 mit *n* Nullen, so bedeutet das Rechnen modulo *N*, dass man vom Ergebnis nur die letzten n Stellen betrachtet und alle anderen ignoriert.
$2^{10} = 24 \pmod{1000}$
In den Anwendungen ist *N* eine sehr grosse Zahl (mehrere hundert bis tausend Stellen). Dies hat den Vorteil, dass man zwar mit sehr grossen Zahlen arbeitet, die Grösse aber dennoch bei allen Rechenoperationen beschränkt bleibt, nämlich $\leq N$.

Tafel III

Schnelles Potenzieren

Das Potenzieren a^n kann auch für grosse Exponenten *n* sehr schnell durchgeführt werden. Ist zum Beispiel $n = 128$, so scheint man für die Berechnung von a^{128} total 127 Multiplikationen zu benötigen. In Tat und Wahrheit kommt man mit 7 Multiplikationen aus! Es gilt nämlich
$(((((((a^2)^2)^2)^2)^2)^2)^2 = a^{2^7} = a^{128}$
das heisst, man quadriert 7-mal hintereinander.

Ist der Exponent keine Zweierpotenz, so benutzt man die duadische Zerlegung. Es ist zum Beispiel $100 = 2^6 + 2^5 + 2$. Damit findet man durch «optimales Ausklammern»
$100 = 2^6 + 2^5 + 2 = ((2 + 1)2^4 + 1)2$
und erhält
$a^{100} = ((a^2 \cdot a)^{2^4} \cdot a)^2$,
was total 8 Multiplikationen benötigt!

Die Umkehrung des Potenzierens, also die Bestimmung des Exponenten n aus dem Ergebnis $b = a^n \pmod N$, heisst *diskreter Logarithmus*: $n = \log_a b \pmod N$.

Tatsache 2:
Es sind keine schnellen Algorithmen für die Berechnung des diskreten Logarithmus $\log_a b \pmod N$ bekannt. Für 200-stellige Zahlen a, b und N würden die schnellsten heutigen Rechner etwa 10^{100} Jahre brauchen.

Man beachte, dass dies eine gänzlich andere Aussage ist als die Tatsache 1! Die Mathematiker vermuten zwar, dass es keine schnellen Algorithmen für den diskreten Logarithmus gibt, aber bisher ist kein Beweis dafür gelungen.

Was hier vorliegt, ist eine so genannte *Einwegfunktion*, also eine Funktion – hier das Potenzieren $p(n) = a^n \pmod N$ mit dem Exponenten n –, die man auch für sehr grosse Werte von n schnell berechnen kann, deren Umkehrfunktion – hier der diskrete Logarithmus $l(b) = \log_a b \bmod N$ – jedoch nicht innert nützlicher Zeit berechenbar ist.

Das Verfahren

Damit haben wir alle Begriffe zusammen, um den oben angedeuteten *öffentlichen Schlüsselaustausch* zu beschreiben. Wir kehren zurück zu Alice und Bob und erleben folgenden Ablauf:

- Als erstes werden *öffentlich* zwei etwa 200-stellige Zahlen a und N bekannt gegeben, wobei a kleiner als N ist.
- Nun wird Alice gebeten, sich *im Geheimen* eine Zahl n der gleichen Grössenordnung zu notieren, und die gleiche Aufforderung geht an Bob, der sich eine Zahl m notiert. (Die Zahl n kennt also nur Alice und m kennt nur Bob, während die Zahlen a und N öffentlich bekannt sind.)
- Nun wird Alice aufgefordert, mit ihrem Laptop die Potenz $p = a^n \pmod N$ zu berechnen. Entsprechend berechnet Bob die Potenz $q = a^m \pmod N$. (Wie wir oben in «Tatsache 1» bemerkt haben, ist diese Berechnung leicht und schnell möglich.)
- Diese beiden Ergebnisse p und q werden nun zwischen Alice und Bob öffentlich ausgetauscht. Jedermann kennt also diese beiden Zahlen. (Wir haben oben in «Tatsache 2» bemerkt, dass es den Anwesenden (ausser Alice bzw. Bob) dennoch unmöglich ist, innert nützlicher Frist aus diesen Angaben die geheimen Zahlen n von Alice beziehungsweise m von Bob zu berechnen.)
- Nun nimmt Alice die Zahl q von Bob und berechnet, unter Benutzung ihrer geheimen Zahl n, die Potenz $s = q^n \pmod N$. Das entsprechende tut Bob: Er nimmt die Zahl p von Alice und berechnet $t = p^m \pmod N$. (Da die Zahlen n und m geheim sind, kann niemand anders diese Berechnung durchführen.)
- Behauptung: *Es gilt $s = t$, und dies ist der gemeinsame geheime Schlüssel*, den nur Alice und Bob kennen! Der Beweis beruht auf elementarem Potenzrechnen: $s = q^n = (a^m)^n = a^{(mn)} = a^{(nm)} = (a^n)^m = p^m = t \pmod N$

Eine typische Anwendung

Wenn man auf dem Internet Zahlungen und Bankgeschäfte erledigt, so verwendet man üblicherweise Passwörter. Nun muss man aber bedenken, dass der Verkehr auf dem Internet öffentlich ist und von einem Hacker leicht abgehört werden kann. Insbesondere kann dieser den Login-Namen und das Passwort herausfinden und den ganzen Datenverkehr mitverfolgen.

Um dies zu vermeiden, wird anders vorgegangen. Sobald man die entsprechende Stelle auf der Homepage der Bank anklickt, führen der Bankcomputer und der eigene PC einen öffentlichen Schlüsselaustausch durch, etwa nach dem oben beschriebenen Schema, und produzieren so einen gemeinsamen geheimen Schlüssel. Dieser wird dann benutzt, um mit einem bekannten Chiffrierverfahren, etwa dem DES, die weiteren Informationen verschlüsselt über das Internet zu schicken. (Voraussetzung ist natürlich, dass auf den verwendeten Computern die notwendige Software installiert ist, was bei den bekannten Browsern heute der Fall ist.)

Das gleiche Verfahren wird benutzt, wenn man über das Internet einkauft und dabei seine Kreditkartennummer sowie weitere persönliche Informationen mitteilt. Auch hier wird zunächst ein Schlüssel ausgetauscht und dann mit einem bekannten Chiffrierverfahren der weitere Datenverkehr verschlüsselt über das Netz gesendet.

Public Keys (öffentliche Schlüssel)

Die bisher betrachteten Chiffrierverfahren haben eines gemeinsam, nämlich dass man für das Verschlüsseln und das Entschlüsseln denselben Schlüssel benutzt. Wollen also 1000 Personen auf einem Netzwerk sicher miteinander kommunizieren, so muss für jedes Paar von Benutzern ein geheimer Schlüssel zur Verfügung gestellt werden, was total etwa eine halbe Million Schlüssel ergibt. Auf dem Netzwerk einer grossen Organisation oder gar auf dem Internet ist dies völlig undenkbar, nicht nur wegen der grossen Anzahl der Schlüssel, sondern vor allem wegen der Frage, wie man diese Schlüssel verwaltet und verteilt.

Wiederum legt dies die Schlussfolgerung nahe, dass das in der Natur der Sache liegt, dass es also keine sichere und geheime weltweite Kommunikation etwa via E-Mail geben kann. Und auch diese Schlussfolgerung ist falsch! Es waren ebenfalls die beiden Mathematiker Diffie und Hellman, die eine überraschende und wiederum geniale Lösung vorschlugen, nämlich die Idee des *öffentlichen Schlüssels*.

Die Grundidee

Die Grundidee ist sehr einfach: *Man finde ein Chiffrierverfahren mit ZWEI Schlüsseln, einem öffentlichen Chiffrierschlüssel zum Verschlüsseln und einem geheimen Dechiffrierschlüssel zum Entschlüsseln, wobei es auch bei Kenntnis des Chiffrierschlüssels (aber ohne Kenntnis des Dechiffrierschlüssels!) nicht möglich ist, einen verschlüsselten Text innert nützlicher Frist zu entziffern.*

Mit anderen Worten, mit dem Chiffrierschlüssel kann man chiffrieren, aber nicht dechiffrieren; das Chiffrierverfahren ist also eine *Einwegfunktion*, wie wir sie oben beim öffentlichen Schlüsseltausch kennen gelernt haben. Allerdings braucht man noch eine geheime Hintertür, welche es dank zusätzlichen Kenntnissen erlaubt, die Umkehrfunktion doch zu berechnen. Solche Funktionen haben den Namen «one-way trap door function» erhalten.

Wenn es so ein Verfahren gäbe, so wäre damit das Problem der geheimen Übermittlung von Nachrichten gelöst. Jeder potentielle Benutzer würde ein solches Paar von Schlüsseln kreieren, den Chiffrierschlüssel öffentlich bekannt geben, zum Beispiel im Telefonbuch, und den Dechiffrierschlüssel geheim halten. Will nun Alice an Bob eine Nachricht schicken, so verwendet sie den im Telefonbuch unter Bob angegebenen Schlüssel, um diese zu verschlüsseln. Dann ist sichergestellt, dass nur Bob diese Nachricht lesen kann.

Das tönt zwar sehr überzeugend, doch kann man sich nicht vorstellen, dass es so ein Verfahren gibt.

Das RSA-Kryptosystem

Im Jahre 1978 haben R.L. Rivest, A. Shamir und L.M. Adleman, drei Mathematiker am MIT, ein solches Verfahren angegeben. Es läuft heute unter dem Namen *RSA-Kryptosystem* und dient vor allem der Übermittlung von Schlüsseln für die klassischen Chiffrierverfahren, aber auch der Authentifizierung von Nachrichten und als digitale Unterschrift. Auf dieser Methode beruht die Sicherheit der heutigen Netzwerkkommunikation, insbesondere auf dem Internet. Ein solches Programm, das vor allem bei der E-Mail eingesetzt wird, ist öffentlich und läuft unter dem Namen «pgp» (= pretty good privacy).

Zur Beschreibung der RSA-Methode benutzen wir wiederum das Rechnen modulo N und benötigen zudem etwas elementare Zahlentheorie. (Die mathematischen Details werde ich im Folgenden unterschlagen.)

– Alice wählt zwei grosse Primzahlen p und q (etwa 150 Stellen) und berechnet die beiden Produkte $N = p \cdot q$ und $R = (p\text{-}1)(q\text{-}1)$. Weiter wählt Alice eine beliebige Zahl $d < N$ von der gleichen Grössenordnung, welche zudem zu R teilerfremd ist.
– Nun gibt Alice das Paar der Zahlen d und N öffentlich bekannt. Dieses Paar (d, N) bildet den *öffentlichen Schlüssel*.
– Das Chiffrierverfahren besteht nun in Folgendem: Will Bob die Zahl x ($< N$) an Alice übermitteln, so berechnet er die Potenz $y = x^d \pmod N$ und sendet dann die Zahl y an Alice. (Entsprechend wie beim diskreten Logarithmus ist es nicht möglich, aus der Kenntnis von y, d und N die Zahl x innert nützlicher Frist zu berechnen.)
– Alice kennt auch die Zahl R und bestimmt damit eine Zahl f mit der Eigenschaft, dass $d \cdot f = 1 \pmod R$ gilt. (Diese Berechnung ist mit wenig Aufwand möglich.)
– Behauptung: Es gilt $y^f = x \pmod N$. Also kann Alice aus der empfangenen Zahl y das ursprüngliche x bestimmen!

(Der Beweis dieser Behauptung beruht auf einem Satz von Euler, welcher den bekannten «Kleinen Satz von Fermat» verallgemeinert, siehe Tafel IV)

Bei der obigen Beschreibung wurde noch nicht klar gesagt, wieso nur Alice x aus y berechnen kann. Der Grund ist der folgende: Das einzige bekannte Verfahren besteht darin, dass man die Zahl $R = (p\text{-}1)(q\text{-}1)$ bestimmt und dann die Gleichung $d \cdot f = 1 \pmod R$ löst. Hierfür ist notwendig, dass man die beiden Primzahlen p und q kennt. Nun hat Alice aber nur das Produkt $N = p\,q$ bekannt gegeben. Es geht also darum, die Primzerlegung dieser etwa 300-stelligen Zahl zu bestimmen. Und hier liegt der entscheidende Punkt: Auch mit den schnellsten heutigen Rechnern und den besten bekannten Verfahren würde dies über 10^{10} Jahre dauern!

Authentifizierung und digitale Unterschrift

Die RSA-Methode lässt sich auch für die Authentifizierung von öffentlichen Informationen verwenden (digitale Unterschrift). Dabei geht es um folgendes Problem.

Alice möchte eine Nachricht verbreiten und zwar so, dass jedermann sicherstellen kann, dass die Nachricht wirklich von Alice stammt. Hierzu geht Alice folgendermassen vor:

– Auf den Text der Nachricht wendet Alice eine so genannte Hash-Funktion an, welche ebenfalls öffentlich bekannt ist und leicht berechnet werden kann. Das Ergebnis ist eine Zahl y.
– Nun berechnet Alice die Zahl $x = y^f \pmod N$ unter Verwendung ihres *geheimen* Schlüssels f. Diese Zahl x wird dann an den veröffentlichten Text angehängt.
– Die Kontrolle für Bob besteht nun darin, dass er die (bekannte) Hash-Funktion auf den Text anwendet und das Ergebnis y mit der Potenz $x^d \pmod N$ unter Verwendung des öffentlichen Schlüssels (d, N) von Alice vergleicht. Sind die beiden Resultate gleich, so kann die Nachricht nur von Alice stammen, denn nur Alice kennt den Dechiffrierschlüssel f und kann daher aus dem Wert y der Hash-Funktion die Zahl $x = y^f \pmod N$ berechnen.
– Gleichzeitig ist damit auch nachgewiesen, dass der Text nicht verändert wurde, da sonst die Hash-Funktion einen anderen Wert angenommen hätte.

Dies ist nur eine der unzähligen Möglichkeiten, wie die RSA-Methode und die Idee der öffentlichen Schlüssel in intelligenter Weise eingesetzt werden kann. Alle am Anfang erwähnten Probleme (elektronische Abstimmungen, Signieren von Verträgen usw.) haben damit Lösungen gefunden.

Schlussbemerkung
Die Sicherheit des öffentlichen Schlüsselaustausches und des RSA besteht darin, dass für bestimmte zahlentheoretische Aufgaben (diskreter Logarithmus bzw. Primzahlzerlegung) keine schnellen Algorithmen bekannt sind. Es ist allerdings nicht *bewiesen*, dass es keine solchen gibt. Eine gewisse Unsicherheit ist also vorhanden. Dazu kommt noch das Problem, dass die Forschung auf diesem Gebiet auch an Orten passiert, welche striktester Geheimhaltung unterliegen. (Man vergleiche hierzu auch den folgenden Abschnitt.)

Addendum

Zur Geschichte
(von Geheimdiensten und Spionen)
Die Idee der öffentlichen Kryptographie entstand lange vor der Erfindung des Internets. Niemand hätte damals daran gedacht, welche zentrale Rolle sie schon 20 Jahre später spielen wird! Whitfield Diffie war ein junger Hacker und Martin Hellman Professor an der Stanford University. Ihre geniale Entdeckung hat eine völlig neue Ära der modernen Kryptographie eingeleitet. Sie lag keineswegs in der Luft; die beiden waren ihrer Zeit weit voraus.

Aber waren sie auch wirklich die ersten?

Nein, die öffentliche Kryptographie wurde schon früher, nämlich 1970, von Mitarbeitern des Britischen Geheimdienstes, J. Ellis, C. Cocks und M. Williamson, entdeckt und beschrieben. Auch die RSA-Methode war ihnen bereits 1973 bekannt. Aber erst 1997 wurden die Archive geöffnet und die «Helden» durften reden. Doch inzwischen war J. Ellis schon gestorben.

Diffie und Ellis trafen sich allerdings bereits 1982 und wurden später gute Freunde. Anscheinend hat sich Ellis nie dazu geäussert, dass ihm für seine wirklich revolutionäre Entdeckung die verdiente Würdigung zeitlebens vorenthalten wurde.

(Einen kurzen Bericht über diese Ereignisse findet man auf dem Internet unter
www.wired.com/wired/archive/7.04/crypto_pr.html.)

Quantum Computing
Seit ein paar Jahren denken Physiker und Mathematiker intensiv über den Quantencomputer nach. Ein solcher würde völlig neue Algorithmen zulassen, insbesondere auch zahlentheoretische, die die Zerlegung von grossen Zahlen in Primfaktoren in polynomialer Zeit ermöglichen würden. Damit wäre die Sicherheit des RSA klar in Frage gestellt. Die Experten sind sich allerdings nicht einig, ob es je einen funktionierenden Quantencomputer von der notwendigen Kapazität geben wird. Die Theorie ist auf jeden Fall faszinierend, die bisher erreichten experimentellen Resultate sind (noch) nicht sehr viel versprechend. Die NSA (National Security Agency in den USA) scheint allerdings etwas nervös zu sein!

Ich danke meinem Kollegen Prof. Ueli Maurer von der ETH Zürich für wertvolle Hinweise.

Prof. Dr.phil. Hanspeter Kraft ist Ordinarius für Mathematik am Mathematischen Institut der Universität Basel.

Tafel IV

Der Satz von Euler
Wir starten mit zwei verschiedenen,
ungeraden Primzahlen p und q und setzen $N = p \cdot q$.
Weiter sei s eine beliebige Zahl mit
$s = 1 \pmod R$,
wobei $R = (p-1)(q-1)$ ist.
Dann gilt für jede Zahl x:
$x^s = x \pmod N$.
Damit kann man das Dechiffrieren des
RSA erklären. Die beiden Zahlen d und f wurden
so gewählt, dass $d \cdot f = 1 \pmod R$ gilt.
Hieraus folgt durch einfaches Potenzrechnen:
$y^f = (x^d)^f = x^{d \cdot f} = x \pmod N$.

Die Variationsrechnung und ihre Basler Ursprünge

Alfred Wagner

Die Variationsrechnung gehört sicher zu den schönsten und elegantesten Zweigen der Mathematik. Sie stellt sich – vereinfacht gesprochen – die Aufgabe, in einer wohldefinierten Klasse von Objekten dasjenige zu finden, welches bezüglich eines vorgegebenen Kriteriums optimal ist. Ihre Ursprünge gehen bis ins Altertum zurück. Zu jener Zeit wurden bereits isoperimetrische Probleme untersucht, zum Beispiel, unter allen Körpern gleichen Volumens denjenigen zu finden, der die kleinste Oberfläche besitzt. Sie ist spätestens seit Beginn der Neuzeit von weitreichender Bedeutung in der Physik. So ist die klassische Mechanik ohne ihre Entwicklung im 19. Jahrhundert nicht denkbar. Umgekehrt hat sie aus der Physik immer wieder wichtige Impulse zu ihrer Weiterentwicklung empfangen.

Lange Zeit wurden variationelle Probleme geometrisch gelöst. Die Geschichte dieser Periode wird in diesem Artikel keine Berücksichtigung finden. Stattdessen betrachten wir die Variationsrechnung als ein Gebiet, welches seine Aussagen auf analytischen Beweisen aufbaut. Den Beginn dieser Geschichte kann man sehr genau datieren. Sie begann 1662 mit den ersten Arbeiten von Fermat über den Weg,. den das Licht bei der Durchquerung zweier optischer Medien nimmt. Wir werden im zweiten Kapitel näher darauf eingehen.

Basierend auf seinen Arbeiten entwickelten die Basler Brüder Bernoulli, namentlich Johann Bernoulli (1667 – 1748) und Jakob Bernoulli (1654 – 1705), einen ersten methodischen Zugang zur Lösung variationeller Probleme. Insbesondere Johann Bernoulli wird mit seiner Lösung des Problems der *Brachistochrone* im Mittelpunkt dieses Artikels stehen.

Das Problem erschien im Juni 1696 in den Acta Eruditorum – der ersten wissenschaftlichen Zeitschrift – und trug den Titel: «Einladung zur Lösung eines neuen Problems»:

Wenn in einer verticalen Ebene zwei Punkte A und B gegeben sind, soll man dem beweglichen Punkte M eine Bahn zuweisen, auf welcher er von A ausgehend vermöge seiner Schwere in kürzester Zeit nach B gelangt.

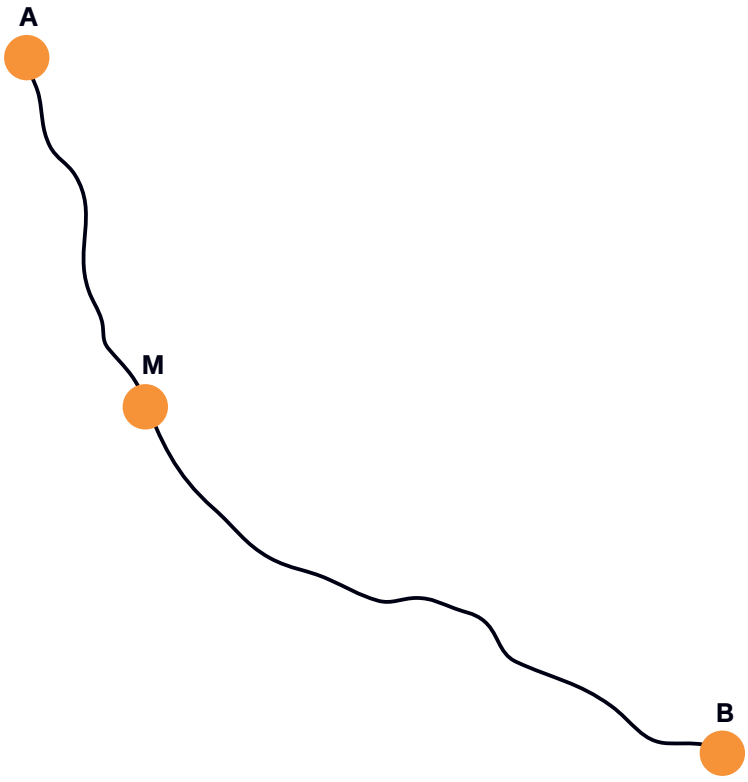


Abbildung 1: Zwei Punkte A, B werden durch einen Weg AMB verbunden.

Wenige Zeilen später warnt er:

Um einem voreiligen Urtheile entgegenzutreten, möge noch bemerkt werden, dass die gerade Linie AB zwar die kürzeste zwischen A und B ist, jedoch nicht in kürzester Zeit durchlaufen wird.

Der Vollständigkeit halber sollte erwähnt werden, dass Galileo Galilei (1564 – 1642) dieses Problem zum ersten Mal in einer seiner Arbeiten 1638 niederschrieb. Als Lösung gab er an, dass die gesuchte Kurve ein Kreisbogen ist, der die beiden Punkte verbindet. Diese Lösung ist jedoch einschliesslich der Beweisidee falsch, weshalb wir diese Arbeit nicht weiter beachten.

Johann Bernoulli kannte Galileis Arbeit wahrscheinlich nicht, und auch der Name Brachistochrone (von *brachystos* = kürzeste und *chronos* = Zeit) geht wohl auf ihn zurück.

Er kündigte an, dass er die Lösung dieses Problems am Ende des Jahres bekannt geben werde, falls kein anderer sie bis dahin gefunden habe. Zu diesem Zeitpunkt gab es zwei Personen, die im Besitz einer korrekten Lösung waren: Johann Bernoulli und Gottfried Wilhelm Leibniz (1646 – 1716). Leibniz war eine der faszinierendsten Persönlichkeiten seiner Zeit. Ausgebildet als Jurist und Diplomat, lernte er in Paris Huygens kennen und wurde durch ihn für die Mathematik begeistert. Innerhalb kürzester Zeit erreichte er ein tiefes Verständnis für den damaligen Stand der Forschung und begann selbst zu veröffentlichen. Ein Höhepunkt war ohne Zweifel die Veröffentlichung des «Calculus», in dem er die Infinitesimalrechnung entwickelte. Sie war es, die ihn in der Folge zum Gegenspieler von Isaac Newton werden liess.

Johann Bernoulli hatte ihm schon vorab, am 9.6.1696, dieses Problem zugeschickt und bekam postwendend am 16.6.1696 (!) eine korrekte Lösung geliefert. Leibniz schlug nicht nur die Veröffentlichung dieses, wie er fand, sehr schönen Problems vor, sondern legte auch eine Liste von Mathematikern vor, die er für geeignet hielt, das Problem zu lösen. Die Liste umfasste vier Namen: L'Hospital, Jakob Bernoulli (Johanns Bruder), Hudde (zu der Zeit Bürgermeister von Amsterdam) und Newton.

Da zur damaligen Zeit die Auslieferung der deutschen Zeitschrift ins Ausland sehr schleppend verlief, wurde im Dezember 1696 der Einsendeschluss auf Ostern 1697 verschoben. Endlich erschien in der Maiausgabe 1697 der Acta Eruditorum die Lösung von Johann Bernoulli. Die Ausgabe enthielt ebenfalls Jakob Bernoullis Lösung und eine Anmerkung von Leibniz, in der er seine Lösung skizzierte. Er verzichtete aber auf deren Veröffentlichung, da sie der von Bernoulli sehr ähnlich war.

Das gespannte Verhältnis zwischen Jakob und Johann Bernoulli tritt in dem Begleitschreiben Jakobs zutage, in dem er behauptet, die Herausforderung seines Bruders (Johann) interessiere ihn überhaupt nicht. Nur deshalb habe er eine Lösung eingeschickt, weil der grosse Leibniz zu diesem Wettbewerb eingeladen habe.

Neben einer Lösung von L'Hospital ging auch eine anonyme Schrift ein. Als Bernoulli sie analysierte, erkannte er – so behauptet er jedenfalls – Newton als Autor. *Tamquam ex ungue leonem*: an der Pranke will er den Löwen erkannt haben. In der Tat hatte Newton am 29.1.1697 das Heft der Philosophical Transactions der Royal Society, in dem die Aufgabe nun ebenfalls abgedruckt war, gelesen. Dies war gegen 16:00 Uhr, als er von seiner Arbeit als Master of the Mint kam. Er hatte das Problem am darauf folgenden Morgen gegen 4:00 Uhr früh gelöst und die Lösung dann anonym an die Redaktion der Royal Society geschickt. Warum anonym? Dem königlichen Astronomen Flamsteed teilte er später den Grund mit: Er liebe es nicht, von Ausländern gemahnt und geärgert zu werden, wenn es um Mathematik gehe.

Alle genannten Lösungen sind heute noch bekannt. Im Folgenden werden wir Johann Bernoullis Lösung vorstellen. Zunächst aber fragen wir: Was waren die Grundlagen, auf denen eine analytische Lösung gefunden werden konnte?

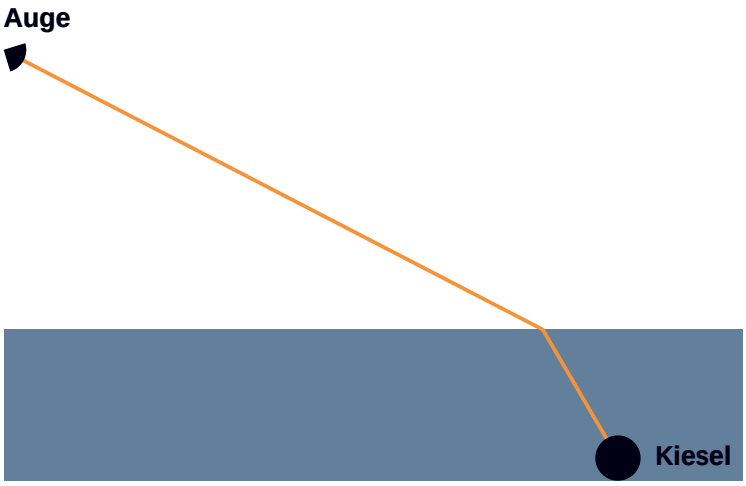


Abbildung 2: Lichtbrechung an einer Grenzschicht

Fermat und die Lichtbrechung

Pierre de Fermat (1601 – 1665) ist eigentlich als Begründer der analytischen Entwicklung der Variationsrechnung zu nennen. Seinem Beitrag liegt eine ganz alltägliche Erfahrung zugrunde. Sieht man zum Beispiel einen Kieselstein im flachen Wasser liegen und greift nach ihm, so greift man in der Regel fehl. Der Grund ist, dass das am Stein reflektierte Licht, welches unser Auge trifft (und damit den Stein «sichtbar» macht), im Wasser einen anderen Weg nimmt als in der Luft – also keinen geradlinigen Weg zu unserm Auge wählt. Dies nicht zu erkennen, verursacht den Fehlgriff. Welchen Weg aber nimmt Licht? Das der Erklärung zugrunde liegende *Fermatsche Prinzip* besagt Folgendes:

Ein Lichtstrahl, der unter einer vorgegebenen Nebenbedingung von einem Punkt P_1 zu einem Punkt P_2 gelangen soll, wählt immer den Weg, der die kürzeste Zeit benötigt.

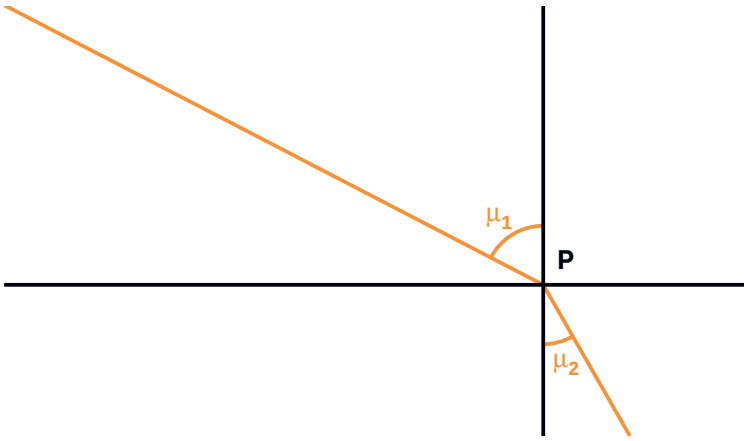


Abbildung 3: Das Brechungsgesetz.

Was bedeutet dies für unsere Beobachtung? Ein Lichtstrahl besitzt in verschiedenen Medien verschiedene Geschwindigkeiten, insbesondere ist die Geschwindigkeit im Wasser geringer als in der Luft. Wasser heisst deshalb auch «optisch dichter» als Luft. Wenn dies aber der Sachverhalt ist und wir das Fermatsche Prinzip akzeptieren, so wird der Lichtstrahl versuchen, eine kürzere Wegstrecke durch die Wasserschicht zu laufen als durch eine gleich dicke Luftschicht. Dies kann er dadurch erzielen, dass er einen kurzen Weg zur Wasseroberfläche sucht und von da aus geradlinig das Auge des Betrachters trifft. Es ist also zu erwarten, dass der Lichtstrahl «gebrochen» wird. Die Aufgabe besteht darin, den Punkt auf der Wasseroberfläche zu finden, der die Summe der beiden Durchlaufzeiten (durch Wasser und Luft) bei gegebenem Anfangspunkt (Kiesel) und Endpunkt (Auge) minimiert. Genau dies gelang Fermat analytisch zu quantifizieren:

Satz: *Sei P der Punkt auf der Wasseroberfläche, an dem der Lichtstrahl in die Luft eintritt. Errichte in diesem Punkt die Senkrechte und bezeichne mit μ_1 den Winkel zwischen ausfallendem Lichtstrahl in der Luft und der Senkrechten. Analog bezeichne μ_2 den Winkel zwischen einfallendem Lichtstrahl im Wasser und der Senkrechten. Weiter sei die Lichtgeschwindigkeit in der Luft mit c_1 und im Wasser mit c_2 bezeichnet. Dann gilt das Brechungsgesetz* $\frac{\sin \mu_1}{c_1} = \frac{\sin \mu_2}{c_2}$.

Wir wollen den Beweis von Fermat nicht nachvollziehen. Wichtig für unsere Geschichte ist, dass dieser Satz zusammen mit dem von Fermat gefundenen Beweis der damaligen mathematischen Gesellschaft bekannt war. Es ist zunächst aber gar nicht klar, warum dies für unser Problem von Bedeutung ist.

Das Problem der Brachistochrone

Die folgenden zwei Schritte enthalten die entscheidenden Ideen zur Lösung des Problems.

1. Schritt: Wir stellen uns vor, die gesuchte Kurve bestünde aus aneinander gereihten Stäben, die durch bewegliche Gelenke miteinander verbunden sind. Die Stäbe haben die Eigenschaft, ihre Länge frei zu variieren. Die Zahl der Stäbe wollen wir später festlegen. Die Gelenke sitzen auf untereinander angeordneten, horizontal gespannten Fäden und können auf ihnen horizontal nach rechts oder links gleiten. Wir können nun durch horizontale Verschiebung der Gelenke beliebig viele Kurven erzeugen, die alle die Punkte A und B miteinander verbinden.

2. Schritt: Die wichtige Einsicht, die Johann Bernoulli nun gewann, war: Angenommen wir haben alle Gelenke so platziert, dass die Durchlaufzeit des Massepunktes minimal ist, dann haben wir auch ein «lokales Problem» gelöst.

Gegeben seien drei benachbarte Gelenke G_1, G_2, G_3. Dann ist G_2 so platziert, dass die Durchlaufzeit eines Massepunkts, der von G_1 nach G_3 läuft, minimal ist.

Wäre dies nämlich nicht der Fall, so könnten wir bei festgehaltenen Gelenken G_1 und G_3 das mittlere Gelenk G_2 so positionieren, dass die Durchlaufzeit des Massepunkts, der von G_1 nach G_3 läuft, kürzer wird. Damit ist aber auch die Gesamtdurchlaufzeit verkürzt, also können die Gelenke nicht, wie vorausgesetzt, optimal platziert gewesen sein.

Betrachten wir das Problem von Fermat aus dem vorigen Kapitel, so sehen wir, dass das lokale Problem genau dem Problem der Lichtbrechung entspricht. Das Auge wurde durch das Gelenk G_1 ausgetauscht, während das Gelenk G_3 den Kiesel ersetzt. Folglich wissen wir, wie das Gelenk G_2 gesetzt sein muss, nämlich so, dass $\frac{\sin \mu_1}{c_1} = \frac{\sin \mu_2}{c_2}$ gilt. Hierbei sind natürlich c_1 und c_2 die Geschwindigkeiten des Massepunktes auf dem linken bzw. rechten Stab. Ansonsten sind die Winkel μ_1 und μ_2 wie oben definiert.

Wir sehen also, dass die Reduktion im ersten Schritt gemacht wurde, damit im zweiten Schritt durch eine Lokalisierung eine schon bekannte Situation erreicht wird. Wir können jetzt eine Beziehung für alle Gelenke ableiten. Tatsächlich ist es nämlich egal, welche drei benachbarten Gelenke wir auswählen. Dies führt sofort zu folgendem Resultat: *Es seien $G_1, \ldots, G_{n-1}$ Gelenke in optimaler Lage. Dann muss die Beziehung*

$$(1)\quad \frac{\sin \mu_1}{c_1} = \frac{\sin \mu_2}{c_2} = \ldots = \frac{\sin \mu_{n-1}}{c_{n-1}}$$

gelten.

Da das erste und letzte Gelenk gerade fest in den Punkten *A* und *B* liegen, können wir unser vereinfachtes Problem als gelöst betrachten, wenn wir die Geschwindigkeiten $c_1, \ldots, c_{n-1}$ bestimmt haben. Dies geschieht mit Hilfe des Fallgesetzes und soll hier nicht vertieft werden.

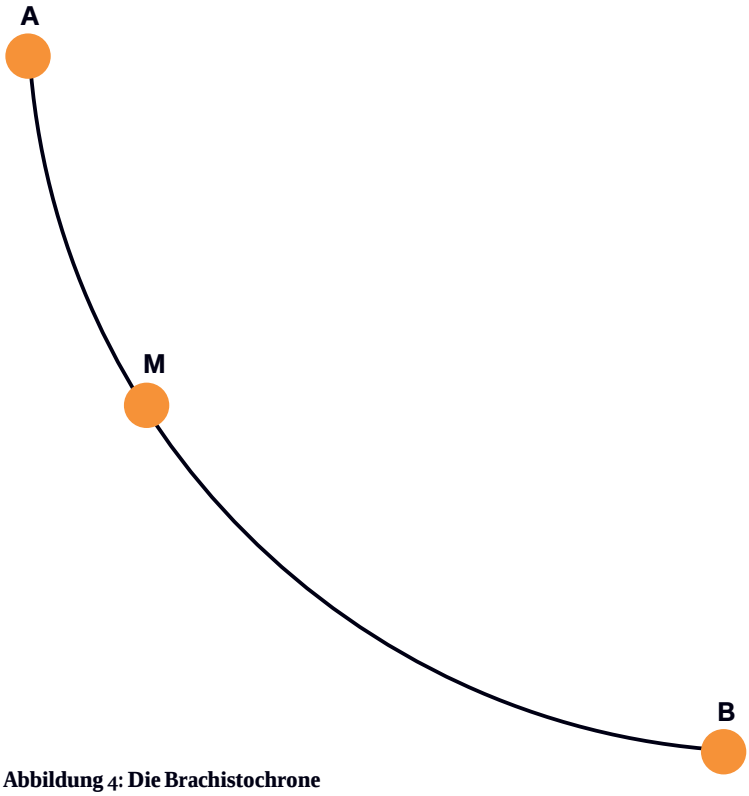


Abbildung 4: Die Brachistochrone

Wie gelangen wir nun zu einer Lösung des Brachistochrone-Problems? Die Idee besteht darin, die Zahl der Gelenke mit den Koordinaten immer weiter zu erhöhen. Im Grenzfall, in dem auf jedem Punkt der Kurve ein Gelenk sitzt, muss dann die Beziehung (1) immer noch gelten. Dies aber impliziert $\frac{\sin \mu_p}{c_p} = const.$ Dabei ist μ_p jetzt der Winkel zwischen der Geschwindigkeitsrichtung und der senkrechten Achse, und c_p beschreibt die Geschwindigkeit des Massepunkts im Punkt p der Kurve. Johann Bernoulli hat in der ersten Veröffentlichung bereits angekündigt, dass die Lösung eine den Geometern bekannte Kurve liefert. Und tatsächlich war die Kurve schon damals unter dem Namen *Zykloide* bekannt gewesen (siehe Abbildung 4). Wir haben damit den folgenden Satz bewiesen:

Satz: *Die Brachistochrone ist eine Zykloide.*

Abschliessend sollten wir kritisch bemerken, dass wir bezüglich des Grenzübergangs zu unendlich vielen Gelenken nicht besonders sauber argumentiert haben. Dies war mit den damaligen Mitteln (und nichts anderes haben wir benutzt) aber auch gar nicht möglich. Solche Grenzübergänge wurden aufgrund von Plausibilitätsbetrachtungen durchgeführt, und es dauerte noch einmal 200 Jahre, bis dieses Problem zum Beispiel von Riemann systematisch untersucht wurde.

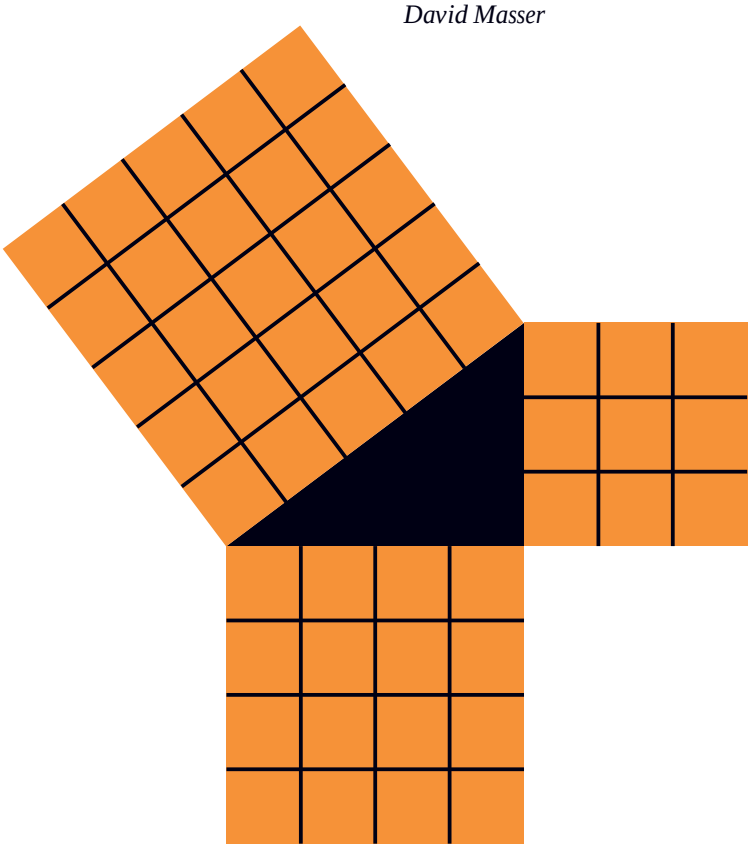
Trotzdem hat diese Lösungsmethode,
- Reduzierung des Problems auf ein diskretes Problem,
- Lösung des diskreten Problems,
- Konstruktion der kontinuierlichen Lösung aus der diskreten Lösung,

sehr befruchtend auf die Variationsrechnung gewirkt. Sie wurde in der Folge von Mathematikern wie Euler (ebenfalls ein Basler), Lagrange, Jacobi und vielen anderen weiterentwickelt.

Dr. Alfred Wagner ist Assistent
am Mathematischen Institut der Universität zu Köln.
Sein Arbeitsgebiet ist die Variationsrechnung.
Im Jahre 1999/2000 war er in Basel tätig.

Fermats letzter Satz ist so einfach wie das ABC

David Masser



Unser Titel stammt von einem Witz von Don Zagier. Genau wie der ursprüngliche Witz, hat er eine präzise Bedeutung, die am Ende dieses Artikels erklärt wird.

Der berühmte Mathematiker Kronecker (1823 – 1891) sagte einmal: «Die natürlichen Zahlen 1,2,3, … hat der liebe Gott geschaffen, alles andere ist Menschenwerk.»

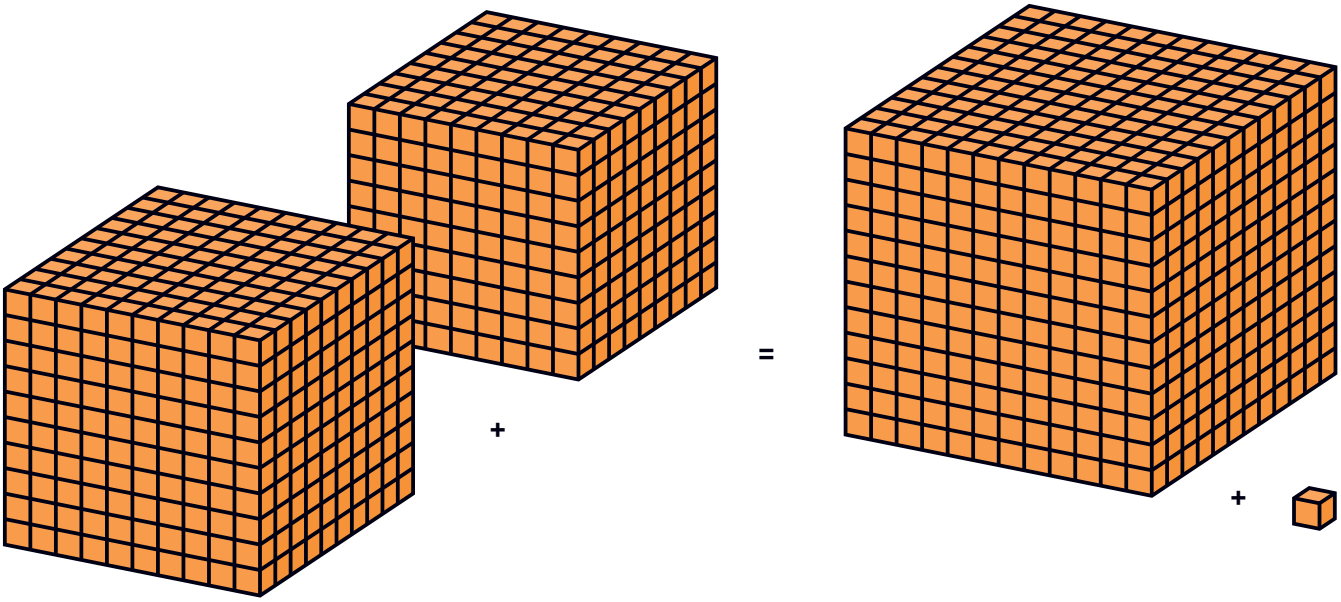
Aber selbst unter den natürlichen Zahlen 1,2,3, … gibt es Probleme, die bis heute nicht gelöst worden sind, und für manche dieser Probleme ist eine Lösung bei weitem nicht in Sicht.

Seit langem weiss man, dass $9 + 16 = 25$ ist, was deshalb bemerkenswert ist, weil $9 = 3 \cdot 3 = 3^2$ genau wie $16 = 4^2$ und $25 = 5^2$ ein perfektes Quadrat ist. Also haben wir eine Lösung $x = 3, y = 4, z = 5$ der pythagoräischen Gleichung

(1) $x^2 + y^2 = z^2$.

Dies ist nicht die einzige Lösung; zum Beispiel ist $5^2 + 12^2 = 13^2$ eine weitere Lösung, oder (wie man nach fünfminütiger Suche feststellt) $123456789^2 + 6535620^2 = 123629661^2$.

Tatsächlich hat man die Gleichung (1) bereits vor beinahe zweitausend Jahren verstanden, und die wesentlichen Bestandteile der Theorie waren bereits Diophant ungefähr im Jahr 250 n. Chr. bekannt.



Die Situation ändert sich schlagartig, wenn man eine kleine Änderung anbringt und Kuben wie $64 = 4 \cdot 4 \cdot 4 = 4^3$ ins Spiel bringt. Nun erhalten wir die Gleichung

(2) $x^3+y^3=z^3$,

die für natürliche Zahlen x,y,z gelöst werden soll. Nun ist es überhaupt ziemlich schwer, irgendwelche Lösungen zu finden. Zum Beispiel ist $9^3 + 10^3 = 12^3$ falsch, aber «nur knapp», wie der Schotte sagte, als man ihn fragte, ob er genug Wechselgeld erhalten habe. Richtig ist hingegen $1729 = 9^3 + 10^3 = 12^3 + 1^3$, das heisst, die Zahl 1729 kann man durch die Summe zweier perfekter Kuben auf zwei verschiedene Arten ausdrücken. Darauf wurde übrigens Hardy (1877 – 1947) auf ungehaltene Art von dem indischen Mathematiker Ramanujan (1887 – 1920) aufmerksam gemacht, der aufgrund des feuchten und kalten englischen Klimas mit einer Erkältung im Krankenhaus lag. Hardy war mit einem Taxi mit der Nummer 1729 zu Besuch gekommen und hatte festgestellt, dass dies eine besonders langweilige Zahl sei.

Unabhängig davon haben wir immer noch keine Lösung von (2) gefunden, und tatsächlich war es Euler (1707 – 1783), der als erster bewies, dass es überhaupt keine Lösungen gibt. Gleichung (2) ist also auch vollständig verstanden.

Gehen wir einen Schritt weiter und betrachten wir perfekte vierte Potenzen wie $81 = 3 \cdot 3 \cdot 3 \cdot 3 = 3^4$. Fermat selbst (1601 – 1665) bewies als erster, dass die zugehörige Gleichung

(3) $x^4+y^4=z^4$

keine einzige Lösung hat.

Der weitere Weg ist nun klar. Für jede natürliche Zahl n schreibt man m^n für das n-malige Produkt von m mit sich selbst, zum Beispiel $2^{10} = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 1024$. Es war ebenfalls Fermat der die Verallgemeinerung formulierte, dass für $n = 3,4,5, \ldots$ die Gleichung

(4) $x^n+y^n=z^n$

keine natürlichen Zahlen x,y,z als Lösungen besitzt. Wie allgemein bekannt ist, schrieb er auf den Rand eines Lehrbuchs über Zahlentheorie: «Es ist nicht möglich, einen Kubus in zwei Kuben oder ein vierte Potenz in zwei vierte Potenzen und allgemein eine Potenz, höher als die zweite, in zwei Potenzen mit demselben Exponent zu zerlegen. Ich habe dafür einen wahrhaft wunderbaren Beweis gefunden, doch ist dieser Rand hier zu schmal, um ihn zu fassen.»

Weil Fermat behauptete, einen Beweis zu haben, ist diese Aussage gemeinhin als *Fermats letzter Satz* bekannt geworden, obwohl nur wenige Mathematiker glauben, dass er tatsächlich im Besitz eines Beweises war.

Die Fälle $n = 3,4$ wurden bereits erörtert. Der Fall $n = 5$ wurde von Legendre (1752 – 1833) und Dirichlet (1805 – 1859) bewiesen.

Der nächste Fall $n = 6$ folgt übrigens leicht aus dem Fall $n = 3$, wenn man die Tatsache benutzt, dass jede perfekte sechste Potenz ebenfalls ein perfekter Kubus ist. Dies gilt, weil $6 = 2 \cdot 3$ ist und weil die Potenzierungsregeln ergeben, dass $m^6=(m^2)^3$ ist.

Der Fall $n = 7$ wurde von Lamé gelöst, der wohl eher aufgrund einer nach ihm benannten Differenzialgleichung bekannt sein dürfte. Kurz darauf, im Jahr 1847, kündigte Lamé einen Beweis für alle grösseren Zahlen n an, der sich jedoch als fundamental falsch herausstellte. Seit damals sind unzählige falsche Beweise aufgetaucht, wobei beinahe alle dieser Beweise von Laienmathematikern stammen, die wenig oder gar nichts davon wussten, was mit einem «Beweis» gemeint ist.

Der Fall n = 8 folgt leicht aus dem Fall n = 4, weil $8 = 2 \cdot 4$ ist. Nun kann man diese Überlegung verallgemeinern, und man erhält die Schlussfolgerung, dass wir unsere Aufmerksamkeit nur noch auf diejenigen n richten müssen, die in der folgenden Liste der ungeraden «Primzahlen» auftauchen:

(5) $3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots,$
$163, \ldots, 691, \ldots, 1999, \ldots$

Die Liste wird dadurch charakterisiert, dass keine in ihr auftauchende Zahl durch eine in der Liste vor ihr stehende Zahl teilbar ist. Deshalb können wir von $n = 7$ direkt zu $n = 11$ springen.

Der nächste wesentliche Fortschritt wurde von Kummer (1810 – 1893) erzielt, der in einem einzigen Satz viele Fälle abhandelte, insbesondere alle n kleiner als 100 ausser 37, 59 und 67. Dies ebnete den Weg für darauf folgende computerunterstützte Rechnungen, die 1993 ergaben, dass für alle n kleiner als 4000000 die Gleichung (4) keine Lösung hat.

Beinahe unerwartet und ziemlich beiläufig gab dann 1993 Andrew Wiles am Ende einer dreiteiligen Vortragsreihe in Cambridge einen vollständigen Beweis für alle $n>2$ bekannt. Heutzutage ist die Geschichte wohlbekannt, wie zuerst eine Lücke im Beweis auftauchte und daraufhin Wiles 1994 am Internationalen Mathematiker Kongress in Zürich zugab, dass sein Beweis unvollständig war. Es sah ganz nach einer modernen Version früherer Fehler von Lamé und anderen aus, bis schliesslich die Lücke durch Wiles selbst mit Hilfe von Richard Taylor geschlossen wurde (Wiles gibt den 19. September 1994 als den Tag der endgültigen Offenbarung an). Die Arbeit wurde 1995 in der berühmten Zeitschrift Annals of Mathematics veröffentlicht, und das Ergebnis selbst lautet (ich zitiere wörtlich und ohne Erklärung):

THEOREM 0.5. Suppose that $u^P + v^P + w^P = 0$ for $u, v, w \epsilon Q$ and $p \geq 3$, then $uvw = 0$.

Ich sagte bereits, dass der Beweis «beinahe unerwartet» kam. Er war unerwartet in dem Sinne, dass er nicht dem so mühsam vorgezeichneten Weg von Fermat, Euler, Dirichlet, u.a. folgte. Er entstand dagegen aus einem völlig unterschiedlichen Zugang, der 1985 von Frey vorgeschlagen wurde. Freys Zugang bestand darin, der Lösung von (4) die folgende Gleichung zuzuordnen

(6) $Y^2=X(X-x^n)(X+y^n).$

Eine derartige Gleichung definiert das, was man heutzutage als elliptische Kurve bezeichnet. Die Idee, die vielen Mathematikern nicht nur absurd, sondern auch inhaltsleer erschien, bestand darin, so viele gute Eigenschaften der Kurve (6) nachzuweisen, dass sie unmöglich existieren kann. Genau dieses Programm wurde von Wiles durchgeführt, nachdem wertvolle Vorarbeiten von anderen wie zum Beispiel Serre und Ribet geleistet worden waren.

Elliptische Kurven erhielten ihren Namen, weil sie aus dem Versuch entstanden, den Umfang von Ellipsen zu messen. Die dazu verwendeten Funktionen, genannt elliptische Funktionen, haben viele schöne Eigenschaften und tauchen ebenfalls in der klassischen Physik auf; zum Beispiel um den Ausschlag eines Pendels zu berechnen. Elliptische Kurven sind neuerdings auch dazu benutzt worden, grosse Zahlen zu faktorisieren, was nicht nur eine nutzlose zahlentheoretische Übung ist, sondern ein wertvolles Werkzeug der modernen Wissenschaft der Kryptologie. Ich glaube, dass einige interessante Ergebnisse über elliptische Kurven aus militärisch begründeten Informationsbeschränkungen nicht veröffentlicht werden können. Dies hätte Hardy zutiefst betrübt, der in seinem Buch «A Mathematician's Apology» (1940) stolz schrieb: «Niemand hat bisher irgendeinen kriegsdienlichen Zweck der Zahlentheorie oder der Relativitätstheorie entdeckt, und es scheint unwahrscheinlich, dass dies irgendjemandem in absehbarer Zeit gelingt.»

Im Jahr 1985 besuchte ich einen Vortrag von Oesterlé am Max-Planck-Institut in Bonn. Er stellte damals eine Vermutung vor, die den «Konduktor» und die «Diskriminante» bestimmter elliptischer Kurven in Beziehung setzte. Mir fiel damals auf,
a) dass diese Vermutung eine natürliche Formulierung hatte, die unabhängig von den elliptischen Kurven war,
b) dass ein verwandtes Ergebnis bereits einige Jahre zuvor von Mason bewiesen worden war,
c) dass dieses verwandte Ergebnis auf eine recht genaue Version der Vermutung hinwies.

Diese genaue Version ist heutzutage bekannt als die abc-Vermutung. Sie bezieht sich auf natürliche Zahlen a,b,c, die nichts anderes als die einfache Gleichung

(7) $a + b = c$

erfüllen. Der Gleichung (7) ordnen wir eine andere Zahl S zu, die das Produkt aller Primzahlen aus der Liste (5) ist, die entweder a oder b oder c teilen. Wir müssen dabei allerdings noch die Einschränkung machen, dass weder die Zahl 2 noch irgendeine dieser Primzahlen gleichzeitig a,b und c teilt. Wenn zum Beispiel die ursprüngliche Beobachtung in (7) aus $9 + 16 = 25$ besteht, dann kommen nur die Primzahlen 3 und 5 in Frage, und folglich ist $S = 15$.

Die abc-Vermutung handelt von der Ungleichung

(8) $c<KS^m$

für bestimmte Werte von m und K. In ihrer schärfsten Form besagt sie, dass es zu jeder reellen Zahl $m>1$ eine Zahl K gibt, so dass (8) für jede Lösung von (7) gilt. Dies ist in Wahrheit eine recht komplexe Aussage, die in ihrer vollen Stärke am ehesten von Berufsmathematikern gewürdigt werden kann. Ihre Stärke wird dadurch gemessen, wie nahe m bei 1 liegt. Zum Beispiel gibt es für $m = 1{,}01$ einen Wert K, so dass (8) gilt; ebenso gibt es für $m = 1{,}001$ einen wahrscheinlich anderen Wert K und so weiter.

Die volle Stärke wird jedoch in Anwendungen selten gebraucht; für gewöhnlich reicht der Wert $m = 2$ aus. In diesem Fall gibt es einen bestimmten Wert von K, zum Beispiel $K = 2^{1000}$ (zweifelsohne eine absurd grosszügige Überschätzung).

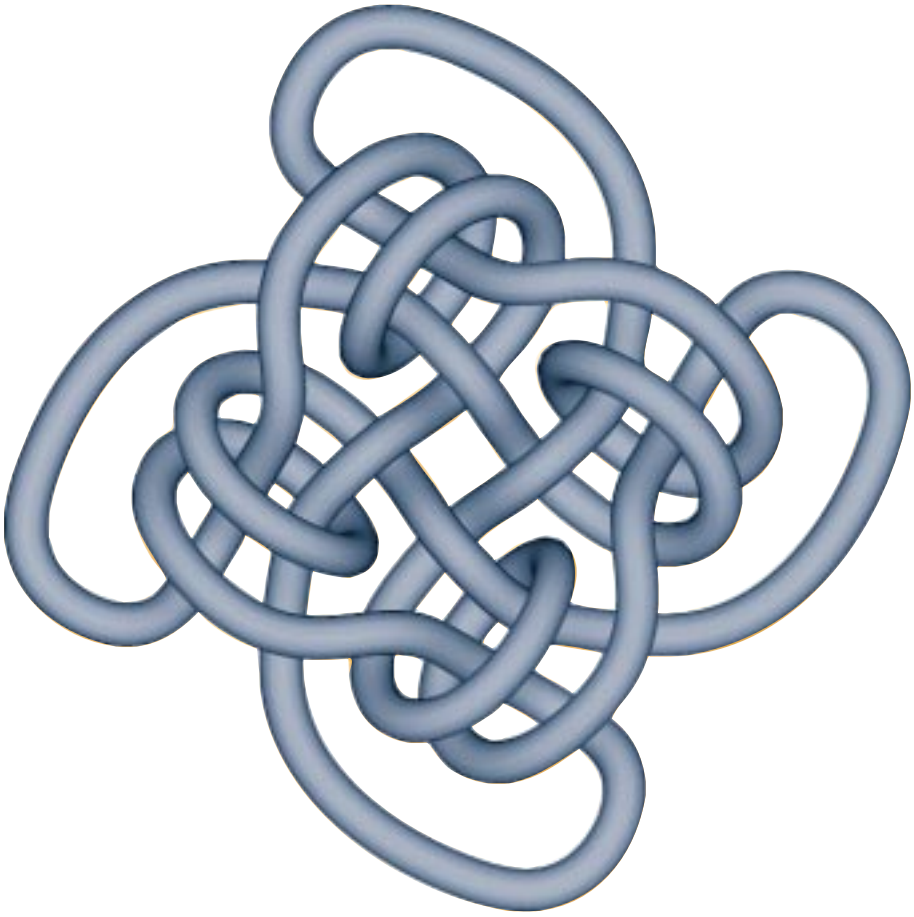
Nehmen wir also an, dass «abc» in der Gestalt (8) mit $m = 2$ und $K = 2^{1000}$ gilt. Dann ist es möglich, durch den ausschliesslichen Gebrauch von Schulmathematik aus (7) mit $a = x^n$ und $b = y^n$ die folgenden Aussagen zu schliessen (die Details fielen editorialen Kürzungen zum Opfer). Erstens hat Fermats Gleichung (4) keine Lösung für $n > 1005$. Zweitens gibt es eine endliche Rechenvorschrift, die theoretisch sehr einfach ist, um alle möglichen Lösungen für $n \leq 1005$ zu bestimmen. Der Haken dabei ist, dass diese Vorschrift in der Praxis gar nicht so einfach ist und wahrscheinlich nicht eher brauchbar, als bis der legendäre *Quantencomputer* gebaut worden ist. Andererseits haben die oben erwähnten Rechnungen des Jahres 1993 die Frage ohnehin für alle $n < 4000000$ erledigt.

Deshalb lässt sich sagen: «*Fermats letzter Satz folgt aus abc*», was tatsächlich logisch äquivalent zum Titel unseres Artikels ist.

Prof. Dr. David Masser ist Ordinarius für Mathematik am Mathematischen Institut der Universität Basel.

Auflösung mathematischer Knoten

Anna Beliakova und Alexander Schumakovitch



O time! thou must untangle this, not I;
It is too hard a knot for me to untie!

William Shakespeare, Twelfth Night

Vom Gordischen Knoten zum mathematischen Knoten

Einen Knoten aufzulösen galt schon in der Zeit Alexanders des Grossen als eine Herausforderung. Alexander hatte mit seiner Technik einen so durchschlagenden Erfolg, dass das Problem über 2000 Jahre lang als gelöst galt. Erst im 19. Jahrhundert haben die Wissenschaftler damit begonnen, die königliche Methode zu verfeinern.

Die ersten waren die Physiker. Lord Kelvin hat 1867 die Vermutung geäussert, dass Atome verknotete Fäden aus Äther sind. Um also Materie zu verstehen, benötigte man eine vollständige Liste aller möglichen Knoten. P. G. Tait, Lord Kelvins Mitarbeiter, hat viele Jahre daran gearbeitet. Das Resultat war vor allem die Einsicht, dass das Problem schwierig ist. Tait hat viele interessante Vermutungen und eine Liste weniger einfacher Knoten hinterlassen. Er konnte aber weder beweisen, dass die aufgelisteten Knoten wirklich verschieden sind noch dass die Liste in irgendeinem Sinn vollständig ist.

Nach dem Niedergang der Kelvinschen Theorie ist das Studium der Knoten zu einem exotischen Zweig der reinen Mathematik namens Knotentheorie geworden. Das erste, was die Mathematiker machten, war, das Objekt der Untersuchungen exakt zu definieren. So sind die *mathematischen* Knoten entstanden. Das sind idealisierte Objekte, die nur die wesentlichen Eigenschaften eines Knotens behalten. Ein mathematischer Knoten unterscheidet sich von einer verknoteten Schnur *erstens* dadurch, dass seine Enden festgehalten oder zusammengebunden sind (ansonsten könnte man den Knoten durch das freie Bewegen eines seiner Enden immer entknoten); und *zweitens* dadurch, dass die Schnur durch eine unendlich dünne Linie (die Schnurachse) ersetzt wird. Im Folgenden beschäftigen wir uns nur mit mathematischen Knoten.

Abbildung 1: Trivialer Knoten und sein Diagramm

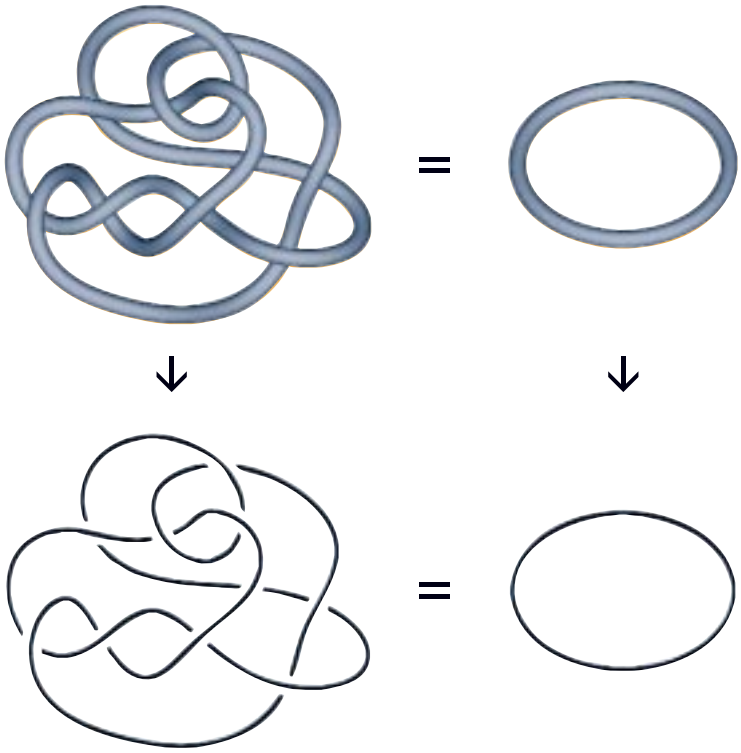
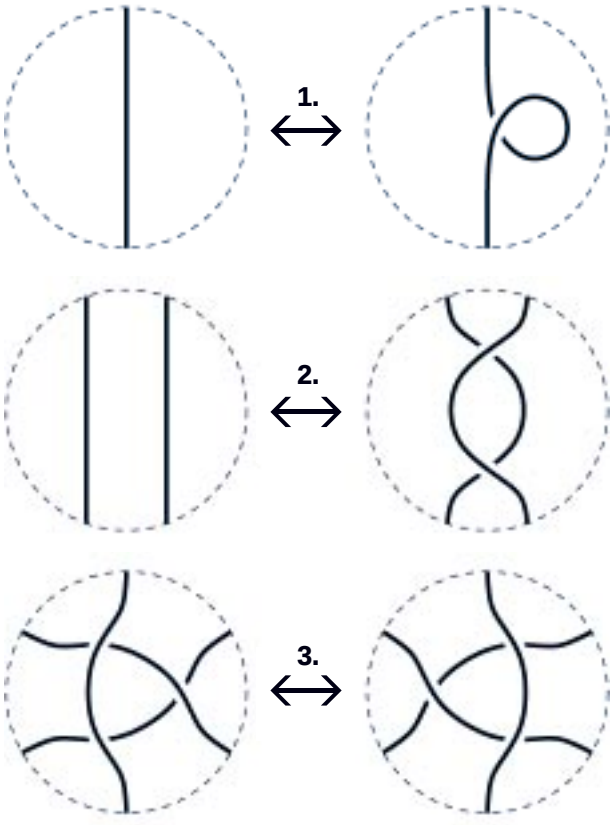


Abbildung 2: Reidemeister-Bewegungen



Zwei Knoten heissen *äquivalent*, wenn man einen in den anderen deformieren kann. Die Deformation bedeutet das Ziehen und Drehen der Schnur an allen möglichen Stellen, ohne sie zu zerreissen. Ein Knoten heisst *trivial*, wenn er zu einem Kreis äquivalent ist. Der Knoten in Abbildung 1 links oben ist erstaunlicherweise trivial.

Mathematiker stellen Knoten mit Hilfe von *Diagrammen* dar. Dafür schaut man den Knoten aus der Entfernung an und zeichnet eine Linie, die die Schnurachse darstellt. Wenn sich zwei Linien schneiden, unterbricht man diejenige, die weiter weg ist (vergleiche mit Abbildung 1). Man kann natürlich den Blickwinkel immer so wählen, dass man keine drei Linien sieht, die sich in einem Punkt schneiden.

Das Hauptproblem der Knotentheorie ist, Knoten zu unterscheiden. Das heisst, entscheiden zu können, ob zwei Knoten, gegeben durch ihre Diagramme, äquivalent sind oder nicht. Ein verwandtes Problem ist, ein Diagramm des trivialen Knotens immer zu erkennen. Diese beiden Probleme sind zur Zeit ungelöst.

Wir wissen allerdings, dass zwei Diagramme genau dann äquivalente Knoten darstellen, wenn man ein Diagramm in das andere durch mehrfaches Anwenden der drei in Abbildung 2 aufgezeichneten Reidemeister-Bewegungen transformieren kann. Die Bewegungen sind nach dem deutschen Mathematiker Reidemeister benannt, der sie in den zwanziger Jahren einführte. Bei *Reidemeister-Bewegungen* bleiben die Knotendiagramme ausserhalb der punktierten Kreise unverändert. Innerhalb der Kreise darf man nur die drei gezeigten Züge in beide Richtungen ausführen.

Jede Eigenschaft eines Knotens, die sich nicht unter Reidemeister-Bewegungen ändert, heisst *Knoteninvariante*. Invarianten spielen eine zentrale Rolle in der Knotentheorie, weil sie zur Unterscheidung von Knoten dienen. Alle Invarianten äquivalenter Knoten müssen übereinstimmen. Deshalb genügt es, eine Invariante (Eigenschaft) zu finden, die für zwei Knoten verschieden ist, um die Knoten zu unterscheiden. Allerdings – selbst wenn man 2000 Invarianten hat, die für beide Knoten gleich sind, kann man daraus nicht schliessen, dass die Knoten äquivalent sind. Vielleicht gibt es eine 2001. Invariante, die sie unterscheidet.

Einfachste Invariante

Wir führen nun eine Invariante ein, welche den Knoten in Abbildung 3a vom trivialen Knoten unterscheidet. Trotz ihrer Einfachheit kennt man diese Invariante erst seit zwanzig Jahren. Sie wurde 1980 von dem amerikanischen Mathematiker Fox entdeckt.

Versuchen wir, ein Knotendiagramm mit drei Farben zu färben. Jedes Knotendiagramm besteht aus mehreren sich miteinander nicht schneidenden Intervallen, die wir Brücken nennen. Wir färben jede Brücke in einer der drei Farben – Weiss, Schwarz oder Orange –, wie es in Abbildung 3a und 3b gezeigt ist.

Dabei betrachten wir nur solche Färbungen, bei denen die drei Brücken, die an jeder Kreuzung zusammenkommen, entweder die gleiche oder verschiedene Farben haben. Solche Färbungen werden als erlaubt bezeichnet (siehe Abbildung 3). Zum Beispiel ist die Färbung in Abbildung 3a erlaubt und in Abbildung 3b nicht.

Definition der ersten Knoteninvariante. *Die Anzahl der möglichen erlaubten Färbungen eines Knotendiagramms ist eine Knoteninvariante.*

Zuerst überlegen wir uns, wozu wir eine solche Invariante brauchen können. Jedes Knotendiagramm hat mindestens drei Färbungen. Man kann immer das ganze Diagramm entweder weiss oder schwarz oder orange färben. Der triviale Knoten hat nur diese drei erlaubten Färbungen. Der Knoten in Abbildung 3a hat eine Färbung mehr. Das ist unser erster nichttrivialer Knoten! Er heisst Kleeblattschlinge und nimmt immer den ersten Platz in jeder Knotenliste ein. In der Tat hat die Kleeblattschlinge neun erlaubte Färbungen. Können Sie die anderen fünf finden?

Wir müssen noch zeigen, dass die Anzahl der Färbungen wirklich eine Invariante ist. Das bedeutet, wir müssen überprüfen, dass sie sich unter keiner der drei Reidemeister-Bewegungen ändert. Mit anderen Worten, die Anzahl der erlaubten Färbungen des Diagramms soll vor und nach jeder Bewegung gleich bleiben. Wir legen eine Färbung ausserhalb der Kreise fest, so dass die ungeänderten Brücken in den Diagrammen vor und nach der Bewegung gleich gefärbt sind. Dann macht die erste Reidemeister-Bewegung gar keine Probleme. Die Färbung ist links und rechts eindeutig festgelegt. Die zweite Bewegung ist fast genauso einfach: Wenn die zwei Brücken auf der linken Seite gleiche Farbe haben, dann muss auch die neue kleine Brücke diese Farbe erhalten. Andererseits, wenn sie verschieden gefärbt sind (z.B. wie in Abbildung 4a schwarz und weiss), dann erhält die kleine Brücke die dritte komplementäre Farbe (Orange).

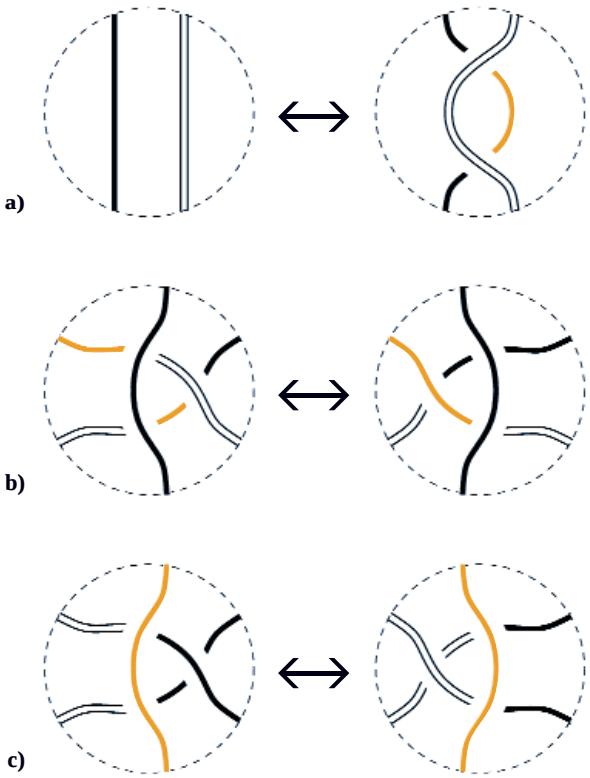
Abbildung 3: Gefärbte Diagramme

a) Kleeblattschlinge **b) Achterknoten**

Erlaubte Färbungen

Verbotene Färbungen

Abbildung 4: Gefärbte Reidemeister-Bewegungen



Nur die dritte Reidemeister Bewegung ist schwieriger zu behandeln. Hier hat man viel mehr (sechs) Brücken, die noch mehr (27) verschiedene Färbungen erlauben. Glücklicherweise kann man diese 27 Fälle auf fünf Grundtypen reduzieren. Diese fünf Möglichkeiten muss man aber direkt eine nach der anderen überprüfen. Für zwei davon ist das in Abbildung 4b und 4c gemacht.

Jetzt sind wir in der Lage, eine beeindruckende Liste aus einem Satz und zwei Korollaren aufzustellen.

1. Satz. *Wenn zwei Knoten eine verschiedene Zahl erlaubter Färbungen haben, dann sind sie nicht äquivalent.*
2. Korollar. *Die Kleeblattschlinge ist kein trivialer Knoten.*
3. Korollar. *Die Kleeblattschlinge ist nicht äquivalent zum Achterknoten.*

Der Achterknoten (siehe Abbildung 3b) nimmt die zweite Stelle in jeder Knotenliste ein, direkt nach der Kleeblattschlinge. Der Achterknoten hat nicht mehr als drei erlaubte Färbungen und ist deshalb von der Kleeblattschlinge verschieden. (Wenn Sie die vierte Färbung entdecken, können Sie die ganze Knotentheorie widerlegen!) Was uns noch fehlt, ist der Beweis, dass der Achterknoten nicht trivial ist. Das können wir mit unseren bescheidenen Methoden leider nicht tun. Die Erfahrung sagt uns aber, dass es stimmt.

Verschlingungszahl

Unsere nächste Invariante war schon dem deutschen Mathematiker Gauss (1777 – 1855) bekannt. Sie hat mindestens zehn sehr verschiedene Definitionen. Eine davon werden wir jetzt diskutieren.

Dafür müssen wir *mehrere* Knoten gleichzeitig betrachten, die sich nicht schneiden, aber ineinander verschlungen sein können. Solche Objekte nennt man *Verschlingungen*. Die einzelnen Knoten, aus denen eine Verschlingung besteht, heissen *Verschlingungskomponenten*. Für Verschlingungen kann man auch Diagramme, Reidemeister-Bewegungen, Invarianten und so weiter definieren. Sie sind eigentlichen Knoten so verwandt, dass man oft über Knoten spricht und dabei Verschlingungen meint. Äquivalente Verschlingungen haben sicher die gleiche Anzahl von Komponenten. Eine triviale Verschlingung ist äquivalent zu einer Vereinigung unverknoteter Kreise. Zum Beispiel sind die Verschlingungen in den Abbildungen 6a und 6b trivial, aber in Abbildung 6c nicht.

Wir beschränken uns auf Verschlingungen mit zwei Komponenten. Es stellt sich eine natürliche Frage: Wie kompliziert können die beiden Komponenten miteinander verknotet sein?

Betrachten wir das Beispiel in Abbildung 5a. Wir versuchen, die erste Komponente von der zweiten wegzuziehen und dabei die zweite festzuhalten. Irgendwann werden die Stückchen der zweiten Komponente das weitere Bewegen blockieren. Wir können die Stückchen nicht überspringen, aber wir dehnen die erste Komponente so aus, dass das weitere Ziehen möglich wird. Schliesslich wird die erste Komponente an manchen Stellen durch die zweite Komponente geklemmt. Die Situation ist in Abbildung 5b gezeigt. Die Anzahl solcher «Klemmen» spiegelt die Komplexität der Verschlingung wider. Wenn wir jetzt auf die Verschlingung einen Blick entgegen der Ziehrichtung werfen, dann sehen wir, dass die Klemmen Stellen entsprechen, an denen die zweite Komponente *über* die erste läuft (siehe Abbildung 5c). Das kann man auch auf dem Diagramm beobachten (Abbildung 5d). Übrigens, wenn die Zieh- und Blickrichtungen übereinstimmen, dann ändert sich das Diagramm beim Ziehen überhaupt nicht.

Die Anzahl der Stellen auf dem Verschlingungsdiagramm, an denen die zweite Komponente *über* die erste läuft, scheint ein guter Kandidat zu sein, um die Komplexität der Verschlingung zu messen. Leider ist es keine Invariante. Sie kann sich unter der zweiten Reidemeister-Bewegung um zwei ändern. Dieses Problem kann man aber relativ einfach beseitigen. Wir wählen eine der zwei Richtungen, in welche wir unsere Komponenten durchlaufen wollen. Wir markieren unsere Wahl mit einem kleinen Pfeil auf jeder Komponente wie in Abbildung 6c. Jetzt ist unsere Verschlingung *orientiert*. Wir blicken nun auf jede Kreuzung so, dass die beiden Linien nach oben orientiert sind, und definieren dann das Vorzeichen der Kreuzung nach der Regel in Abbildung 7.

Es sei jetzt ein orientiertes Verschlingungsdiagramm mit zwei nummerierten Komponenten gegeben. Wir summieren über alle Vorzeichen solcher Kreuzungen, an denen die zweite Komponente *über* die erste läuft. Das Resultat heisst *Verschlingungszahl*. Beispiele der Berechnung der Verschlingungszahl sind in Abbildung 8 gezeigt. Beim Umdrehen der Orientierung einer der Komponenten ändert sich das Vorzeichen jeder Kreuzung und als Resultat das Vorzeichen der Verschlingungszahl.

4. Satz. *Die Verschlingungszahl ist eine Invariante der orientierten Verschlingung mit zwei Komponenten.*
5. Korollar. *Die Verschlingungen in Abbildung 8 sind nicht äquivalent, obwohl sie ähnlich aussehen.*

Der Beweis des Satzes ist analog zum vorherigen. Man muss alle Reidemeister-Bewegungen überprüfen – übrigens haben die zwei neuen Kreuzungen bei der zweiten Reidemeister-Bewegung immer verschiedene Vorzeichen. Wir überlassen Ihnen, aufmerksamer Leser, den Rest des Beweises. Dies werden Ihre ersten Schritte in die bezaubernde Welt der Knotentheorie sein!

Einige Bemerkungen müssen wir trotzdem noch machen. Erstens ändert sich beim Vertauschen der Rollen der beiden Komponenten die Verschlingungszahl nicht. Zweitens kann man die Regel in Abbildung 7 auch dazu benutzen, das Vorzeichen jeder Kreuzung eines orientierten *Knotendiagramms* zu definieren. Leider ist die Summe über alle Vorzeichen keine Knoteninvariante, weil sie schon die erste Reidemeister-Bewegung nicht überlebt.

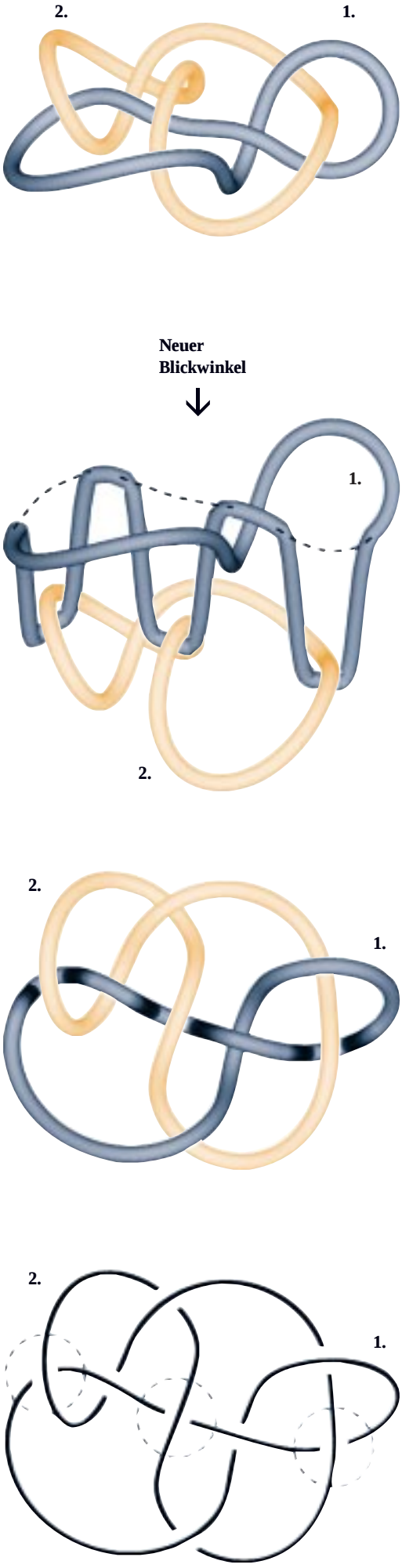
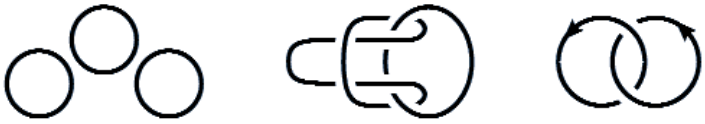


Abbildung 5: Begründung der Definition der Verschlingungszahl

Abbildung 6: Beispiele von Verschlingungen



a) **b)** **c)**

Abbildung 7: Regel für Vorzeichen

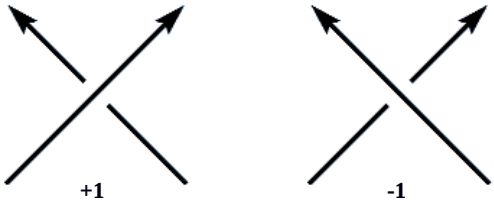
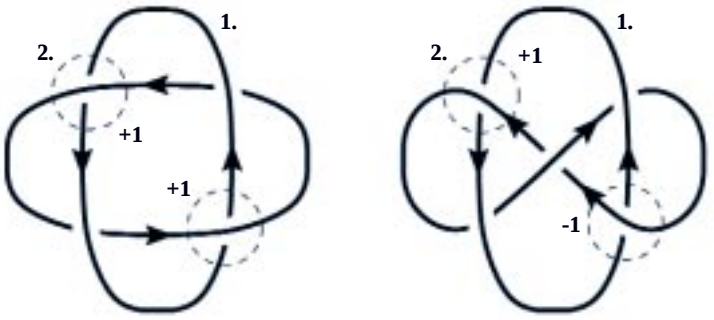
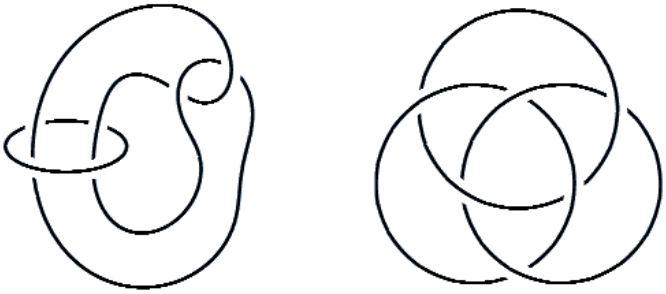


Abbildung 8: Berechnung der Verschlingungszahl



a) Verschlingungszahl: + 1 + 1 = 2 **b) Verschlingungszahl: + 1 – 1 = 0**

Abbildung 9: Interessante Verschlingungen



a) Whitehead-Verschlingung **b) Borromäische Ringe**

Drittens, wenn die Verschlingungszahl null ist, heisst es noch nicht, dass man die Komponenten auseinander ziehen kann. Die so genannte Whitehead-Verschlingung ist ein gutes Beispiel dafür (siehe Abbildung 9a).

Ein sonderbares Beispiel ist in Abbildung 9b gezeigt. Diese Verschlingung (mit dem Namen Borromäische Ringe) hat drei Komponenten, wobei je zwei davon die Verschlingungszahl null haben. Die drei Komponenten kann man aber nicht auseinander ziehen. Allerdings: wenn wir eine Komponente weglassen, ist der Rest eine triviale Verschlingung aus zwei Komponenten.

Die Verschlingungszahl ist die erste Invariante aus einer unendlichen Reihe der so genannten *Invarianten des endlichen Typs*. Die Theorie dieser Invarianten ist erst zehn Jahre alt. Sie entwickelt sich aber sehr rasch. Zurzeit sind nur einige Invarianten des endlichen Typs berechnet. Die zweite Invariante dieser Reihe kann zum Beispiel den Achterknoten vom trivialen Knoten unterscheiden. Die dritte Invariante trennt die Kleeblattschlinge von ihrem Spiegelbild, das *linke* Kleeblattschlinge heisst. Es gibt viele Gründe zu glauben, dass mit Hilfe der Invarianten des endlichen Typs das Hauptproblem der Knotentheorie gelöst wird!

Wir danken Gregor Fels, Hans-Christoph Im Hof und Christof Schmidhuber für ihr Interesse für Knoten und für viele nützliche Hinweise.

Unser besonderer Dank gilt Robert Scharein, dem Autor des wunderbaren Zeichenprogramms KnotPlot.
www.cs.ubc.ca/nest/imager/contributions/scharein/KnotPlot.html

Dr. Anna Beliakova ist seit 1998 Assistentin am Mathematischen Institut.
Ihr Arbeitsgebiet ist die niedrigdimensionale Topologie und die Knotentheorie.
Zurzeit ist sie Inhaberin eines Habilitations-Stipendiums der Universität Basel zur Förderung des wissenschaftlichen Nachwuchses.

Dr. Alexander Schumakovitch ist seit 1996 Assistent am Mathematischen Institut.
Er arbeitet auf dem Gebiet der Topologie.

Komplexitätstheorie

Bruno Scarpellini

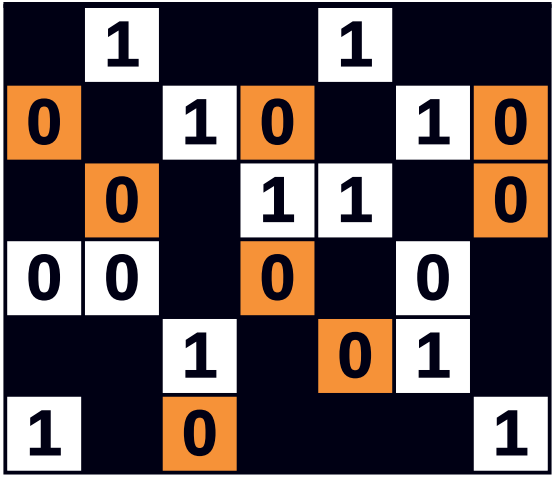
Es gibt viele Interpretationen des Begriffs «Komplexität». Die für uns relevante ist aufs engste mit der theoretischen Computerwissenschaft verbunden. Eine sehr grobe, weiter unten zu präzisierende Form dieses Begriffs kann wie folgt beschrieben werden: Ein Problem, das in geeigneter Form der Behandlung durch den Computer zugänglich ist, heisst «komplex», wenn die Rechenzeit *t*, die benötigt wird, um es zu lösen, gross ist und wenn keine noch so schlaue Programmierung in der Lage ist, die Rechenzeit unterhalb eine gewisse grosse Schranke t_0 hinunterzudrücken. Es ist nun zweckmässig, unsere Betrachtungen mit einigen Bemerkungen zur Vorgeschichte des Gegenstandes einzuleiten.

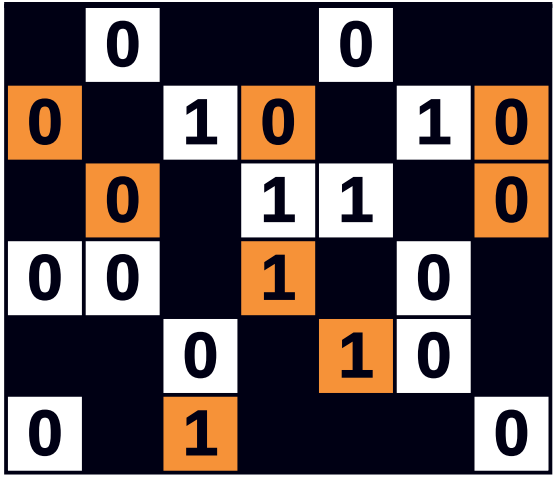
In den Jahren um 1930 herum unternahmen es der berühmte Mathematiker David Hilbert und seine Schüler, die Begründung der Mathematik mit streng formal-logischen Mitteln durchzuführen. Das Kernstück dieses logischen Apparates war der so genannte Prädikatenkalkül. Dieser erlaubt es, praktisch jedes mathematische Problem P durch einen formalen Ausdruck F_P darzustellen, der bei geeigneter Interpretation genau einen von zwei Werten, *t* = wahr respektive *f* = falsch, annimmt: ist der Wert *t*, so ist P lösbar, ist der Wert *f*, so ist P nicht lösbar. Hilbert stellte nun die Aufgabe, eine mechanische (oder «finite») Universalmethode M zu finden, die Folgendes leistet: Angesetzt auf F_P soll M nach endlich vielen Schritten den Wert von F_P, das heisst *t* oder *f*, bestimmen. Zwischen 1930 und 1940 wurde aber von verschiedenen Logikern (A. Church, S. C. Kleene, A. Turing) bewiesen, dass es eine solche Universalmethode M nicht gibt. Unter dem Einfluss dieser negativen Resultate erlahmte die Suche nach einer Universalmethode.

Auf Grund der Arbeiten der von der Logik herkommenden Informatiker Stephen A. Cook und Richard M. Karp (1971, 1972) erfuhr aber die Hilbertsche Fragestellung eine unerwartete Wiederbelebung. Es sei an dieser Stelle darauf hingewiesen, dass bei Hilbert die Frage nach der Anzahl der Schritte, die eine allfällige Methode M braucht, um das Problem F_P zu entscheiden, keine Beachtung fand. Ganz anders bei S. Cook. In seiner grundlegenden Arbeit 1971 zeigt er, dass unter Berücksichtigung des Zeit- respektive Schrittfaktors die Frage nach einer Universalmethode ganz neue Formen annimmt. Zum einen definierte Cook die «Anzahl Schritte» als Anzahl Rechenschritte eines Computers. Diese Definition ist noch etwas ungenau, da sie abhängig vom zugrunde gelegten Computertyp ist. Auf diesen Punkt sei später nochmals kurz eingegangen. Um den Zeitfaktor ins Spiel zu bringen, beachtet man, dass sich jeder vernünftigen Codierung F_P eines Problems P in einfacher Weise eine Länge $|F_P|$ zuordnen lässt: z.B. die Anzahl Zeichen, die in F_P vorkommen. Man gibt nun eine Funktion $h(x)$ vor, die für $x = 1, 2, \ldots$ definiert ist und Werte ≥ 0 annimmt. Man sagt, ein Programm M entscheide die Klasse Γ von Problemen P in Zeit $h(x)$, falls M, angesetzt auf F_P, höchstens $h(|F_P|)$ Rechenschritte braucht, um den Wert (*t* oder *f*) zu berechnen. Schliesslich nennt man eine Klasse Γ von Problemen polynomial entscheidbar, falls es ein Programm M und ein Polynom $h_0(x) = cx^n$ gibt ($c > 0$ und n eine natürliche Zahl), so dass M die Klasse Γ in Zeit $h_0(x)$ entscheidet. Die Familie der polynomial entscheidbaren Problemklassen ist für die Komplexitätstheorie von grundlegender Bedeutung.

Eine besondere Problemklasse

Wir wenden uns nun einer Problemklasse zu, die in der Fachliteratur mit dem Kürzel 3SAT (kurz für «three satisfaction») bezeichnet wird. Diese Problemklasse nimmt in der Komplexitätstheorie eine Schlüsselposition ein. Um technisches Vokabular zu vermeiden, sei hier eine etwas unorthodoxe Darstellung von 3SAT gewählt.





Wir betrachten ein Spielbrett, eine Art verallgemeinertes Schachbrett, das aus M (waagrechten) Zeilen und N Spalten (Kolonnen) besteht, also rechteckig ist und $M \cdot N$ Felder enthält. Jedes dieser Felder ist mit einer «Farbe» weiss, grau oder schwarz gefärbt. Die Färbung ist beliebig bis auf eine Einschränkung: In jeder Kolonne dürfen genau drei nichtschwarze Felder vorkommen. Ein solches Brett heisse «zulässig». Die Aufgabe besteht nun darin, die weissen und grauen (also nichtschwarzen) Felder so mit 0 und 1 zu belegen, dass folgende Vorschriften erfüllt sind: (V_1) in jeder Zeile sind die Felder gleicher Farbe mit der gleichen Zahl belegt, (V_2) in jeder Zeile sind Felder verschiedener Farbe mit verschiedenen Zahlen belegt, (V_3) in jeder Spalte kommt mindestens ein Feld vor, das mit 1 belegt ist. Die zu lösende Aufgabe (P_{MN}) lautet also: bei vorgegebenem zulässigem $M \cdot N$-Brett zu entscheiden, ob eine 0,1-Belegung der nichtschwarzen Felder existiert, die (V_1)–(V_3) erfüllt. Diese Definitionen seien durch zwei Beispiele illustriert.

Die linke Figur stellt ein zulässiges 6·7 Brett dar, das mit einer 0,1-Belegung versehen ist, die das Problem (P_{67}) löst, während die rechte Figur das gleiche Brett zeigt, aber jetzt mit einer 0,1-Belegung versehen, die das Problem (P_{67}) nicht löst.

Da es nur endlich viele Möglichkeiten gibt, die weissen und grauen Felder eines zulässigen $M \cdot N$-Bretts mit 0 und 1 zu belegen, ist klar, dass das Problem (P_{MN}) durch endliches Ausprobieren gelöst werden kann. Mit 3SAT bezeichnen wir nun die Klasse (Gesamtheit) der Einzelprobleme (P_{MN}). Die zentrale Frage lautet: (Problem von Cook) Ist 3SAT polynomial entscheidbar? Alles deutet darauf hin, dass dem nicht so ist, aber bis jetzt ist noch niemand in der Lage gewesen, das zu beweisen. In der Tat scheint das Problem von Cook eines der schwierigsten kombinatorischen Probleme zu sein, die zurzeit in der Mathematik bekannt sind. Nachzutragen ist, dass der Begriff «Rechenschritt» sich auf eine so genannte Turingmaschine bezieht und so abgefasst ist, dass die polynomiale Berechenbarkeit maschinenunabhängig ist.

Die zentrale Rolle der Problemklasse 3SAT wird durch folgenden Sachverhalt begründet. Man kennt mehr als zweitausend Problemklassen Γ_i von kombinatorischem, zahlentheoretischem oder geometrischem Charakter mit der Eigenschaft: ist 3SAT polynomial entscheidbar, so jede dieser Klassen Γ_i, und ist eine dieser Klassen Γ_i polynomial entscheidbar, so alle anderen, inklusive 3SAT. Diese Resultate ergeben sich aus dem Kernstück der Komplexitätstheorie, der so genannten NP-Vollständigkeitstheorie.

Aus Platzgründen müssen wir uns damit begnügen, vier wichtige Problemklassen von praktischer Bedeutung stichwortartig zu erwähnen: das Problem des Handlungsreisenden («travelling salesman problem»), das Rucksackproblem, Partitionsprobleme und Färbungsprobleme von Graphen. Nachzutragen ist, dass sich das 3SAT-Problem verallgemeinern lässt, indem man bei der Definition des zulässigen Bretts genau n nicht schwarze Felder pro Spalte zulässt; man erhält dann die Problemklasse nSAT.

Für $n \geq 3$ ändert sich nichts am oben Gesagten: für n ≥ 3 ist nSAT genau dann polynomial entscheidbar, wenn 3SAT es ist. Für $n = 2$ hingegen hat man einen polynomialen Algorithmus gefunden, der 2SAT entscheidet.

Die oben skizzierte Komplexitätstheorie nach Cook und Karp hat Beziehungen zu anderen Bereichen, welche nur noch stichwortartig erwähnt werden können. Da ist zum einen die praktisch wichtige Klasse der kombinatorischen Optimierungsprobleme zu nennen, zu denen auch das Problem des Handlungsreisenden gehört. Zum anderen fanden die Physiker Beziehungen zur Theorie der Spin-Gläser, und neuerdings werden Analogien zwischen dem 3SAT-Problem und der Theorie der Phasenübergänge untersucht (Anderson, Nature, Vol. 400, 1999).

Prof. Dr. sc.math. Bruno Scarpellini
ist emeritierter Extraordinarius für Mathematik am Mathematischen Institut der Universität Basel.

Der wackelnde Gartentisch

Hanspeter Kraft

Die Situation ist Ihnen sicher wohlbekannt: Sie sitzen draussen im Freien, in bester Stimmung versammelt um einen runden Gartentisch und in Erwartung erfrischender Getränke. Doch leider wackelt der Tisch und die Gläser schwappen über. Die Reaktion darauf ist immer dieselbe: Zuerst schiebt man den Tisch erfolglos hin und her, wobei meistens noch mehr verschüttet wird, und dann sucht man sich irgendeinen Gegenstand, etwa ein Stück Papier oder Karton, um ihn unter das zu kurze Tischbein zu schieben. Damit gelingt es in der Regel, das Wackeln so zu reduzieren, dass nichts mehr überschwappt, mindestens solange niemand an den Tisch stösst und ihn wieder verschiebt. Damit ist die Sache zunächst erledigt, und die Gartenparty kann ihren Lauf nehmen.

Wir wollen jedoch dieses Ereignis dazu benutzen, über das eigene Verhalten in solchen Situationen nachzudenken. Es gibt nämlich eine überraschende und sehr elegante Lösung für dieses Problem, wie wir gleich sehen werden. Noch interessanter als die Lösung selbst ist jedoch die Frage, wie man darauf gekommen ist. Wir wollen einmal versuchen uns vorzustellen, wie die verschiedenen Ingenieure und Wissenschaftler an dieses Problem herangehen würden.

Der Praktiker

Stellen wir uns zunächst den typischen Praktiker vor, zum Beispiel einen Ingenieur, der mit diesem Problem konfrontiert wird. Er stellt fest, dass eines der Beine zu kurz (oder zu lang?) ist und dass man das Wackeln leicht beheben könnte, wenn die Länge der Beine variierbar wäre. Eine kurze Überlegung zeigt ihm, dass es genügt, die Länge eines Beines verstellbar zu machen. Natürlich hat er auch gleich eine Idee, wie man so etwas mit Hilfe eines Schraubengewindes konstruieren könnte. Bevor er jedoch an die Arbeit geht, gibt es verschiedene Dinge abzuklären.

– Patentanmeldung: *Gibt es bereits etwas Ähnliches und lässt sich die Konstruktion patentieren?*
– Marktabklärung: *Besteht ein Bedarf für diese «Anti-Wackel-Füsse», und mit welchen Firmen könnte man zusammenarbeiten?*

Falls dies alles positiv aussieht, wird der erste Prototyp gebaut und im praktischen Einsatz getestet. Ist dies erfolgreich, so muss die Finanzierung des Projektes geklärt werden. Dann geht es nach bekannten Schemata weiter. Entweder wird das Patent an eine Firma verkauft oder man findet einen Geldgeber und stellt die Anti-Wackel-Füsse selber her. Zum Schluss kommt natürlich noch ein zentraler Punkt, nämlich der Verkauf des Produktes, also das weltweite Marketing, denn schliesslich möchten alle Beteiligten etwas dabei verdienen.

Das Vorgehen des Praktikers ist also im Wesentlichen «Symptombekämpfung», ohne lange über die Ursachen nachzudenken. Neue Erkenntnisse werden zwar keine erbracht, doch sind einige Leute am Projekt beteiligt und verdienen daran. Es handelt sich also um einen *interdisziplinären Technologietransfer*, welcher Stellen schafft und Positives zum Bruttosozialprodukt beiträgt.

Der Experimentator

Nehmen wir als zweites Beispiel den typischen Experimentator, zum Beispiel einen Physiker. Er stellt fest, dass verwandte Probleme auch anderswo auftauchen und zum Teil schon Lösungen gefunden haben. So fährt zum Beispiel ein Auto auch auf vier Rädern und ebenfalls auf unebenen Oberflächen, ohne dass es wackelt und ohne dass ab und zu ein Rad in der Luft ist! (Auf jeden Fall nicht bei Normalbetrieb!)

Er kommt zur Ansicht, dass hier ein interessantes Problem vorliegt, bei dem es sich lohnt, eine genauere Abklärung vorzunehmen. Er beschliesst deshalb, ein Forschungsprojekt mit dem Titel «Über die Stabilität von Vielbeinern auf rauhen Oberflächen» einzureichen. Darin wird die allgemeine Problemstellung formuliert, bereits vorhandene Lösungen diskutiert und neue Ansätze und Ideen vorgeschlagen.

Sobald das Projekt bewilligt ist und die Mittel zur Verfügung stehen, wird das Forschungsteam zusammengestellt und mit den Experimenten begonnen. Unter anderem wird festgestellt, dass das Herumschieben des Gegenstandes kaum zum Erfolg führt, was auch durch eine theoretische Überlegung untermauert werden kann: *Die «stabilen» Positionen auf einer unebenen Oberfläche haben das Mass null. Damit ist die Wahrscheinlichkeit, durch Schieben auf eine solche zu treffen, also gleich null.*

Dann wird auch die Idee der «gedämpften Füsse» in Analogie zu den Autofedern und den Stossdämpfern untersucht. Bei einer solchen Lösung besteht allerdings die Gefahr, dass der Tisch ins Schwingen kommt, ein Problem, das sicher genauer untersucht werden muss.

Inzwischen ist einige Zeit vergangen, und es ist der erste Zwischenbericht fällig. (Dieser endet üblicherweise mit der Feststellung, dass noch mehr Mittel benötigt werden, um das Projekt zu einem erfolgreichen Abschluss zu bringen.) Wir wollen hier nicht weiter auf die Details eingehen; diese sind den Eingeweihten wohlbekannt.

Die umfangreichen Versuche und Versuchsergebnisse werden detailliert dokumentiert und mit statistischen Auswertungen versehen. Daraus entstehen in der Regel Diplom- und vielleicht sogar Doktorarbeiten. Es ist auch zu erwarten, dass die Forschungsergebnisse selber zu neuen Ideen Anlass geben und damit zu weiteren Projekten führen.

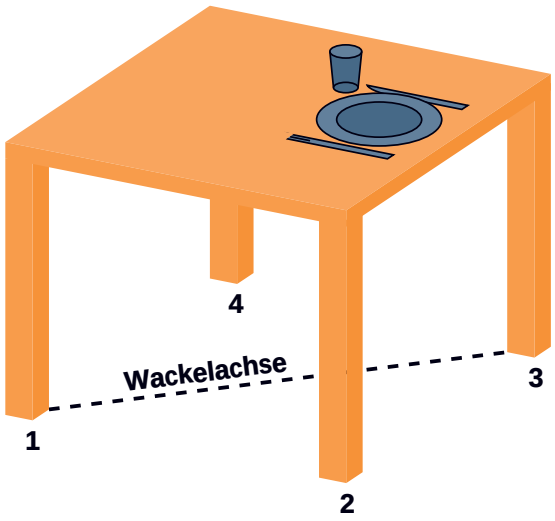
Damit hat der Experimentator die Relevanz seiner Forschungstätigkeit bei der Lösung praktischer Probleme nachgewiesen, dem Nachwuchs Gelegenheit zur eigenen Profilierung gegeben und somit einen wichtigen Beitrag zum Weiterbestand seiner Wissenschaft geleistet.

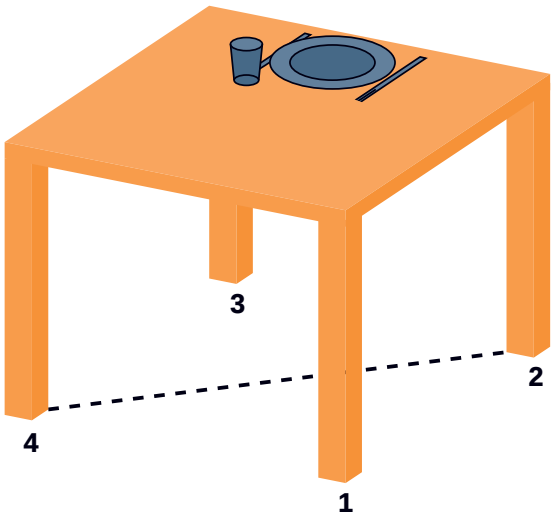
Der Theoretiker

Nehmen wir zum Schluss einen typischen Theoretiker, z.B. einen Mathematiker. Dieser stellt zunächst die Frage: Was ist «*wackeln*»?

Hierzu macht er die wichtige Beobachtung, dass beim Wackeln zwei gegenüberliegende Füsse auf dem Boden sind – die Gerade durch diese beiden Füsse ist die so genannte *Wackelachse* – und dass jeweils einer der andern beiden Füsse in der Luft ist. Daraus ergibt sich folgende zentrale Feststellung: *Es gibt zwei Wackelzustände für einen 4-beinigen Tisch, entsprechend den beiden möglichen Wackelachsen.*

Nun macht er das folgende Gedankenexperiment. Er denkt sich die Tischfüsse von 1 bis 4 durchnummeriert und startet mit einem Zustand mit Wackelachse 1 – 3, das heisst, die Füsse mit Nummer 1 und 3 sind am Boden und durch sie läuft die Wackelachse, während einer der Füsse mit Nummer 2 oder 4 in der Luft ist. *Nun hebt er in Gedanken den Tisch hoch, dreht ihn um 90° und stellt ihn wieder auf den Boden.* Selbstverständlich wackelt der Tisch nun genauso wie vorher, denn der Boden darunter hat sich ja nicht verändert[1]. Vom Tisch aus gesehen, sieht es allerdings anders aus, denn die Wackelachse läuft jetzt durch die Füsse mit den Nummern 2 und 4! (Er hat den Tisch ja um 90° gedreht.) Daraus kann er nun folgenden Schluss ziehen: *Im Laufe der Drehung um 90° ist die ursprüngliche Wackelachse in die dazu senkrechte Wackelachse «hinübergesprungen». Es muss also eine Zwischenposition geben, bei der dieser Wechsel der Wackelachse stattgefunden hat. In dieser Position kann der Tisch jedoch nicht wackeln!*





Damit hat er folgendes Ergebnis gefunden:
Schlussfolgerung: *Dreht man einen wackelnden Gartentisch um die eigene Achse in eine beliebige Richtung, so erreicht man innerhalb von 90° einen Zustand, in dem der Tisch nicht mehr wackelt.*

Dieses überraschend einfache Resultat lässt sich leider nicht patentieren, also auch nicht «technologisch transferieren» oder gar finanziell auswerten. Es ist auch nicht interdisziplinär entstanden, führte zu keinen Forschungsprojekten und erzeugte keine Diplom- oder Doktorarbeiten. Es ist schlicht und einfach originell, elegant und wirkungsvoll! Spontan glaubt es allerdings keiner, denn den meisten Menschen fehlt das Vertrauen in den abstrakten logischen Schluss, vor allem bei so genannten praktischen Problemen.

Wir überlassen es daher Ihnen, diese Methode in der Praxis zu überprüfen: Sie können damit Ihre Gäste beeindrucken! Wenn Sie dann noch anführen, dass Sie dies von einem theoretischen(!) Mathematiker gelernt haben, so bin ich Ihnen dafür dankbar.

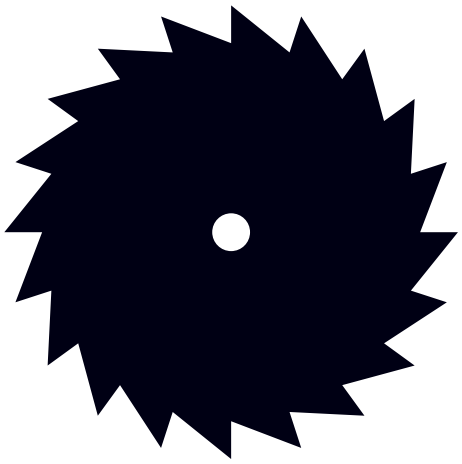
PS. Für den mathematisch gebildeten Laien sei hier angemerkt, dass hinter diesem Resultat ein Satz der Infinitesimalrechnung steckt, nämlich der so genannte «Zwischenwertsatz», welcher besagt, dass eine stetige Funktion f auf dem Intervall $[a,b]$ jeden Wert zwischen den beiden Randwerten $f(a)$ und $f(b)$ annimmt.

Prof. Dr.phil. Hanspeter Kraft ist Ordinarius für Mathematik am Mathematischen Institut der Universität Basel.

[1]Wir gehen davon aus, dass der Tisch keine Fehlkonstruktion ist, auf einer ebenen Oberfläche also nicht wackelt. Das ist sicher eine vernünftige Annahme für die Praxis.

Symmetrie in Schulalltag und Theorie

Hans Walser



Wie viel Fachwissen brauchen Lehrerinnen und Lehrer?

Am mathematischen Institut werden auch angehende Lehrerinnen und Lehrer für die Sekundarstufe 1 (7. – 9. Schuljahr, Orientierungsstufe, Weiterbildungsschule) ausgebildet. Die Frage nach den Inhalten der Fachausbildung beschäftigt uns immer wieder. Um es auf den Punkt zu bringen: Brauchen Lehramtskandidaten etwas zu wissen, das über den Satz des Pythagoras oder das Lösen linearer Gleichungen hinausgeht?

Am Beispiel *Symmetrie* soll gezeigt werden, wie wir den Zusammenhang zwischen Theorie und Schulpraxis sehen.

Symmetrie?

Narziss sieht sein Spiegelbild im Wasser. Die Spiegelsymmetrie ist die bekannteste Symmetrieart. Symmetrie bedeutet allgemein das Vorhandensein einer gleichmässigen Entsprechung. Dazu gehört die «Opfersymmetrie» in einer Budgetdebatte ebenso wie die mehrfache Wiederholung in einem Lied.

Was können wir an der Position eines Kreissägeblattes verändern, ohne dass eine Beobachterin, welche den Raum kurzzeitig verlassen hat, eine Veränderung feststellen kann? Wir können das Sägeblatt um einen oder mehrere Zähne drehen; das Sägeblatt hat eine *Drehsymmetrie*.

In einem Scherenschnitt finden wir zusätzlich zu einer meist achtteiligen Drehsymmetrie auch *Achsensymmetrien*, welche durch das Falten des Blattes vor dem Schneiden entstanden sind.

blablablablablablabl

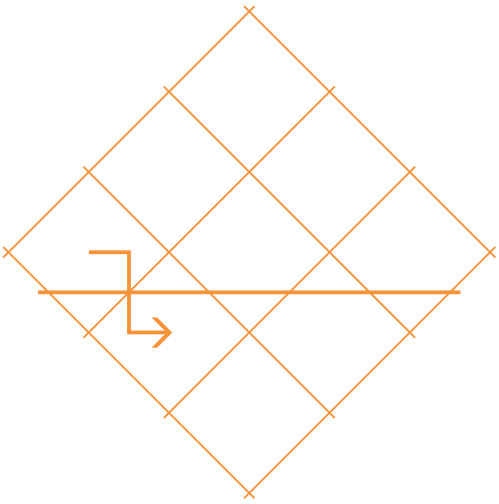
Translationssymmetrie

Schubspiegelsymmetrie

Eine ewige Wiederholung wie im monotonen *blabla* heisst *Schubsymmetrie* oder *Translationssymmetrie*. Dabei muss das *blabla* allerdings unendlich lang, das heisst ohne Anfang und ohne Ende, gedacht werden. Haben Sie auch schon solche Vorträge gehört?

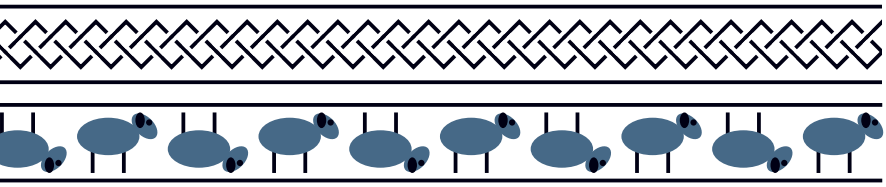
Translationssymmetrie liegt auch jedem Bandornament zugrunde, dabei können allerdings noch andere Symmetrien auftreten.

Eine regelmässige Fussspur im Sand ist translationssymmetrisch, nach jedem Doppelschritt ergibt sich dasselbe Bild. Wenn wir die Fussspur aber nur um einen einfachen Schritt verschieben, kommen wir auch mit einer Spiegelung an der Längsachse auf das ursprüngliche Bild zurück; wir haben eine *Schubspiegelsymmetrie*. Dies ist die am wenigsten bekannte Symmetrieart. Sobald wir aber das Auge dafür schärfen, sehen wir sie an unerwarteten Orten. Als einfaches Beispiel finden die Studierenden Schubspiegelsymmetrie in einem Karomuster. Eine Schubspiegelachse läuft schräg über die Kantenmitten der einzelnen Quadrate. Viel schwieriger ist die Frage, ob die Spur eines Hinkenden ebenfalls Schubspiegelsymmetrie aufweist – sie tut es nicht. Wir können nach einer Verschiebung entweder die linken Fussspuren auf die rechten spiegeln oder die rechten Fussspuren auf die linken, aber nicht beide gleichzeitig. Dies kann am besten mit einer Kopie der Fussspur auf einer Transparentfolie gezeigt werden: Nach dem Abheben und Umdrehen der Transparentfolie können wir die Kopie nicht mehr mit dem Original zur Deckung bringen.

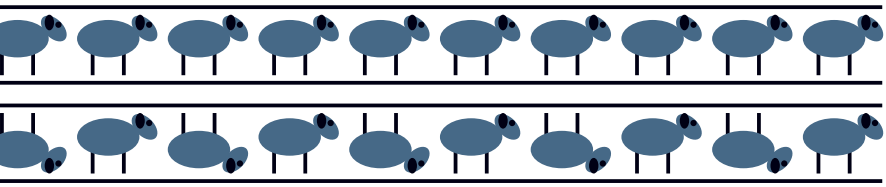


Schubspiegelsymmetrie

Keine Schubspiegelsymmetrie



Verschiedene Bildinhalte, aber gleiche Symmetrieklasse: Schubspiegelsymmetrie



Gleiche Bildinhalte, aber verschiedene Symmetrieklassen: Translationssymmetrie und Schubspiegelsymmetrie

Symmetrieklasse F_1: Nur Translationen

Symmetrieklasse F_2: Punktspiegelungen (Drehungen um 180°)

Symmetrieklasse F_3: Achsenspiegelung vertikal

Symmetrieklasse F_4: Achsenspiegelung horizontal

Symmetrieklasse F_5: Punktspiegelungen, Achsenspiegelung horinzontal und vertikal

Symmetrieklasse F_6: Punktspiegelungen, Achsenspiegelungen horizontal

Symmetrieklasse F_7: Schubspiegelungen

Bandornamente

Wie viele Bandornamente gibt es? Die Frage wirkt befremdlich; natürlich gibt es unendlich viele Bandornamente. Dabei ist es allerdings so, dass zwei Bandornamente mit völlig verschiedenen Bildinhalten dasselbe Symmetrieverhalten zeigen können. Sie gehören zur selben *Symmetrieklasse*, während andererseits Bandornamente mit denselben Bildbestandteilen zu verschiedenen Symmetrieklassen gehören können. Damit stellt sich eine neue Frage: Wie viele *Symmetrieklassen* gibt es bei Bandornamenten?

Diese Frage wird von Schülerinnen und Schülern der Sekundarstufe auf zwei verschiedenen Wegen angegangen: Sie zeichnen Bandornamente (ein dankbares Thema für den Einsatz von Graphiksoftware, bei welcher sich die Translationssymmetrie durch Kopieren bewerkstelligen lässt) und versuchen hinterher, die Beispiele zu ordnen und zu klassifizieren. Andererseits werden auf theoretischem Weg die möglichen Symmetrien bei einem Bandornament festgehalten: Spiegelung an der Mittellinie, Spiegelung an einer senkrechten Linie, Punktsymmetrie, Schubspiegelsymmetrie sowie – und das ist das Entscheidende – Kombinationen davon. Eine Spiegelung an einer schrägen Symmetrieachse ist nicht möglich, weil dabei das Band seine horizontale Lage verlieren würde. Ebenso ist eine Vergrösserung ausgeschlossen, weil sonst das Band breiter würde. Mit diesem Vorgehen bewegen sich Schülerinnen und Schüler auf dem Boden der mathematischen *Gruppentheorie*.

Klassifikation der Bandornamente

Mit gruppentheoretischen Überlegungen kann gezeigt werden, dass es nur sieben Symmetrieklassen gibt. Die Erfahrung im Unterricht zeigt allerdings, dass Schülerinnen und Schüler oft vermeintlich mehr als sieben Klassen finden; es ist offenbar nicht ganz einfach, in verschiedenen Bandornamenten dieselben Symmetrieklassen zu sehen.

Die einfachste Symmetrieklasse F_1 enthält nur Translationssymmetrie; die anderen Symmetrieklassen enthalten zusätzlich weitere Symmetriearten. Die Symmetrieklassen können durch Angabe der vorkommenden Symmetriearten beschrieben werden. Eindrücklicher ist allerdings die Illustration durch ein einfaches Beispiel. Dies kann durch stilisierte Buchstaben geschehen.

Bandornamente und Scherenschnitte

Wird ein Papierstreifen mehrfach mit senkrechten Faltlinien gefaltet, in gefaltetem Zustand beschnitten und dann wieder aufgefaltet, entsteht ein Bandornament der Symmetrieklasse F_4. Lässt sich jede Symmetrieklasse der Bandornamente durch einen Scherenschnitt darstellen? Dies ist tatsächlich möglich; das Schwierige dabei ist der Faltvorgang.

Soll der Scherenschnitt zum Beispiel nur Translationssymmetrie (Symmetrieklasse F_1) enthalten, darf der Streifen weder waagrecht noch senkrecht gefaltet werden, da ansonsten Achsensymmetrien entstehen. Der Streifen kann aber rechtwinklig abgebogen werden, wodurch Faltlinien entstehen, welche in einem Winkel von 45° über den Streifen laufen. Der Faltvorgang ist periodisch, indem der Anfangsteil nach vier Schritten wieder in die ursprüngliche Richtung zeigt. Wir erhalten schliesslich (nach Einbiegen der Anfangs- und Endteile) ein auf der Spitze stehendes Quadrat. Wenn wir dieses Quadrat vor dem Auffalten an den Seiten zuschneiden, ergibt sich nach dem Auffalten ein Bandornament, das nur Translationssymmetrie enthält. Man wird einwenden, dass dieser Scherenschnitt doch offensichtlich auch achsensymmetrische Figuren enthält. Dies ist richtig, aber diese Symmetrien sind immer nur *lokale Symmetrien*, welche sich nicht auf das ganze Bandornament ausdehnen lassen.

Bei einem Scherenschnitt, welcher lediglich Translationssymmetrie und Schubspiegelsymmetrie (Symmetrieklasse F_7) enthalten soll, ist ein Falten unter Winkeln von 60° erforderlich. Bei dieser Symmetrieklasse ist uns kein glattrandiger Scherenschnitt gelungen.

Dr. sc.math. Hans Walser ist Lehrbeauftragter für Mathematik für die Sekundarstufe I am Mathematischen Institut der Universität Basel.

Symmetrieklasse F_1

Symmetrieklasse F_2

Symmetrieklasse F_3

Symmetrieklasse F_4

Symmetrieklasse F_5

Symmetrieklasse F_6

Symmetrieklasse F_7

Ostrowski und der Ostrowski-Preis

Walter Gautschi

Professor Alexander Ostrowski in den 50er-Jahren

Alexander M. Ostrowski, langjähriger Ordinarius für Mathematik an der Universität Basel, hat den Ruhm der Basler Mathematik, der durch Euler und die Bernoullis begründet wurde, in höchst eindrücklicher Weise weitergetragen. Er war einer der letzten grossen Mathematiker, die noch eine Gesamtübersicht über die Mathematik besassen und die wichtige Beiträge zu praktisch allen Teilgebieten der Mathematik leisten konnten. So sind Ostrowskis Arbeiten in der Algebra, der reellen und komplexen Analysis, der Zahlentheorie, der Geometrie, der Wahrscheinlichkeitsrechnung und selbst der Numerik weltweit bekannt.

Leben und Person

Ostrowski wurde am 25. September 1893 in Kiev geboren. Schon im Alter von 18 Jahren begann er, privat mit Dimitrii Aleksandrowitsch Grave zu studieren, einem Begründer der russischen Schule der Algebra und selbst ein ehemaliger Schüler von Tschebyscheff in St. Petersburg. Aus diesem Kontakt mit Grave entstand Ostrowskis erste mathematische Publikation: eine lange, in Russisch abgefasste Arbeit über Galois-Körper.

Studium

Er ging weiter nach Marburg, um dort zu studieren, geriet aber in zivile Haft, als der Erste Weltkrieg ausbrach. Dank einer Intervention von Hensel wurden die Einschränkungen seiner Bewegungsfreiheit etwas erleichtert, und es wurde ihm erlaubt, die Universitätsbibliothek zu benutzen. Das war alles, was er wirklich brauchte. Während dieser Periode der Isolation entwickelte Ostrowski, praktisch ohne Hilfe, seine jetzt berühmte Bewertungstheorie von Körpern.

Nach dem Krieg, als der Frieden zwischen der Ukraine und Deutschland wieder hergestellt war, zog Ostrowski 1918 nach Göttingen, damals weltweit die Hochburg der Mathematik. Dort stach er bald unter den Studenten durch sein phänomenales Gedächtnis hervor und seine schon ausgiebige und auf breiter Basis beruhende Kenntnis der mathematischen Literatur. Einer der Studenten erinnerte sich später, dass die mühsame Literatursuche in Göttingen sehr einfach war: Man brauchte nur den russischen Studenten Ostrowski zu fragen und man bekam die Antwort – unverzüglich! Er konnte so etwas sagen wie: Oh ja, das können Sie in einer 1882 publizierten Dissertation von Herrn so und so in Rostock finden – einer Quelle, in der niemand im Traum nachgeschlagen hätte. Einmal musste er sogar Hilbert zu Hilfe kommen, als dieser während eines Vortrags, wie er sagte, ein schönes Theorem brauchte, an dessen Autor er sich nicht mehr erinnern konnte. Es war Ostrowski, der ihm zuflüstern musste: «Aber, Herr Geheimrat, es ist ja eines Ihrer eigenen Theoreme!»

Es ist deshalb nicht überraschend, dass Felix Klein Ostrowski als einen seiner Assistenten zu sich nahm und ihm, zusammen mit Fricke, die Herausgabe des ersten Bandes seiner gesammelten Werke anvertraute. 1929 promovierte er *summa cum laude* mit einer unter Hilbert und Landau geschriebenen Dissertation. Auch diese sorgte für einige Aufregung, weil sie zum Teil eine Antwort gab auf Hilberts 18. Problem. Es gelang Ostrowski zu beweisen, dass Dirichlets Zeta-Reihe keiner algebraischen Differenzialgleichung genügen kann.

Weiterbildung

Ostrowskis Habilitation fand in Hamburg statt mit einer ebenfalls von Hilbert angeregten Arbeit, die mit Modulen über polynomiale Ringe zu tun hatte. 1922 kehrte Ostrowski nach Göttingen zurück, wo er über neuere Entwicklungen in der komplexen Funktionentheorie lehrte. Das führte zu seinen Arbeiten über Lückentheoreme, Überkonvergenz von Potenzreihen und das Randverhalten von konformen Abbildungen. Nach einem Jahr als Rockefeller Research Fellow in Oxford, Cambridge und Edinburgh erhielt er 1927 – und akzeptierte – einen Ruf an die Universität Basel. Die lokale Zeitung konnte es nicht unterlassen zu kommentieren, dass 200 Jahre früher die Universität Euler nach St. Petersburg verlor, wegen des Losentscheids, der damals angewandt wurde, um zwischen sich bewerbenden Kandidaten auszuwählen . Jetzt aber gewann die Universität das grosse Los, indem sie Ostrowski aus Russland nach Basel brachte!

Hilberts berühmte 23 Probleme wurden von ihm am Internationalen Mathematiker-Kongress im Jahre 1900 in Paris vorgetragen. Sie haben viel dazu beigetragen, der Mathematik des 20. Jahrhunderts neue Impulse und Forschungsrichtungen zu verleihen. Einige dieser Probleme sind bis heute offen geblieben.

Die Basler Jahre

Ostrowski blieb während seiner ganzen akademischen Karriere in Basel, mit Ausnahme gelegentlicher Besuche in den Vereinigten Staaten und Kanada. Es war in Basel, wo der Grossteil seines mathematischen Werkes sich entfaltete. Es ist weder der Ort noch die Zeit, hier sein Werk im Einzelnen darzustellen. Selbst wenn es so wäre, wäre es unmöglich, auch nur eine Andeutung zu geben von der enormen Vielfalt und Tiefe seiner Beiträge. Erwähnt werden soll, dass am Anfang der 30er-Jahre, und besonders nach den 50er-Jahren, eine beachtliche Verschiebung seiner Interessen von der reinen Mathematik zur mehr angewandten Mathematik stattgefunden hat, die zweifellos das Aufkommen leistungsfähiger elektronischer Rechner widerspiegelte. Ostrowski blieb mathematisch aktiv bis in seine 80er-Jahre und konnte noch im Alter von 90 Jahren die Veröffentlichung seiner Gesammelten Werke übersehen. Diese erschienen schliesslich in sechs Bänden (Alexander Ostrowski, Collected mathematical papers, Vols. 1 – 6, Birkhäuser, Basel, 1983 – 1985). Im Jahr 1949 heiratete Ostrowski Margret Sachs, eine Psychoanalytikerin aus der Schule von Carl Gustav Jung, die auch einmal, wie sie mir erzählt hat, Sekretärin und Vertrauensperson des Schweizer Schriftstellers Carl Spitteler gewesen war. Ihre warme, charmante Persönlichkeit half, den strengen Lebensstil des Gelehrten Ostrowski zu mildern, und vermittelte ein gewisses Mass von Lebensfreude.

Emeritierung

Nach Ostrowskis Emeritierung im Jahr 1958 nahmen er und seine Frau Wohnsitz in Montagnola, wo sie eine schöne Villa gebaut hatten – Almarost (ALexander MARgret OSTrowski), wie sie sie nannten – mit einem schönen Blick auf den Luganersee. Sie waren immer froh, Besucher in Almarost zu empfangen, und ihre anmutige Gastfreundschaft war legendär. Frau Ostrowski, die die Neigungen der Mathematiker gut kannte, führte sie immer hinunter in Ostrowskis Bibliothek, um sie eine Weile allein zu lassen, so dass sie das Neueste in der Mathematik und den neuesten Klatsch einholen konnten. Die Wände der Bibliothek waren voll mit Büchern, nicht nur mathematischen, sondern auch einigen mit Science-fiction- und Detektivgeschichten, die seine bevorzugte Freizeitlektüre ausmachten.

Frau Ostrowski starb 1982, vier Jahre vor Ostrowskis Tod im Jahr 1986. Beide sind auf dem schönen Friedhof von Gentilino begraben, nicht weit vom Grab von Hermann Hesse, mit dem sie befreundet waren. Ostrowski ist mir in Erinnerung als ein Mann, der sich vollständig seiner Wissenschaft hingegeben hat, der aussergewöhnlich hartnäckig war im Umgang mit Problemen, so sehr, dass, wenn er mit ihnen fertig geworden war, wenige Fragen, wenn überhaupt welche, offen blieben. Er konnte den Scharfsinn in den Arbeiten anderer aufrichtig bewundern, aber zur gleichen Zeit auch seiner Verachtung Ausdruck geben über allfällige Unsorgfältigkeiten.

Der Ostrowski-Preis

Der Preis für Mathematik wurde anfangs der 80er-Jahre von Professor und Frau Ostrowski gegründet mit der Festsetzung, dass er nach deren Tod alle zwei Jahre zuerkannt werden soll. Der Zweck des Preises ist: « … die mathematischen Wissenschaften durch periodische Verleihung eines internationalen Preises zu fördern, der die besten Leistungen anerkennen soll, die in den vorangegangenen fünf Jahren auf dem Gebiet der reinen Mathematik und der theoretischen Grundlagen der numerischen Mathematik erzielt worden sind». Es ist charakteristisch für Ostrowskis Einschätzung der Mathematik als eine internationale und universelle Wissenschaft, dass er ausdrücklich stipulierte, dass die Verleihung «gänzlich ohne Berücksichtigung von Politik, Rasse, Religion, Wohnort, Nationalität oder Alter des Preisträgers» erfolgen soll.

Der Stiftungsrat betreut das Vermögen der Stiftung und setzt die Preissumme fest. Die Auswahl der Preisträger ist die Aufgabe einer Jury, die aus je einem Vertreter von fünf wissenschaftlichen Institutionen zusammengesetzt sein soll: den mathematischen Instituten der Universität Basel, Jerusalem und Waterloo und den wissenschaftlichen Akademien von Kopenhagen und Amsterdam. Einer dieser Vertreter amtiert abwechslungsweise als Präsident der Jury.

Die bisherigen Preisträger

Bis anhin wurde der Preis sechsmal verliehen. Der erste ging an Louis de Branges für seinen Beweis der Bieberbachschen Vermutung. Der zweite Gewinner war Jean Bourgain, dessen Arbeit in Ergodentheorie anerkannt wurde. Der dritte Preis wurde gemeinsam Miklós Laczkovich und Marina Ratner verliehen für ihre Arbeiten über Lie-Gruppen. Den vierten Preis erhielt Andrew Wiles für seinen Beweis der Letzten Fermatschen Vermutung. Der fünfte Preis wurde gemeinsam Yuri V. Nesterenko und Gilles Jean Georges Pisier für ihre Arbeiten in Algebraischer Zahlentheorie und der Theorie der Operatoren verliehen. 1999 ging der Preis an Alexander Beilinson und Helmut Hofer für ihre Arbeiten in Algebraischer resp. Symplektischer Geometrie.

Leicht überarbeitete Deutsche Fassung von «Ostrowski and the Ostrowski Prize», Mathematical Intelligencer, 20 (1998), 32 – 34, mit Bewilligung des Springer-Verlages.

Walter Gautschi war Assistent und 1953 Doktorand von Ostrowski und ist seit 1963 Professor für Mathematik und Informatik an der Purdue University in Lafayette, Indiana, USA. Zurzeit ist er Gastdozent an der Universität Basel.

Mathematik und Computer

Das Vier-Farben Problem

Jede Landkarte kann mit höchstens vier Farben so koloriert werden, dass je zwei benachbarte Länder verschiedene Farben erhalten.

Anders gesagt: Eine beliebige, endliche Ansammlung offener, disjunkter ebener Polygone (Länder) kann derart in vier Klassen (Farben) eingeteilt werden, dass sich die Abschliessungen zweier unterschiedlicher Polygone derselben Klasse in nur endlich vielen Punkten schneiden.

Geschichte: Formuliert von Francis Guthrie und niedergeschrieben von seinem Bruder Frederick (1852) in einem Brief an Sir William Rowan Hamilton.

Anspruch auf Beweise erhoben der Rechtsanwalt Kempe (1879) und der Physiker Tait (1880); erhebliche Fehler wurden von Heawood (1890) gefunden, Teilresultate von Birkhoff (1913), Heesch (1969) und Mayer (1969, 1975); Letzterer war Professor für französische Literatur in Montpellier und entdeckte später in den Tagebüchern von Valéry Aufzeichnungen zum Vier-Farben-Problem. Schliesslich gelang Appel und Haken (1976) in Urbana, Illinois, ein Beweis mit Hilfe eines IBM-360-Computers. Seit damals ist der Beweis überprüft und vereinfacht worden, allerdings bleibt der Einsatz des Computers unvermeidbar.

Die Keplersche Vermutung

Die «übliche» Kugelpackung ist die dichteste unter allen möglichen Kugelpackungen. (Bei der «üblichen» Kugelpackung bilden die Kugelmittelpunkte ein flächenzentriertes Würfelgitter.)

Anders gesagt: Mit $n(r)$werde die maximale Anzahl disjunkter Einheitskugeln bezeichnet, die in eine Kugel vom Radius r eingepasst werden können. Dann gilt, dass die Packungsdichte $\limsup n(r)/r^3$ für $r \to \infty$, höchstens so gross ist wie die Packungsdichte der üblichen Kugelpackung, nämlich $\pi\sqrt{2}/6$.

Geschichte: Formuliert von Kepler (1610) in *Strena seu de nive sexangula* (über Schneeflocken).

Teilresultate von Gauss (1831), Thue (1910), Fejes Tóth (1953) und Rogers (1958); Letzterer kommentierte: «Viele Mathematiker glauben, und alle Physiker wissen, dass die Packungsdichte stets kleiner oder gleich $\pi\sqrt{2}/6$ ist.» Den Schlüssel zur Lösung fand Muder (1993), gefolgt von der Veröffentlichung eines vollständigen Beweises durch Hsiang (1993), der allerdings keine allgemeine Anerkennung fand. Schliesslich kündigten Hales und Ferguson (1998) einen Beweis an und reichten ihre Arbeit bei den *Annals of Mathematics* ein. Dort versucht zurzeit eine Gruppe von 12 Experten, die Korrektheit des Beweises zu überprüfen. Das Haupthindernis ist der massive Einsatz des Computers.