Hier gibt es zwei Vorzeichenwechsel, also haben wir zwei Nullstellen in $[-3, 2]$ und eine in $[2, 6]$. Letzteres Intervall enthält also bereits nur eine einzige Nullstelle und kann somit, falls wir keine Ansprüche an die Intervallängen stellen, in die Ergebnisliste.

Das Intervall $[-3, 2]$ muß weiter zerlegt werden, z.B. an der Stelle $x = 0$:

```
> Sturm(0);
```

$$[-1, 1, 1, -1, -1, -1]$$

Wieder zwei Vorzeichenwechsel, also gibt es keine Nullstelle in $[0, 2]$, aber zwei in $[-3, 0]$. Wir zerlegen weiter an der Stelle $x = -1$:

```
> Sturm(-1);
```

$$[1, 1, -1, 1, -1, -1]$$

Das sind drei Vorzeichenwechsel, also haben wir eine Nullstelle in $[-3, -1]$ und eine in $[-1, 0]$.

Wenn uns die Intervallängen nicht interessieren, sind wir damit fertig; wenn wir allerdings Intervalle der Länge eins wollen, müssen wir $[-3, -1]$ und $[2, 6]$ noch weiter unterteilen:

```
> Sturm(-2);
```

$$[-1, 1, -1, 1, -1, -1]$$

Vier Vorzeichenwechsel, die Nullstelle liegt also in $[-2, -1]$.

```
> Sturm(4);
```

$$[1, 1, 1, 1, -1, -1]$$

Ein Vorzeichenwechsel; die Nullstelle liegt in $[2, 4]$.

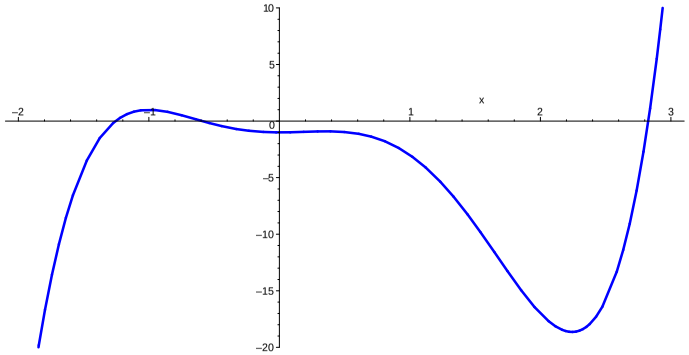
```
> Sturm(3);
```

$$[1, 1, 1, 1, -1, -1]$$

Dieselbe Folge, also liegt die Nullstelle in $[2, 3]$.

Wir haben also drei reelle Nullstellen, und sie liegen in den Intervallen $[-2, -1]$, $[-1, 0]$ und $[2, 3]$. Durch eine Zeichnung können wir uns vergewissern, daß die Nullstellen wirklich so liegen:

```
> plot(f, x=-3..2, color=blue, thickness=5);
```

Wie gut (und schnell) man die Nullstellen im konkreten Fall isolieren kann, hängt natürlich ab von deren Abstand. Erfahrungsgemäß funktioniert der Algorithmus recht gut; er ist auch in vielen Computeralgebrasystemen standardmäßig vorhanden. In Maple bestimmt `realroot(f)` für ein Polynom mit *ganzzahligen* Koeffizienten diese Intervalle; gibt man noch ein zweites Argument ℓ an, so werden Intervalle einer Länge von höchstens ℓ berechnet.

Da der Algorithmus in der Praxis gut funktioniert, könnte man es dabei bewenden lassen und an eine Bemerkung von ZASSENHAUS denken, der in einem Kolloquiumsvortrag an der Universität Karlsruhe einmal sagte: „In der experimentellen Mathematik haben wir es nicht nötig, die Sätze zu beweisen, die wir für wahr halten.“ Tatsächlich aber ist von ZASSENHAUS so gut wie keine unbewiesene Behauptung überliefert, und auch für unser Problem gibt es bewiesene Resultate: Wie KURT MAHLER 1964 zeigte, ist der Betrag des Abstands zwischen zwei verschiedenen Nullstellen eines Polynoms $f \in \mathbb{C}[x]$ vom Grad n mit Diskriminante D mindestens gleich

$$\frac{\sqrt{3D}}{n^{(n+2)/2}\,\|f\|_1^{n-1}}\,.$$

Der Beweis verwendet abgesehen von den üblichen Techniken, die wir schon mehrfach beim Beweis von Schranken kennengelernt haben, vor allem die Ungleichung von HADAMARD; da er relativ lang ist, sei hier darauf verzichtet. Interessenten finden ihn gut lesbar in der (auch frei im Netz zugänglichen) Originalarbeit

K. MAHLER: An inequality for the discriminant of a polynomial, *Michigan Math. J.* **11** (1964), 257–262

oder in §7.2.4 des Buchs

ALKIVAIDIS G. AKRITAS: Elements of Computer Algebra with Applications, *Wiley*, 1989

KURT MAHLER wurde 1903 in Krefeld als Sohn eines Buchdruckers geboren. Da er seit früher Kindheit an Knochen-Tuberkulose litt, ging er nur 1 1/2 Jahre zur Vorschule und 2 1/2 Jahre zur Volksschule. Um Feinmechaniker zu werden besuchte er ab 1917 zwei Jahre lang elementare technische Schulen in Krefeld. Dabei entdeckte er sein Interesse an Mathematik und kaufte sich entsprechende Bücher, die er parallel zur Schule studierte. Der Direktor seiner Schule schickte einige seiner Arbeiten an FELIX KLEIN, der sie seinem damaligen Assistenten CARL LUDWIG SIEGEL zur Begutachtung gab. Dieser befand, daß man MAHLER ein Mathematikstudium ermöglichen sollte. Mit Hilfe mehrerer Lehrer seiner Schule konnte er das Abitur bestehen und studierte dann ab 1923 bei SIEGEL in Frankfurt, ab 1925 bei HILBERT, COURANT, EMMY NOETHER, BORN, HEISENBERG und anderen in Göttigen, wo er auch eine Zeitlang als unbezahlter Assistent von NORBERT WIENER arbeitete. 1927 wurde er in Frankfurt promoviert mit einer Arbeit über die Nullstellen der Γ-Funktion. 1933 erhielt er eine Stelle an der Universität Königsberg, konnte diese jedoch als Jude wegen der Machtergreifung der Nationalsozialisten nicht antreten. Auf Einladung von MORDELL ging er stattdessen nach Manchester, wo er abgesehen von zwei Jahren in Groningen trotz einer dreimonatigen Internierung als feindlicher Ausländer bis 1962 blieb. Seine letzten sechs Berufsjahre verbrachte er in Canberra, Australien, wo er auch nach seiner Emeritierung noch regelmäßig publizierte. Er starb dort im Februar 1988; seine letzte mathematische Arbeit erschien 1989. Praktisch alle seiner vielen Arbeiten befassen sich mit der Zahlentheorie; besonders berühmt sind seine Beiträge zur Theorie der transzendeten Zahlen.

§5: Rechnen mit reellen Zahlen

Trotz ihres Namens sind die reellen Zahlen alles andere als real: Es wäre beispielsweise völlig sinnlos, von einem realen Gegenstand zu sagen, er haben eine Länge von $\sqrt{2}\,m$ oder eine Masse von $\pi\,kg$. Die reellen Zahlen bilden schließlich eine überabzählbare Menge, während wir in einer endlichen Welt leben. Auch unsere Gehirne und unsere Computer

sind endlich. Trotzdem zeigt die Erfahrung von über zwei Jahrtausenden, daß die reellen Zahlen gerade wegen der idealisierten Annahmen, die ihnen zugrunde liegen, extrem nützlich sind für die Beschreibung naturwissenschaftlicher und teilweise auch wirtschaftlicher und sozialer Phänomene.

Wirklich rechnen können wir aber nicht mit reellen Zahlen: wie DANIEL RICHARDSON 1969 zeigte, können wir nicht einmal immer entscheiden, ob eine durch einen relativ einfachen Ausdruck gegebene reelle Zahl verschwindet oder nicht. Mit dem, was wir heute wissen, können wir seinen Satz so formulieren:

Satz von Richardson: Es gibt kein Verfahren, das in endlich vielen Schritten entscheidet, ob ein beliebig vorgegebener Ausdruck bestehend aus rationalen Zahlen, π, einer Variablen x sowie den Funktionen $+$, $\cdot$, Sinus und Betrag verschwindet.

DANIEL RICHARDSON wurde 1941 in Chicago geboren. Er studierte Mathematik in New York und in San Fransisco, wo er 1962 seinen Bachelor bekam. Danach ging er an die Universität von Bristol und promivierte dort 1965 in mathematischer Logik. Nach verschiedenen ein- bis zweijährigen Tätigkeiten an Universitäten und in der Industrie wurde er 1988 zunächst Lecturer, später Senior Lecturer, an der Universität von Bath. `http://people.bath.ac.uk/masdr/`

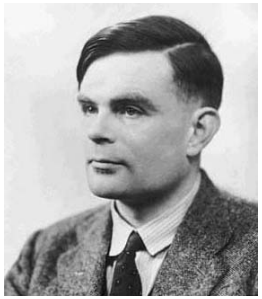
Ein vollständiger Beweis des Satzes von RICHARDSON wäre fast eine eigene zweistündige Vorlesung; deshalb sollen hier nur die wesentlichen Ideen kurz skizziert werden.

Das erste Unentscheidbarkeitsresultat in der Geschichte der Mathematik war ein berühmter Satz von KURT GÖDEL (1906–1978), wonach jedes Axiomensystem zur Charakterisierung der natürlichen Zahlen entweder Widersprüche enthält oder aber nicht jede wahre Aussage als Folgerung ableiten läßt.

Die damit bewiesene Unentscheidbarkeit der Zahlentheorie wurde wenig später mit anderen Ansätzen auch von ALAN TURING (1912–1954), EMIL POST (1897–1954) und von ALONZO CHURCH (1903–1995) gezeigt. Am einfachsten verständlich ist wohl der Ansatz von TURING in seiner (auch vielfach im Netz zu findenden) Arbeit

ALAN K. TURING: On computable numbers with an application to the Entscheidungsproblem, *Proc. London Math. Soc.* **42** (1936), 230–265 *und* **43** (1937), 544–546

Darin zeigt er, daß es kein Verfahren geben kann, das für einen beliebigen Algorithmus zeigt, ob er abbricht: Gäbe es nämlich so ein Verfahren $V(A, E)$, das genau dann die Antwort „bricht ab“ liefert, wenn der Algorithmus A mit Eingabe E nach endlich vielen Schritten abbricht, und „bricht nicht ab“ sonst, so könnten wir V auch auf den folgenden Algorithmus $W(A)$ anwenden: Breche ab, falls $V(A, A)$ zum Ergebnis „bricht nicht ab“ kommt, und gehe sonst in eine Endlosschleife. Offensichtlich bricht $W(W)$ genau dann ab, wenn $V(W, W)$ uns sagt, daß $W(W)$ *nicht* abbricht und umgekehrt. Somit kann V nicht immer das richtige Ergebnis liefern. Er stellt auch die Verbindung mit natürlichen Zahlen her, indem er Programmen Zahlen zuordnet.



ALAN MATHISON TURING wurde 1912 in London geboren. Ab 1931 studierte er Mathematik an der Universität Cambridge; 1935 wurde er auf Grund einer Arbeit über den zentralen Grenzwertsatz *fellow* am King's College; dort publizierte er 1936 die oben zitierte Arbeit. Da CHURCH im gleichen Jahr mit anderen Methoden dasselbe Unentscheidbarkeitsresultat veröffentlich hatte, kam es zu Diskussionen zwischen den beiden und TURING ging 1937 zu CHURCH and die Universität Princeton. 1938 kehrte er nach England zurück und begann mit Plänen zum Bau eines Computers zur Berechnung der Nullstellen der RIEMANNschen ζ-Funktion. Diese Arbeit wurde unterbrochen durch den zweiten Weltkrieg; ab 1939 arbeitete er in der Code and Cypher School in Bletchley Park, wo er unter anderem Rechenmaschinen (die sogenannten Bomben) zum Knacken der deutschen Enigma-Verschlüsselung entwickelte. 1942/43 war er in den USA an einem britisch-amerikanischen Projekt zur Sprachverschlüsselng beteiligt.

Nach Kriegsende entwarf und baute er am National Physical Laboratory in London einen der ersten Computer; 1948 wurde er nach einem kurzen Zwischenaufenthalt in Cambridge Mathematikprofessor in Manchester. Dort arbeitete er unter anderem am Wortproblem für Gruppen und über Reaktions-Diffusionsgleichungen zur Modellierung der Morphogenese, d.h. der Entstehung biologischer Formen und Strukturen. Sein Tod 1954 wurde offiziell als Selbstmord bezeichnet, könnte aber auch ein Unfall bei einem chemischen Experiment gewesen sein.

Wie man heute weiß, gibt es unentscheidbare Mengen auch im Zusammenhang mit Polynomgleichungen. Ausgangspunkt dafür ist eines der 23 Probleme, die DAVID HILBERT 1900 auf dem Internationalen Mathematikerkongreß in Paris vorstellte und von denen er glaubte, daß sie für die Mathematik des 20. Jahrhunderts wichtig sein sollten. Die Probleme kamen aus allen Teilgebieten der Mathematik und hatten auch sehr unterschiedlichen Schwierigkeitsgrad: Einige wurden schon sehr bald gelöst, andere sind auch heute nach mehr als ein Jahrhundert noch offen. Das zehnte Problem lautete:

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung

Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoeffizienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

DAVID HILBERT (1862–1943) wurde in Königsberg geboren, wo er auch zur Schule und zur Universität ging. Er promovierte dort 1885 mit einem Thema aus der Invariantentheorie, habilitierte sich 1886 und bekam 1893 einen Lehrstuhl. 1895 wechselte er an das damalige Zentrum der deutschen wie auch internationalen Mathematik, die Universität Göttingen, wo er bis zu seiner Emeritierung im Jahre 1930 lehrte. Seine Arbeiten umfassen ein riesiges Spektrum aus unter anderem Invariantentheorie, Zahlentheorie, Geometrie, Funktionalanalysis, Logik und Grundlagen der Mathematik sowie auch zur Relativitätstheorie. Er gilt als einer der Väter der modernen Algebra.

Die unerwartete „Lösung“, die YURI MATIYASEVICH 1970 im Alter von 22 Jahren als Doktorarbeit veröffentlichte, besagt, daß es *kein solches Verfahren geben kann.* Er zeigt dies über ein positives Resultat: Jede *rekursiv aufzählbare* Teilmenge M von $\mathbb{N}^n$, $\mathbb{N}_0^n$ und $\mathbb{Z}^n$ ist *diophantisch,* d.h. es gibt eine nichtnegative ganze Zahl m und ein Polynom

$$f \in \mathbb{Z}[a_1, \ldots, a_n, x_1, \ldots, x_m]$$

derart, daß

$$M = \left\{(a_1, \ldots, a_n) \;\middle|\; \exists_{(x_1,\ldots,x_m)} : f(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\right\}.$$

Die a_i und die x_j müssen dabei jeweils in $\mathbb{N}$, $\mathbb{N}_0$ *bzw.* $\mathbb{Z}$ liegen.

YURI VLADIMIROVICH MATIYASEVICH (Юрий Владимирович Матиясевич) wurde 1947 in Sankt Petersburg (damals Leningrad) geboren, ging dort zur Schule und studierte an der dortigen Universität. 1969-1979 arbeitete er am Petersburger Steklov Institut für Mathematik an seiner Dissertation, dem gerade erwähnten Resultat. Seit 1980 leitet er die dortige Arbeitsgruppe für Logik; außerdem hat er einen Lehrstuhl für Algebra und Zahlentheorie an der Sankt Petersburger Universität. http://logic.pdmi.ras.ru/∼yumat/

Eine rekursiv aufzählbare Menge ist eine (in allen interessanten Fällen unendliche) Menge, für die es einen Algorithmus gibt, der nach hinreichend langer Anwendung jedes ihrer Elemente produziert. Sie heißt *rekursiv entscheidbar*, wenn es auch einen entsprechenden Algorithmus für ihre Komplementärmenge gibt; dann läßt sich für jedes Element der Grundgesamtheit in endlich vielen Schritten entscheiden, ob es in der Menge liegt oder aber in der Komplementärmenge.

Beispiel einer rekursiv aufzählbaren Menge ist etwa die Menge aller Primzahlen; sie ist rekursiv aufzählbar, etwa durch den einfachsten (und dümmsten) Algorithmus, der nacheinander alle natürlichen Zahlen n darauf untersucht, ob es unter den Zahlen $1 < m < n$ eine gibt, die m teilt; falls nicht, ist n eine Primzahl. In der Tat zeigten

JAMES J. JONES, DAIHACHIRO SATO, HIDEO WADA, DOUGLAS WIENS: Diophantine repressentations of the set of prime numbers, *Am. Math. Monthly* **83** (1976), 449-464,

daß das Polynom

$$\begin{aligned}
&[wz+h+j+q]^2+[(gk+2g+k+1)(h+j)+h+z]^2+[2n+p+q+z+e]^2\\
&+[16(k+1)^3(k+2)(n+1)^2+1+f^2]^2+[e^3(e+2)(a+1)^2+1+o^2]^2\\
&+[(a^2+1)y^2+1+x^2]^2+[16r^2y^4(a^2+1)+1+u^2]^2\\
&+[((a+u^2(u^2+a))^2+1)(n+4dy)^2+1+(x+cu)^2]^2\\
&+[n+\ell+v+y]^2+[(a^2+1)\ell^2+1+m^2]^2+[ai+k+1+\ell+i]^2\\
&+[p+\ell(a+n+1)+b(2an+2a+n^2+2n+2)+m]^2\\
&+[q+y(a+p+1)+s(2ap+2a+p^2+2p+2)+x]^2\\
&+[z+p\ell(a+p)+t(2ap+p^2+1)+pm]^2
\end{aligned}$$

genau für die $k \in \mathbb{N}_0$, für die $k+2$ prim ist, eine Nullstelle

$$(a,b,c,d,e,f,g,h,i,j,k,\ell,m,n,o,p,q,r,s,t,u,v,w,x,y,z) \in \mathbb{N}_0^{26}$$

hat. Da eine Summe von Quadraten reeller Zahlen x_i genau dann verschwindet, wenn jede einzelne x_i verschwindet, ist das gleichbedeutend damit, daß das System aus den 14 Polynomen in den eckigen Klammern eine entsprechende Lösung hat.

Die Komplementärmenge der Primzahlen, die Menge der zusammengesetzten Zahlen plus der Eins, ist natürlich auch rekursiv aufzählbar: Dazu müssen wir einfach die Menge $(\mathbb{N} \setminus 1) \times (\mathbb{N} \setminus 1)$ irgendwie anordnen und jedes Produkt ab eines Paars (a,b) als zusamengesetzt betrachten. Die Menge der Primzahlen sowie die Menge der zusammengesetzten Zahlen sind damit auch rekursiv entscheidbar.

Die Menge M aller Paare (A,E) bestehend aus einem Algorithmus A und dessen Eingabedaten E derart, daß A mit Eingabe E nach endlich vielen Schritten stoppt, ist ebenfalls rekursiv aufzählbar. Zum Beweis kann man beispielsweise die Paare (A,E) irgendwie anordnen und dann nach Art der Zeitscheibentechnik eines Betriebssystems quasiparallel ausführen in einer solchen Weise, daß jedes Paar (A,E), für das $A(E)$ nach endlich vielen Schritten ein Ergebnis liefert, dieses Ergebnis auch hier nach endlich vielen Schritten liefert. Setzt man nach Ende eines Programms $A(E)$ das Paar (A,E) auf eine Liste endender Programme, so muß offensichtlich jedes solche Paar nach und nach auf dieser Liste erscheinen, die Menge aller dieser Paare ist also rekursiv aufzählbar. Nach TURING können wir die Menge *aller* Paare (A,E) in Bijektion mit $\mathbb{N}$ setzen und so M mit einer Teilmenge von $\mathbb{N}$ identifizieren.

Diese Menge kann nach TURING nicht entscheidbar sein, ist nach MATIYASEVICH aber diophantisch. Somit muß es Familien von diophantischen Gleichungen geben, bei denen nicht entscheidbar ist, für welche Parameterwerte sie lösbar sind.

Um den Satz von RICHARDSON zu beweisen, müssen wir daraus ein Problem mit reellen Zahlen machen. Das ist relativ einfach: Eine reelle Zahl x ist genau dann ganz, wenn $\sin \pi x$ verschwindet. Wenn wir daher von einem Polynom $f \in \mathbb{Z}[x_1,\ldots,x_m]$ nicht entscheiden können, ob

es eine Nullstelle $(x_1, \ldots, x_m) \in \mathbb{N}_0^m$ hat, können wir von der Funktion

$$f\big(|x_1|, \ldots, |x_m|\big)^2 + \sum_{i=1}^{m} \sin^2 \pi x_i$$

nicht entscheiden, ob sie eine reelle Nullstelle hat.

Für Einzelheiten und Folgerungen sei etwa auf das Buch

YURI V. MATIYASEVICH: Hilbert's Tenth Problem, *MIT Press*, 1993

verwiesen. Einen einfachen und kurzen Beweis des Satzes von MATIYASEVICH findet man im (via `www.jstor.org` auch online erhältlichen) Artikel

J. P. JONES, Y. V. MATIJASEVIČ: Proof of Recursive Unsolvability of Hilbert's Tenth Problem, *American Mathematical Monthly* **98** (1991), 689–709

Die wesentliche Folgerung für uns besteht darin, daß wir im Körper der reellen Zahlen nicht wirklich rechnen können. Mit Hilfe der in diesem Kapitel behandelten Techniken können wir allerdings in einem Teilkörper der reellen Zahlen exakt rechnen und auch die gängigen Relationen entscheiden:

Definition: Eine reelle Zahl $z \in \mathbb{R}$ heißt algebraisch, wenn es ein Polynom $f \in \mathbb{Q}[x]$ gibt, so daß $f(z)$ verschwindet; andernfalls heißt z transzendent.

So ist beispielsweise $\sqrt{2}$ als Nullstelle des Polynoms $x^2 - 2$ algebraisch, π dagegen ist nach einem 1882 bewiesenen Resultat von FERDINAND VON LINDEMANN (1852–1939) transzendent.

Eine reelle algebraische Zahl kann eindeutig beschrieben werden durch Angabe eines Polynoms f aus $\mathbb{Q}[x]$ und eines Intervalls $[a, b]$, in dem f nur eine Nullstelle hat. Die Intervallenden wählen wir – um exakt rechnen zu können – als rationale Zahlen. Wir wollen uns überlegen, daß wir mit solchen Paaren $\big(f, [a, b]\big)$ alle Grundrechenarten durchführen können, was gleichzeitig zeigen wird, daß die reellen algebraischen Zahlen einen Körper bilden und daß wir auch Gleichheit sowie Größenbeziehungen entscheiden können.

Dazu seien u und v zwei reelle algebraische Zahlen, gegeben durch die Paare $\big(f, [a, b]\big)$ und $\big(g, [c, d]\big)$.

Beginnen wir mit der Addition: Ist $w = u + v$, so ist $g(w - u) = 0$. Wir führen eine neue Variable z ein und schreiben $g(z - x)$ als Polynom in x mit Koeffizienten aus $\mathbb{Q}[z]$. Natürlich können wir auch $f \in \mathbb{Q}[x]$ als ein solches Polynom auffassen: Die Koeffizienten von f sind rationale Zahlen und damit auch (konstante) Polynome aus $\mathbb{Q}[z]$. Wir haben damit zwei Polynome in x mit Koeffizienten aus $\mathbb{Q}[z]$, die für $z = u + v$ die gemeinsame Nullstelle $x = u$ haben.

Aus Kapitel II, §7, wissen wir, daß zwei Polynome in x über einem faktoriellen Ring R genau dann eine gemeinsame Nullstelle haben, wenn ihre Resultante verschwindet. Diese ist hier ein Polynom $h \in \mathbb{Q}[z]$, das somit für $z = u + v$ verschwinden muß. Damit haben wir ein Polynom h mit rationalen Koeffizienten gefunden, das $w = u + v$ als Nullstelle hat.

Da $a \le u \le b$ und $c \le v \le d$, liegt w natürlich im Intervall $[a + c, b + d]$; es ist allerdings nicht klar, daß h in diesem Intervall nur w als Nullstelle hat. Dies läßt sich aber nach STURM (oder DESCARTES-JACOBI oder BUDAN-FOURIER) überprüfen; gegebenenfalls müssen die Intervalle $[a, b]$ und $[c, d]$ so lange verkleinert werden, bis auch das Intervall $[a + c, b + d]$ hinreichend klein ist.

Damit wissen wir, wie man Summen berechnet; um auch Differenzen berechnen zu können, müssen wir uns nur überlegen, wie man für eine durch $\big(f, [a, b]\big)$ dargestellte reelle algebraische Zahl u ihr Negatives darstellt. Mit

$$f = \sum_{i=0}^{n} a_i x^i \quad \text{ist} \quad h = \sum_{i=0}^{n} (-1)^i a_i x^i$$

offensichtlich ein Polynom, das $-u$ als Nullstelle hat, und $-u$ liegt im Intervall $[-b, -a]$. Es ist dort auch die einzige Nullstelle, denn jede Nullstelle von h ist das Negative einer Nullstelle von f.

Für Produkte können wir fast genauso vorgehen wir für Summen: Ist $w = uv$ und $u \neq 0$, so ist $g(w/u) = 0$. Um aus $g(z/x)$ ein Polynom zu machen, müssen wir mit x^m multiplizieren, wobei m den Grad von g

bezeichnet: Für $g = b_m x^m + \cdots + b_0$ betrachten wir also

$$x^m g(z/x) = b_m z^m + b_{m-1} z^{m-1} x + \cdots + b_1 z x^{m-1} + b_0 x^m ,$$

ein Polynom vom Grad m in x mit Koeffizienten aus $\mathbb{Q}[z]$. Auch f können wir als so ein Polynom auffassen und erhalten wie oben, daß die Resultante dieser beiden Polynome ein rationales Polynom ist, das in w verschwindet. Das Intervall, in dem w liegt, läßt sich leicht aus a, b, c und d berechnen, allerdings sind Fallunterscheidungen bezüglich der Vorzeichen nötig. Auch hier kann es wieder notwendig werden, die Ausgangsintervalle zu verkleinern um sicherzustellen, daß w die einzige Nullstelle im Intervall ist.

Fehlen schließlich noch die Quotienten, und dazu reicht es, wenn wir zu einer gegebenen reellen algebraischen Zahl u ein Polynom und ein Intervall für ihren Kehrwert finden. Ist u eine Nullstelle von f, so ist $1/u$ offensichtlich Nullstelle von

$$x^n f(1/x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n .$$

Beim Intervall $[a, b]$ für u müssen wir zunächst sicherstellen, daß es die Null nicht enthält, daß also a und b dasselbe Vorzeichen haben; dann liegt $1/u$ im Intervall $[1/b, 1/a]$.

Damit lassen sich alle vier Grundrechenarten algorithmisch ausführen, und wir haben auch gezeigt, daß die reellen algebraischen Zahlen einen Körper bilden.

Als Beispiel wollen wir Summe und Produkt von $\sqrt{2}$ und $\sqrt{3}$ auf diese Weise behandeln. $\sqrt{2}$ können wir darstellen durch das Polynom $f = x^2 - 2$ und das Intervall $[0, 2]$, für $\sqrt{3}$ nehmen wir entsprechend $g = x^2 - 3$ und das Intervall $[0, 3]$.

$$g(z - x) = (z - x)^2 - 3 = x^2 - 2zx + z^2 - 3 ;$$

wir müssen also die Resultante

$$\begin{vmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 1 & -2z & z^2 - 3 & 0 \\ 0 & 1 & -2z & z^2 - 3 \end{vmatrix} = z^4 - 10z^2 + 1$$

von f und diesem Polynom berechnen. Das Ergebnis ist, wie kaum anders zu erwarten, das SWINNERTON-DYER-Polynom mit den Nullstellen $\pm 2 \pm 3$, denn schließlich ändert sich nichts an f und g, wenn wir $\sqrt{2}$ und/oder $\sqrt{3}$ durch ihr Negatives ersetzen.

Da die Summe einer Zahl aus $[0, 2]$ und einer aus $[0, 3]$ in $[0, 5]$ liegt, ist $\sqrt{2} + \sqrt{3}$ somit eine Nullstelle des Polynoms $x^4 - 10x^2 + 1$; wir müssen mit dem Satz von STURM überprüfen, ob es die einzige ist.

Da wir alle vier Nullstellen kennen, können wir bei diesem einfachen Beispiel darauf verzichten; wir sehen auch so, daß die Nullstelle $\sqrt{3} - \sqrt{2}$ ebenfalls in diesem Intervall liegt. Daher müssen wir die Ausgangsintervalle verkleinern.

Da $1^2 < 2 < 3 < 2^2$, liegen sowohl $\sqrt{2}$ als auch $\sqrt{3}$ im Intervall $[1, 2]$; ihre Summe liegt daher in $[2, 4]$. In diesem Intervall liegt keine weitere Nullstelle, denn $\sqrt{3} - \sqrt{2} \in [0, 1]$. Somit können wir $\sqrt{2} + \sqrt{3}$ charakterisieren als *die* Nullstelle von $x^4 - 10x^2 + 1$ im Intervall $[2, 4]$.

Für das Produkt $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$ müssen wir, wenn wir strikt nach Schema vorgehen, zunächst das Polynom

$$x^2 g(z/x) = x^2 \left(\frac{z^2}{x^2} - 3 \right) = z^2 - 3x^2$$

berechnen und seine Resultante mit f berechnen:

$$\begin{vmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ -3 & 0 & z^2 & 0 \\ 0 & -3 & 0 & z^2 \end{vmatrix} = (z^2 - 6)^2 .$$

Dieses Polynom hat nur die Nullstellen $\pm\sqrt{6}$, wir können das Produkt von $\sqrt{2}$ und $\sqrt{3}$ also charakterisieren als die Nullstelle von $(z^2 - 6)^2$ in $[0, 6]$. Natürlich reicht auch $z^2 - 6$; die Resultante liefert offensichtlich nicht immer das kleinstmögliche Ergebnis.

Wir müssen uns noch überlegen, daß wir auch entscheiden können, wann zwei Darstellungen $\big(f, [a, b]\big)$ und $\big(g, [c, d]\big)$ die gleiche Zahl darstellen. Wenn der Durchschnitt der beiden Intervalle leer ist, kann

das unmöglich der Fall sein, ebenso wenig, wenn f und g teilerfremd sind, denn dann gibt es keine gemeinsame Nullstelle.

Falls ggT(f, g) positiven Grad hat und $[a, b] \cap [c, d]$ nicht leer ist. können wir zunächst (z.B. nach STURM) überprüfen, ob der ggT im Durchschnitt der beiden Intervalle eine Nullstelle hat. Falls nein, können die Ausgangszahlen nicht gleich sein.

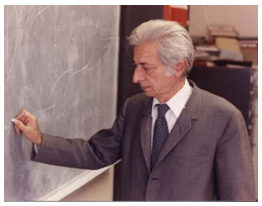
Andernfalls ist diese Nullstelle auch eine Nullstelle von f, und sie liegt insbesondere im Intervall $[a, b]$. Da f dort nur die eine Nullstelle x hat, muß sie also gleich x sein. Genauso folgt, daß sie gleich y sein muß, und das zeigt die Gleichheit von x und y.

Die Relationen $<$ und $>$ lassen sich ebenfalls leicht entscheiden, z.B. durch Verkleinerung der Intervalle oder durch Berechnung der Differenz und Untersuchung auf positive oder negative Nullstellen von deren definierendem Polynom.

Damit haben wir einen Teilkörper von $\mathbb{R}$ gefunden, in dem wir (wenn auch mit relativ großem Aufwand) exakt rechnen und Relationen entscheiden können.

Tatsächlich gilt sogar noch mehr: Nach einem Satz von TARSKI und SEIDENBERG läßt sich für jeden Formel bestehend aus Quantoren, Junktoren, Variablen für reelle algebraische Zahlen und Ordnungsrelationen algorithmisch entscheiden, ob sie wahr ist.

ALFRED TARSKI wurde 1902 im damals russischen Warschau als ALFRED TEITELBAUM geboren. An der Universität Warschau wollte er 1918 zunächst Biologie studieren, wechselte dann aber unter dem Einfluß des Logikers STANISŁAW LEŚNIEWSKI zur Mathematik, wo er bereits 1924 über Probleme der Mengenlehre promovierte. Um 1923 konvertierte er zum Katholizismus und änderte seinen Namen in TARSKI. Ab 1922 lehrte er Logik am Polnischen Pädagogigschen Institut, ab 1925 an der Universität Warschau. Wegen des geringen Gehalts hatte er gleichzeitig noch eine Vollzeitstelle als Mathematiklehrer an einem Gymnasium. Während des deutschen Angriffs auf Polen war er bei einer Konferenz in Harvard; er blieb in USA und bekam nach temporären Stellen in Harvard, New York und Princeton 1942 eine Professur in Berkeley. Dort lehrte er über seine Emeritierung hinaus bis 1973. Bekannt ist er vor allem für seine Arbeiten zur Logik, jedoch behandeln seine zahlreichen Arbeiten auch Themen aus der Algebra, Geometrie und weiteren Gebieten. Er starb 1983 in Berkeley.



ABRAHAM SEIDENBERG wurde 1916 in Washington, D.C. geboren. Er studierte zunächst an der University of Maryland, wo er 1937 seinen Bachelor bekam, dann bei OSKAR ZARISKI (1899–1986) an der Johns Hopkins University, wo er über Bewertungen von Polynomringen in zwei Veränderlichen promovierte. 1945 bekam er eine Stelle als Instructor in Berkeley, aus der schließlich 1958 eine Professur wurde. Er blieb dort bis zu seiner Emeritierung 1987. Die meisten seiner Arbeiten stammen aus dem Gebiet der kommutativen Algebra und algebraischen Geometrie, der Differentialalgebra und der Geschichte der Mathematik. Er starb 1988 während einer Gastvorlesung an der Universität von Milano.

Beweise des Satzes von TARSKI und SEIDENBERG findet man in Lehrbüchern der reell-algebraischen Geometrie, z.B. bei

RICCARDO BENEDETTI, JEAN-JACQUES RISLER: Real algebraic and semi-algebraic sets, *Hermann*, 1990

Ausgangspunkt der dort behandelten sogenannten zylindrischen Zerlegung ist das folgende Lemma, das auch zu einer einfacheren Darstellung reeller algebraischer Zahlen führt:

Lemma von Thom: $\mathcal{F} = \{f_1, \ldots, f_r\}$ sei eine endliche Menge von Polynomen aus $\mathbb{R}[x]$ mit der Eigenschaft, daß mit jedem Polynom f aus $\mathcal{F}$ auch dessen Ableitung in $\mathcal{F}$ liegt. Weiter sei R_i für $i = 1, \ldots, r$ jeweils eine der Relationen $<, =, >$. Dann ist

$$M = \left\{ x \in \mathbb{R} \;\middle|\; f_i(x)\ R_i\ 0 \quad \forall i = 1, \ldots, r \right\}$$

eine zusammenhängende Menge, d.h. $M = \emptyset$, oder M besteht aus genau einem Punkt, oder M ist ein (eventuell unendliches) Intervall.

Beweis durch vollständige Induktion nach r: Für $r = 0$ gibt es keine Bedingungen, d.h. M ist das unendliche „Intervall“ $\mathbb{R}$. Für $r > 0$ können wir durch Umordnen erreichen, daß kein Element aus $\mathcal{F}$ größeren Grad als f_r hat. Dann kommt f_r nicht als Ableitung eines anderen Polynoms aus $\mathcal{F}$ in Frage, so daß auch $\mathcal{F}' = \mathcal{F} \setminus \{f_r\}$ die Voraussetzung des Lemmas erfüllt. Nach Induktionsvoraussetzung ist daher

$$M' = \left\{ x \in \mathbb{R} \;\middle|\; f_i(x)\ R_i\ 0 \quad \forall i = 1, \ldots, r-1 \right\}$$

eine zusammenhängende Menge und $M \subseteq M'$. Falls $M' = \emptyset$ oder M' nur aus einem Element besteht, ist die Behauptung klar. Ist M' ein Intervall, so ist im Falle einer konstanten Funktion f_r alles klar. Andernfalls ist f_r' entweder positiv auf ganz M' oder negativ auf ganz M'. In beiden Fällen ist f_r monoton, womit die Behauptung klar ist. ∎

RENÉ THOM wurde 1923 in Montbéliard geboren. Er studierte an der Ecole Normale Supérieure in Paris bei HENRI CARTAN (1904–2008) und ging mit diesem 1946 an die Universität Straßburg, wo er 1951 über Faserräume promovierte. Dank eines Stipendiums konnte er anschließend durch die USA reisen und mehrere prominente Mathematiker besuchen. 1953 bis 1954 lehrte er in Grenoble, danach bis 1963 in Straßburg. Für seine Arbeiten aus dem Gebiet der Topologie erhielt er 1958 die Fields-Medaille, damals die höchste Auszeichnung in der Mathematik. 1964 ging er ans Institut des Hautes Etudes Scientifique in Bures-sur-Yvette bei Paris; gleichzeitig wechselte er sein Arbeitsgebiet und beschäftigte sich nun mit Singularitäten von differenzierbaren Abbildungen. Außerhalb der Mathematik ist er vor allem bekannt als Schöpfer der aus diesen Studien entstandenen Katastrophentheorie. Er starb 2002 in Bures-sur-Yvette.

Besteht $\mathcal{F}$ nur aus einem Polynom f und dessen sämtlichen Ableitungen, und betrachten wir nur Nullstellen von f, so haben wir Mengen der Form

$$M = \left\{ x \in \mathbb{R} \;\middle|\; f(x) = 0 \text{ und } f^{(i)}(x)\ R_i\ 0 \text{ für } i \geq 1 \right\}.$$

Abgesehen vom uninteressanten Fall, daß f das Nullpolynom ist, haben wir hier eine endliche Menge, denn f hat höchstens endlich viele reelle Nullstellen. Somit enthält M nach dem Lemma von THOM entweder genau ein Element oder ist leer.

Die verschiedenen Nullstellen von f sind daher eindeutig charakterisiert durch die Folgen $\left(\operatorname{sgn} f'(x), \operatorname{sgn} f''(x), \ldots, \operatorname{sgn} f^{(n)}(x)\right)$ der Vorzeichen der Ableitungen. Statt durch ein Polynom und ein Intervall können wir eine reelle algebraische Zahl also auch darstellen durch ein Polynom und eine Folge von Vorzeichen. Algorithmen für das Rechnen mit so dargestellten Zahlen findet man bei

M. COSTE, M.F. TOY: Thom's Lemma, the Coding of Real Algebraic Numbers and the Computation of the Topology of Semi-algebraic Sets, *J. Symbolic Computation* **5** (1988), 121–129.

Als Beispiel können wir uns das Polynom

$$\prod_{i=1}^{10}(x - i)$$

mit den Nullstellen $1, 2, 3, \ldots, 10$ ansehen; die Vorzeichen der Ableitungen bei den einzelnen Nullstellen sind

x	$f'(x)$	$f''(x)$	$f'''(x)$	$f^{(4)}(x)$	$f^{(5)}(x)$	$f^{(6)}(x)$	$f^{(7)}(x)$	$f^{(8)}(x)$	$f^{(9)}(x)$	$f^{(10)}(x)$
1	−	+	−	+	−	+	−	+	−	+
2	+	−	+	+	−	+	−	+	−	+
3	−	+	+	−	+	+	−	+	−	+
4	+	−	−	+	+	−	+	+	−	+
5	−	+	+	−	−	+	+	−	−	+
6	+	+	−	−	+	+	−	−	+	+
7	−	−	+	+	−	−	−	+	+	+
8	+	+	−	−	−	+	+	+	+	+
9	−	−	−	+	+	+	+	+	+	+
10	+	+	+	+	+	+	+	+	+	+

Wie man sieht, sind die Vorzeichenfolgen in der Tat für jede Nullstelle anders.