D 20577
102. Band Heft 1
ausgegeben am 20.4.2000

DMV

Jahresbericht

der Deutschen Mathematiker-Vereinigung

Herausgegeben von A. Krieg
unter Mitwirkung von
U. Gather, E. Heintze, B. Kawohl,
H. Lange, H. Triebel

B. G. Teubner Wiesbaden · Stuttgart · Leipzig 2000

Jahresbericht

der Deutschen Mathematiker-Vereinigung

Der „Jahresbericht" ist das offizielle Veröffentlichungsorgan der Deutschen Mathematiker-Vereinigung, für dessen inhaltliche Gestaltung im Auftrag des Präsidiums der jeweilige Herausgeber zuständig ist. Im „Jahresbericht" sollen vornehmlich Überblicksartikel über Teilgebiete der reinen und angewandten Mathematik, Nachrufe sowie historische Artikel und Buchbesprechungen veröffentlicht werden.

Manuskripte:

Alle für die Schriftleitung des Jahresberichts bestimmten Briefe und Manuskripte sind an Prof. Dr. A. Krieg zu richten. Für Buchbesprechungen ist Prof. Dr. H. Lange zuständig. Bücher, von denen eine Besprechung erfolgen soll, werden bei den Verlagen angefordert. Autoren von Buchbesprechungen und Artikeln werden gebeten, die vorhandenen LATEX-style-files für den Jahresbericht zu verwenden. Somit kann der Aufwand für die Satzarbeiten erheblich reduziert werden. Sollten Illustrationen in die Arbeiten integriert werden, können diese auch in das Satzsystem übernommen werden. Dazu ist es erforderlich, dass die Bilddaten der Abbildungen nochmals in separaten Dateien einzeln abgespeichert werden. Die LATEX-style-files sind neben weiteren Informationen im Internet verfügbar unter

http://www.mathA.rwth-aachen.de/dmv/index.html

Auf Anfrage können die style-files auch auf Diskette zugeschickt werden.
Grundsätzlich sollen nur solche Manuskripte eingereicht werden, die nicht gleichzeitig an anderer Stelle zur Veröffentlichung eingereicht oder bereits veröffentlicht worden sind. Mit der Annahme zur Veröffentlichung erwirbt der Verlag das Verlagsrecht zur Vervielfältigung und Verbreitung sowie das Recht der Übersetzung in andere Sprachen.

Verlag:
GWV Fachverlage
B. G. Teubner GmbH Wiesbaden · Stuttgart · Leipzig
Postfach 1546, 65173 Wiesbaden
Abraham-Lincoln-Str. 46, 65189 Wiesbaden
http://www.teubner.de
http://www.gwv-fachverlag.de

Geschäftsführer: Dr. Hans-Dieter Haenel
Verlagsleitung: Dr. Heinz Weinheimer
Gesamtleitung Anzeigen: Thomas Werner
Gesamtleitung Produktion: Reinhard van den Hövel
Gesamtleitung Vertrieb: Heinz Detering

Abo-/Leserservice:
Tatjana Hellwig
Telefon: (0611) 7878-151
Fax: (0611) 7878-423
E-Mail: tatjana.hellwig@bertelsmann.de

Marketing/Sonderdrucke:
Stefanie Hoffmann
Telefon: (0611) 7878-379
Fax: (0611) 7878-439
E-Mail: stefanie.hoffmann@bertelsmann.de

Abonnentenverwaltung:
(Änderung von Adressen und Bankverbindung, Rückfragen zu Rechnungen oder Mahnung) VVA-Zeitschriftenservice, Abt. D6F6/Jahresbericht der Deutschen Mathematiker-Vereinigung,
Postfach 777, 33310 Gütersloh
Ursula Müller
Telefon: (05241) 80-801965
Fax: (05241) 80-9620
E-Mail: ursula.mueller@bertelsmann.de

Bezugsbedingungen:
Die Zeitschrift erscheint 4 mal jährlich zum Jahresabonnementspreis von DM 178 (1299 öS; 158 sFr) inkl. Versandkosten. Der Bezug von Einzelheften ist nicht möglich. Schriftliche Kündigung des Abonnements spätestens sechs Wochen vor Ablauf des Bezugsjahres.
Für persönliche Mitglieder der DMV, die den Jahresbericht zu beziehen wünschen, ist der zwischen DMV und Verlag vereinbarte Bezugspreis maßgebend, der im Rahmen des Mitgliedsbeitrags erhoben wird.

Satz: Fotosatz Behrens, D-68723 Oftersheim
Druck: pagina media gmbh, D-69502 Hemsbach

ISSN 0012-0456

Jahresbericht

der Deutschen Mathematiker-Vereinigung

Inhalt Band 102, Heft 1

1. Abteilung

2. Abteilung

In den nächsten Heften erscheinende Arbeiten:

M. Aigner: Die Ideen von Penrose zum 4-Farbenproblem
M. Aschbacher: The classification of finite simple groups
R. Thiele: Felix Klein in Leipzig

Anschriften der Herausgeber

Prof. Dr. Aloys Krieg, Lehrstuhl A für Mathematik, RWTH Aachen,
Templergraben 55, 52056 Aachen
E-mail: krieg@mathA.rwth-aachen.de

Prof. Dr. Ursula Gather, Fachbereich Statistik, Universität Dortmund,
Vogelpothsweg 87, 44221 Dortmund
E-mail: gather@omega.statistik.uni-dortmund.de

Prof. Dr. Ernst Heintze, Institut für Mathematik, Universität Augsburg,
86135 Augsburg
E-mail: heintze@math.uni-augsburg.de

Prof. Dr. Bernhard Kawohl, Mathematisches Institut, Universität zu Köln, 50923 Köln
E-mail: kawohl@mi.uni-koeln.de

Prof. Dr. Herbert Lange, Mathematisches Institut, Friedrich-Alexander-Universität
Erlangen-Nürnberg, Bismarckstraße 1½, 91054 Erlangen
E-mail: lange@mi.uni-erlangen.de

Prof. Dr. Hans Triebel, Mathematisches Institut, Friedrich-Schiller-Universität,
Ernst-Abbe-Platz 1–4, 07740 Jena
E-mail: triebel@minet.uni-jena.de

Bezugshinweis

Früher erschienene Bände (ab Band 68) des „Jahresberichts der Deutschen Mathematiker-Vereinigung" können durch den Buchhandel oder den Verlag bezogen werden.

Nachdruck der Bände 41 bis 67 liefert: Swets & Zeitlinger, Heereweg 347b, POB 810,
NL-2160 SZ Lisse/Holland

Jber. d. Dt. Math.-Verein. 102 (2000) 1–14
Mathematics Subject Classification: 11Y05, 11Y11, 11A51, 11Y16
Keywords: factorization, algorithms, prime numbers

Faktorisieren ganzer Zahlen

G. Nebe, Aachen

1 Einleitung

Dieser allgemein gehaltene Übersichtsartikel entstand aus meinem Habilitationsvortrag an der RWTH Aachen. Er soll die modernen Faktorisierungsverfahren kurz darstellen. Die meisten schönen Ideen findet man schon in den klassischen Algorithmen, die dazu entwickelt wurden, Zahlen mit Bleistift und Papier zu faktorisieren. Viele aktuelle, für den Computer entwickelte Faktorisierungsalgorithmen bauen auf diesen Ideen auf.

Schon Euklid wußte, daß sich jede natürliche Zahl als Produkt von Primzahlen darstellen läßt. Diese *vollständige Faktorisierung* ist bis auf die Reihenfolge der Faktoren eindeutig. Streng bewiesen wurde dieser *Fundamentalsatz der Arithmetik* erst von Gauß [6], der das Problem der Berechnung der Faktorisierung als eines der Hauptprobleme der Arithmetik bezeichnet hat. Gauß sah, daß das Faktorisieren sich in 2 Schritte gliedert:

(1) Man teste, ob die zu faktorisierende Zahl zusammengesetzt ist.
(2) Je nach dem Ergebnis von (1) faktorisiere man die zusammengesetzte Zahl oder beweise, daß sie eine Primzahl ist.

Zum ersten Schritt gibt es sehr schnelle Methoden (siehe Abschnitt 2.1) die als Resultat entweder „ist zusammengesetzt" oder „ist sehr wahrscheinlich eine Primzahl" liefern. Für viele Anwendungen genügt es, die Primzahleigenschaft mit hoher Wahrscheinlichkeit zu wissen. Aber auch für rigorose Primzahlbeweise gibt es recht gute Algorithmen (Abschnitt 2.2). Während es beim Faktorisieren genügt, einen nichttrivialen Teiler zu raten, ist hier ein echter Beweis gefragt.

Weiß man nach (1), daß die Zahl N zusammengesetzt ist, so will man in der Regel eine *Faktorisierung* oder *Zerlegung* von N finden, also

$$N = a \cdot b$$

als Produkt zweier ganzer Zahlen $a, b \neq \pm 1$ schreiben. a und b sind meist einfacher zu faktorisieren als N und rekursiv erhält man eine vollständige Faktorisierung von N. Auch das Faktorisieren selbst geschieht in mehreren Etappen. Die Wahl des Verfahrens hängt stark von den Natur der Zahl N ab. Zum Abspalten kleiner Teiler von N werden die Methoden aus Abschnitt 3 angewandt. Für einige Algorithmen ist es auch von Vorteil, wenn man N als Wert eines „kleinen" Polynoms schreiben kann.

In diesem Artikel kann nicht auf alle bekannten Methoden eingegangen werden und die Algorithmen werden oft nur in einer Rohform vorgestellt, die das Erkennen des groben Ablaufs erleichtert. Für detailliertere Beschreibungen aller wichtigen Faktorisierungsalgorithmen und weitere Literaturangaben sei auf die Lehrbücher [4], [14], [15] und [16] sowie die Übersichtsartikel [3], [5] und [9] verwiesen. Ich bedanke mich bei C. Pomerance, der mir relevante Kapitel des Buches [14] vor Drucklegung zur Verfügung gestellt hat.

2 Primzahltests

2.1 Zusammengesetzheits-Tests

Der *kleine Satz von Fermat* sagt aus, daß für jede Primzahl p und jede zu p teilerfremde Zahl a die Kongruenz

$$a^{p-1} \equiv 1 \pmod{p}$$

erfüllt ist. Algebraisch formuliert heißt das, daß der Exponent der multiplikativen Gruppe $(\mathbf{Z}/p\mathbf{Z})^*$ ein Teiler von $p-1$ ist. Einige zusammengesetzte Zahlen N, die sogenannten *Carmichael-Zahlen*, haben auch die Eigenschaft, daß die Ordnung eines jeden Elements von $(\mathbf{Z}/N\mathbf{Z})^*$ ein Teiler von $N-1$ ist. Die kleinste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$. Es gilt jedoch, daß eine ungerade Zahl N eine Primzahl ist, wenn für alle teilerfremden Zahlen a die Kongruenz

$$\text{(JK)} \quad a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{N}$$

gilt, wobei $\left(\frac{\cdot}{N}\right) = \prod_{i=1}^{s} \left(\frac{\cdot}{p_i}\right)^{a_i} : (\mathbf{Z}/N\mathbf{Z})^* \to \{\pm 1\}$ für $N = \prod_{i=1}^{s} p_i^{a_i}$ das Jacobi-Kronecker-Symbol ist. Ist p eine Primzahl und a nicht durch p teilbar, so ist $\left(\frac{a}{p}\right) = 1$, falls a ein Quadrat modulo p ist und -1 sonst. Das Jacobi-Kronecker-Symbol läßt sich mit Hilfe des quadratischen Reziprozitätsgesetzes leicht ausrechnen (siehe [16, Appendix 3]). Ist N zusammengesetzt, so erfüllen mindestens die Hälfte aller Zahlen $a \in \{1, \ldots, N-1\}$ nicht die Kongruenz (JK). Erfüllt N also die Kongruenz (JK) für 50 zufällig ausgewählte Zahlen a, so ist die Wahrscheinlichkeit, daß N zusammengesetzt ist, ungefähr $2^{-50} < 10^{-15}$ und damit im allgemeinen kleiner als die Wahrscheinlichkeit eines Hardware-Fehlers.

Einen schnelleren Test, den sogenannten *Rabin-Miller-Test*, der auch die Berechnung der Jacobi-Kronecker-Symbole vermeidet, liefert das folgende Kriterium: Sei N ungerade und $N-1 = d2^s$ mit ungeradem d. Dann ist N eine Primzahl, falls für alle zu N teilerfremden Zahlen a entweder $a^d \equiv 1 \pmod{N}$ gilt oder $a^{d \cdot 2^r} \equiv -1 \pmod{N}$ für ein $r = 0, 1, \ldots, s-1$. Ist N zusammengesetzt, so wird diese Bedingung nur von höchstens einem Viertel der Zahlen $a \in \{1, \ldots, N-1\}$ erfüllt.

2.2 Primzahlbeweise

Um zu beweisen, daß N eine Primzahl ist, kann man dieselbe Idee wie im vorangegangenen Abschnitt benutzen: Ist $N = p_1^{a_1} \ldots p_s^{a_s}$ für paarweise verschiedene Primzahlen p_i, so ist nach dem chinesischen Restsatz der Ring $\mathbf{Z}/N\mathbf{Z}$ isomorph

zu $\oplus_{i=1}^{s} \mathbf{Z}/p_i^{a_i}\mathbf{Z}$ und damit ist auch die Einheitengruppe $(\mathbf{Z}/N\mathbf{Z})^*$ das direkte Produkt der Gruppen $(\mathbf{Z}/p_i^{a_i}\mathbf{Z})^*$. Insbesondere ist der Exponent von $(\mathbf{Z}/N\mathbf{Z})^*$ genau dann durch $N-1$ teilbar, wenn N eine Primzahl ist. Kann man also $N-1$ primfaktorisieren, so bietet sich folgender schneller Primzahltest an:

(1) Sei $N-1 = q_1^{b_1} \ldots q_r^{b_r}$ mit verschiedenen Primzahlen q_j.

(2) Gibt es für alle $j = 1, \ldots, r$ Zahlen $c_j \in \{2, \ldots, N-1\}$, für welche $c_j^{(N-1)/q_j} \not\equiv 1 \pmod{N}$ und $c_j^{N-1} \equiv 1 \pmod{N}$ ist, so ist die Ordnung von $c_j \in (\mathbf{Z}/N\mathbf{Z})^*$ durch $q_j^{b_j}$ teilbar. Deshalb teilt $N-1$ den Exponenten von $(\mathbf{Z}/N\mathbf{Z})^*$ und N ist eine Primzahl.

Dieser Test setzt eine (fast) vollständige Faktorisierung von $N-1$ voraus, wie sie leider nicht für alle Primzahlkandidaten N erreicht werden kann. Eine berühmte Folge von Zahlen, für die man $N-1$ leicht faktorisieren kann, sind die *Fermat-Zahlen* $F_n := 2^{2^n} + 1$, für die Fermat vermutet hat, sie seien Primzahlen. Es gilt, daß $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65537$ Primzahlen sind, doch schon 1732 fand Euler den Teiler 641 von F_5. Man kennt bis heute keine weitere Fermat-Primzahl. Das kleinste n, für das man nicht weiß, ob F_n zusammengesetzt ist, ist $n = 31$ (Internetseite [FERMAT]).

Die größten bekannten Primzahlen sind jedoch *Mersenne-Primzahlen* $M_p := 2^p - 1$. Da jeder Teiler d von p den Teiler $X^d - 1$ von $X^p - 1$ in $\mathbf{Z}[X]$ liefert, kann M_p nur für Primzahlen p eine Primzahl sein. Man kennt die ersten 37 Zahlen p, für die M_p eine Primzahl ist - die 37te Mersenne-Primzahl ist $2^{3021377} - 1$. Erst kürzlich wurde die noch größere Mersenne-Primzahl $M_{6972593}$, die mehr als 2 Millionen Dezimalstellen hat, entdeckt, wobei allerdings nicht bekannt ist, ob es dazwischen noch weitere Mersenne-Primzahlen gibt (Internetseite [PRIME]). Die Mersenne-Zahlen haben die Eigenschaft, daß man eine Faktorisierung von $M_p + 1$ (jedoch i. a. nicht von $M_p - 1$) kennt. Um die Faktorisierung von $N+1$ zum Beweis der Primzahleigenschaft auszunutzen, sucht man wieder eine abelsche Gruppe, in der man leicht rechnen kann, und deren Exponent genau dann $N+1$ ist, wenn N eine Primzahl ist. Dazu betrachtet man eine quadratische Erweiterung Q von $\mathbf{Z}/N\mathbf{Z}$ und potenziert in der Faktorgruppe $Q^*/(\mathbf{Z}/N\mathbf{Z})^*$ ([16, S. 107 ff]).

Indem man elliptische Kurven modulo N betrachtet, kann man viele weitere abelsche Gruppen ganz unterschiedlicher Ordnung benutzen, um zu beweisen, daß N prim ist. Dazu sei N teilerfremd zu 6. Man wähle $A, B \in \mathbf{Z}/N\mathbf{Z}$, so daß $4A^3 + 27B^2$ teilerfremd zu N ist. Da man annimmt, daß N prim ist, wird mit N wie mit einer Primzahl gerechnet. Dann ist

$$E_N = E_N(A,B) = \{[x,y,z] \in \mathbf{P}^2(\mathbf{Z}/N\mathbf{Z}) \mid y^2 z \equiv x^3 + Axz^2 + Bz^3 \pmod{N}\}$$

eine Gruppe. Das Einselement ist $[0,1,0]$. Nach einem Satz von Hasse ist

$$(\sqrt{N} - 1)^2 < |E_N| < (\sqrt{N} + 1)^2$$

(falls N eine Primzahl ist). Beim *Goldwasser-Kilian-Test* sucht man in E_N ein Element $P = [x,y,z]$ mit $\mathrm{ggT}(z,N) = 1$, welches $P^q = 1 = [0,1,0]$ für eine Primzahl $q > (N^{1/4} + 1)^2$ erfüllt. Existiert solch ein Element, dann ist N eine Primzahl: Denn sonst hat N einen Primteiler $p \leq \sqrt{N}$. In der Reduktion E_p von E_N modulo p hat das Element P immer noch Ordnung q. Damit ist $|E_p| \geq q > (\sqrt{p} + 1)^2$, was dem

Satz von Hasse widerspricht. Eine Schwierigkeit bei diesem Test ist es, die Primzahl q zu finden. Deshalb betrachtet man nicht beliebige elliptische Kurven E_N, sondern nur solche mit komplexer Multiplikation. Für diese läßt sich nämlich die Gruppenordnung $|E_N|$ leicht berechnen und man hofft, einen geeigneten Primteiler q von $|E_N|$ zu finden. Die Primzahleigenschaft der meist sehr viel kleineren Zahl q kann man wieder mit geeigneten elliptischen Kurven beweisen. Man erhält so ein *Primzahlzertifikat*, in dem die verwendeten Daten $(N, E_N, |E_N|, q, P)$, $(q, E_q, |E_q|, \ldots)$, ... angegeben werden, mit dem sich die wesentlichen Schritte des Primzahlbeweises leicht überprüfen lassen.

3 Finden kleiner und spezieller Teiler

3.1 Trial Division

Den *Trial Division* Algorithmus hat wohl jeder schon einmal angewandt, um durch Kopfrechnen kleine Primfaktoren einer Zahl N zu finden. Die Grundidee ist es, N sukzessive durch die Primzahlen $2, 3, 5, 7, 11, \ldots$ zu teilen.

Dabei kann man alle Primzahlen, die kleiner als eine feste Schranke S sind, zum Beispiel mit dem *Sieb des Eratosthenes* bestimmen. Dazu schreibt man die Zahlen $2, \ldots, S$ in eine Liste. Das erste Element der Liste ist eine Primzahl und wird zur Primzahlliste hinzugefügt. Streicht man alle Vielfachen dieser Primzahl (einschließlich der Zahl selber) aus der Liste, so ist wieder das erste Element eine Primzahl, etc.

Anstelle der Primzahlen kann man auch eine leichter zu berechnende Folge von Zahlen benutzen, die die Primzahlen als Teilfolge besitzt, also z. B. die Folge $2, 3, 6k \pm 1$, mit $k \in \mathbf{N}$.

Ein Problem bei der Trial Division ist es, daß man die i. a. recht große Zahl N häufig vergeblich durch kleine Primzahlen zu teilen versucht. Dieses kann man abkürzen, indem man vorher Produkte von Primzahlen, also z. B.

$$P_i := \prod_{\substack{(i-1)\cdot 100 < p < i\cdot 100 \\ p \text{ prim}}} p$$

berechnet und für jedes P_i, den größten gemeinsamen Teiler $\mathrm{ggT}(N, P_i)$ von N und P_i mit dem Euklidischen Algorithmus bestimmt.

Der *Euklidische Algorithmus* wird in vielen Faktorisierungsmethoden als Hilfsmittel benutzt. Er ergibt sich aus der Beobachtung, daß für $N = qP + r$ mit $N, P, r, q \in \mathbf{Z}$ die Beziehung $\mathrm{ggT}(N, P) = \mathrm{ggT}(P, r)$ gilt.

3.2 Der Pollard-ρ-Algorithmus

Der *Pollard-ρ-Algorithmus* hat seinen Namen zum einen von seinem Entdecker, J. Pollard [12], zum anderen von seinem Verhalten: Sei $f \in \mathbf{Z}[X]$ ein Polynom mit ganzen Koeffizienten (z. B. $f(X) = X^2 + 1$) und $x_0 \in \{0, \ldots, N-1\}$. Die Folge $x_n := f(x_{n-1}) \pmod N$ wird nach einer Vorperiode (dem Aufstrich des Buchstabens ρ) schließlich periodisch, was durch den Kreis im ρ veranschaulicht werden kann. Ist f zufällig gewählt, so erwartet man, daß sowohl die Länge des Aufstrichs als auch der Umfang des Kreises in etwa $\sqrt{N}$ betragen. Ist p ein Teiler

von N, so wird die Folge $x_n \pmod p$ i. a. sehr viel eher periodisch mit einer wesentlich kürzeren Periode, sagen wir der Länge k, d.h. der $\mathrm{ggT}(x_n - x_{n+k}, N)$ ist mit großer Wahrscheinlichkeit ein nichttrivialer Teiler von N. Da man weder die Vorperiode noch die Periode der Folge $x_n \pmod p$ kennt und nicht jedes Paar $(n, n+k)$ betrachten möchte, berechnet man zwei Folgen x_n und $y_n := x_{2n}$ parallel und testet in jedem Schritt, ob der $\mathrm{ggT}(x_n - y_n, N)$ ein nichttrivialer Teiler von N ist. Auch hier kann man einige ggT-Berechnungen sparen, indem man direkt das Produkt über mehrere $x_n - y_n$ betrachtet. Es ist erstaunlich, wie schnell man mit diesem Algorithmus, den man sehr leicht z. B. mit MAPLE programmieren kann, kleine Primteiler von N findet.

Pollard-ρ-Algorithmus

(0) Wähle ein Polynom $f(X) \in \mathbf{Z}[X]$.
(1) Wähle $x = y$ zufällig in $\{0, \ldots, N-1\}$.
(2) Setze $x := f(x) \pmod N$, $y := f(y) \pmod N$, $y := f(y) \pmod N$.
(3) Berechne $d := \mathrm{ggT}(x - y, N)$.
Ist $d = N$, so wiederhole das Verfahren mit einen neuen Startwert in (1).
Sonst setze $N := N/d$ und fahre bei (2) fort.

3.3 Der Pollard-$(p-1)$-Algorithmus

Der *Pollard-$(p-1)$-Algorithmus* ist ein Algorithmus, der Primfaktoren von N findet, für die $p-1$ eine glatte Zahl ist. Sei $S \in \mathbf{N}$ fest. Dann nennt man eine Zahl *S-glatt*, wenn all ihre Primteiler $\leq S$ sind und *S-potenzglatt*, wenn alle Primzahlpotenzen, die die Zahl teilen, $\leq S$ sind. Sei V das kleinste gemeinsame Vielfache der Zahlen $\{1, \ldots, S\}$. Hat N einen Primteiler p, für den $p-1$ eine S-potenzglatte Zahl ist, so ist nach dem kleinen Satz von Fermat p ein Teiler von $\mathrm{ggT}(a^V - 1, N)$ für alle zu N teilerfremden Zahlen a.

Pollard-$(p-1)$-Algorithmus

(0) Wähle Schranken $S < S'$. Bestimme die Primzahlen $p_1 < \ldots < p_r \leq S$ z. B. mit dem Sieb des Eratosthenes und für jede dieser Primzahlen das maximale $e_i \in \mathbf{N}$ mit $p_i^{e_i} \leq S$.
(1) Wähle $a \in \{2, \ldots, N-2\}$, z. B. $a = 2$.
(2) Für $i = 1, \ldots, r$ berechne $a := a^{(p_i^{e_i})} \pmod N$.
(3) Bestimme $d = \mathrm{ggT}(a - 1, N)$.
(4) Ist $d = 1$, so bestimme die Primzahlen $p_{r+1} < \ldots < p_s$ in $(S, S']$ und speichere die Differenzen $d_i := p_i - p_{i-1}$ $(i = r+1, \ldots, s)$ ab. Sei $b := a$. Für $i = r+1, \ldots, s$ setze $a := ab^{d_i}$. Bestimme $d = \mathrm{ggT}(a - 1, N)$.

In der Praxis ist es sinnvoll, während der Berechnung von a^V in Schritt (2) gelegentlich den $\mathrm{ggT}(a-1, N)$ (Schritt (3)) zu bestimmen. Schritte (1) – (3) finden das Produkt der Primteiler p von N, für die $p-1$ eine S-potenzglatte Zahl ist. Ist $p - 1 = qn$ für eine Primzahl $S < q \leq S'$ und eine S-potenzglatte Zahl n, so wird p durch den zusätzlichen Schritt (4) gefunden.

Wie schon bei den Primzahltests kann man den $(p-1)$-Algorithmus auch auf $(p+1)$ [21] ausdehnen. Mit Hilfe von elliptischen Kurven erhält man jedoch Gruppen beliebiger Ordnung zwischen $(\sqrt{p}-1)^2$ und $(\sqrt{p}+1)^2$:

3.4 Die Elliptische-Kurven-Methode

Die *Elliptische-Kurven-Methode* [7] ist eines der drei wichtigsten Arbeitspferde zum Faktorisieren großer Zahlen. Sie stellt den einzigen modernen Faktorisierungsalgorithmus dar, dessen Laufzeit wesentlich von der Größe des zweitgrößten Primteilers von N abhängt. Mit ihr können deshalb sehr viel größere Zahlen faktorisiert werden als mit den beiden anderen wichtigen Verfahren, dem Quadratischen Sieb (Abschnitt 4.3) und dem Zahlkörpersieb (Abschnitt 4.4), sofern ihre Primteiler relativ klein sind. Wie schon beim Primzahltest rechnet man in elliptischen Kurven E_N modulo N. Da N zusammengesetzt ist, bildet die Menge E_N keine Gruppe mehr: Kann man eine Gruppenoperation nicht ausführen, so hat man einen nichttrivialen Teiler von N gefunden. Daraus ergibt sich der folgende Algorithmus, der analog zum Pollard $(p-1)$-Algorithmus abläuft:

Elliptische-Kurven-Methode

(0) Wähle Schranken $S < S'$. Bestimme die Primzahlen $p_1 < \ldots < p_r \leq S$ und für jede dieser Primzahlen das maximale $e_i \in \mathbf{N}$ mit $p_i^{e_i} \leq S$.
(1) Wähle zufällige $x, y, A \in \{0, \ldots, N-1\}$.
Setze $B := (y^2 - x^3 - Ax) \pmod N$.
Ist $d := \mathrm{ggT}(4A^3 + 27B^2, N)$ ein nichttrivialer Teiler von N, so gib d aus.
Ist $d = N$, so wähle neue x, y, A.
Setze $P := [x, y, 1] \in E_N := E_N(A, B)$.
(2) Rechne in der elliptischen Kurve E_N:
Für $i = 1, \ldots, r$ berechne $P := P^{(p_i^{e_i})} = [p_i^{e_i}]P \in E_N$, und brich ab, falls während der Berechnung ein nichttrivialer Teiler d von N gefunden wird.
(3) Bestimme die Primzahlen $p_{r+1} < \ldots < p_s$ in $(S, S']$ und speichere die Differenzen $d_i := p_i - p_{i-1}$ $(i = r+1, \ldots, s)$ ab.
Sei $Q := P$. Für $i = r+1, \ldots, s$ berechne $P := PQ^{d_i} = P + [d_i]Q \in E_N$, und brich ab, falls während der Berechnung ein nichttrivialer Teiler d von N gefunden wird.
(4) Wähle die nächste Kurve in Schritt (1).

Ein offensichtlicher Vorteil gegenüber dem Pollard-$(p-1)$-Algorithmus ist, daß in Gruppen ganz unterschiedlicher Ordnung in $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$ gerechnet wird, so daß mit großer Wahrscheinlichkeit eine der Gruppenordnungen S-glatt ist. Der größte Faktor, der mit der Elliptische-Kurven-Methode gefunden wurde, hat 49 Stellen und ist ein Teiler von $6^{250} - 1$ (siehe Internetseite [ECM]).

4 Faktorisieren beliebiger Zahlen

Hat man mit den Algorithmen aus Abschnitt 3 alle kleinen Primteiler von N abgespalten, und ist N immer noch zusammengesetzt, so muß nun schweres Geschütz aufgefahren werden. Es wird dabei angenommen, daß N keine kleinen Teiler mehr hat, also insbesondere ungerade ist. Ist N eine nichttriviale Potenz, etwa $N = n^k$ mit $k > 1$, so läßt sich der nichttriviale Teiler $n \in \mathbf{N}$ von N durch näherungsweises Wurzelziehen bestimmen. Hat N keine Primteiler $\leq N^{1/K}$, so muß man für k nur die Zahlen $2, \ldots, K-1$ überprüfen. Also ist N keine Potenz.

4.1 Fermat

Ist $N = a \cdot b$ eine zusammengesetzte ungerade Zahl, so sind auch a und b ungerade, und $x := \frac{a+b}{2}$ und $y := \frac{a-b}{2}$ sind ganze Zahlen. Also ist

$$N = (x+y) \cdot (x-y) = x^2 - y^2$$

die Differenz zweier Quadrate. Da $y^2 \geq 0$ ist, ist also $x \geq \lceil \sqrt{N} \rceil$. Daraus ergibt sich der folgende Faktorisierungsalgorithmus:

(1) Setze $x := \lceil \sqrt{N} \rceil$ und $z := x^2 - N$.
(2) Ist $z = y^2$ ein Quadrat, so gib die Faktorisierung $N = (x-y) \cdot (x+y)$ aus. Sonst setze $x := x+1$ und $z := z + 2x + 1$ und wiederhole (2).

Aus diesem Fermatschen Faktorisierungsalgorithmus entstand die grundlegende Idee für die meisten modernen Faktorisierungsmethoden. Gauß und Legendre beobachteten nämlich, daß es genügt, ein Vielfaches von N als Differenz von zwei Quadraten zu schreiben

$$x^2 - y^2 = (x+y) \cdot (x-y) = kN$$

für ein $k \in \mathbf{N}$. In dem Ring $\mathbf{Z}/N\mathbf{Z}$ der Restklassen modulo N sind dann y und $\pm x$ Wurzeln von x^2. Hat N genau d verschiedene Primteiler, so gibt es in $\mathbf{Z}/N\mathbf{Z}$ genau 2^d verschiedene Wurzeln von x^2. Also ist die Chance, daß $y \not\equiv \pm x \pmod{N}$ und damit der größte gemeinsame Teiler $\mathrm{ggT}(x-y, N)$ ein nichttrivialer Teiler von N ist, gleich $(2^d - 2)/2^d$, insbesondere $\geq 1/2$ für $d \geq 2$, vorausgesetzt, x ist „unabhängig" von y.

Die Algorithmen, die in den nächsten 3 Abschnitten beschrieben werden, streben eine solche Lösung von $x^2 \equiv y^2 (\mathrm{mod}\ N)$ mit $y \not\equiv \pm x \pmod{N}$ an. Das Grundprinzip ist bei allen Algorithmen gleich: Man bestimmt genügend viele quadratische Reste modulo N, also ganze Zahlen z_i, so daß $z_i \equiv x_i^2 \pmod{N}$ für ein $x_i \in \mathbf{N}$ $(i = 1, \ldots, m)$ ist, in der Hoffnung, daß das Produkt einiger der Zahlen z_i ein Quadrat einer natürlichen Zahl ist,

$$\prod_{i \in I} z_i = y^2$$

für eine Teilmenge $I \subseteq \{1, \ldots, m\}$ und ein $y \in \mathbf{N}$. Setzt man $x := \prod_{i \in I} x_i$, so ist $x^2 - y^2$ durch N teilbar. Die Schwierigkeit ist nur, geeignete Zahlen z_i zu finden, so daß ein Teilprodukt über sie ein Quadrat ist. Dazu sucht man glatte Zahlen, also Zahlen z_i, deren sämtliche Primteiler kleiner als eine fest vorgegebene Schranke S sind, deren optimale Wahl von der Größe von N und von dem verwendeten Algorithmus abhängt. Sind $\{p_1, \ldots, p_r\}$ die Primzahlen $\leq S$, so kann man die S-glatten Zahlen als

$$z_i = (-1)^{e_{i0}} \prod_{j=1}^{r} p_j^{e_{ij}}$$

schreiben. Man erhält so eine Matrix $E = (e_{ij} \pmod 2) \in \mathbf{F}_2^{m \times (r+1)}$. Jede Linearkombination des Nullvektors aus den Zeilen von E liefert eine Menge I mit $\sum_{i \in I} e_{ij} \equiv 0 \pmod 2$ für alle $j = 0, \ldots, r$, also ein Quadrat $y^2 = \prod_{i \in I} z_i$.

Eine Beschleunigung des Verfahrens kann man mit der Strategie der „Large-Prime Variations" erzielen. Dazu betrachtet man nicht nur die S-glatten Zahlen z_i, sondern auch *S-semiglatte Zahlen*, also solche von der Form $z_i = q_i d_i$ für eine S-glatte Zahl d_i und $S < q_i \leq S^2$, so daß q_i keine Primteiler $\leq S$ hat; denn dann ist q_i notwendigerweise eine Primzahl. Die Matrix E erhält dabei keine zusätzlichen Spalten, sondern man merkt sich die jeweiligen Werte q_i. Ist $\prod_{i\in I} z_i$ ein Quadrat, so kommt jedes q_i mit einer geraden Vielfachheit vor. Man merkt sich also die erste zu q_i gehörende Zeile, addiert sie zu allen anderen Zeilen mit demselben $q_j = q_i$, multipliziert die zugehörigen z_j mit dem entsprechenden z_i und streicht dann die zu z_i gehörende Zeile aus E.

4.2 Der Kettenbruchalgorithmus

Gehen wir noch einmal zurück zum Fermatschen Faktorisierungsalgorithmus: Ist in Schritt (2) $z = x^2 - N$ kein Quadrat, so liefert dies eine Einschränkung für die möglichen Primteiler von N: Dann ist nämlich $z \equiv x^2 \pmod N$. Also ist auch $z \equiv x^2 \pmod p$ für jeden Primteiler p von N, d. h. z ist ein Quadrat modulo p. Mit Hilfe des quadratischen Reziprozitätsgesetzes erhält man Kongruenzen (modulo $4z$) für p und schließt so etwa die Hälfte der Primzahlen als Teiler von N aus. Um solche a priori Eigenschaften der Primteiler von N zu erhalten, suchten schon Legendre und Gauß nach kleinen quadratischen Resten modulo N. Dazu benutzten sie die Kettenbruchentwicklung von $\sqrt{kN}$ für kleine natürliche Zahlen k. Ist nämlich $z = x^2 - kN$ klein, so ist x eine gute Approximation von $\sqrt{kN}$. Bei der Kettenbruchentwicklung von $\sqrt{N}$ schreibt man

$$\sqrt{N} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots}}}$$

mit $c_i \in \mathbf{Z}_{\geq 0}$. Dazu setzt man $u_0 := \sqrt{N}$, $c_i := \lfloor u_i \rfloor$, $u_{i+1} = \frac{1}{u_i - c_i}$ $(i = 0, 1, \ldots)$. Man kann nachrechnen, daß $u_i = c_i + \frac{\sqrt{N} - P_{i+1}}{Q_i}$, wobei $(-1)^i Q_i = A_i^2 - B_i^2 N$ ein Quadrat modulo N ist und $2\sqrt{N} > Q_i > 0$ gilt ([16, Appendix 8]). Insbesondere sind die $(-1)^i Q_i$ kleine quadratische Reste modulo N.

Kleine Zahlen sind mit größerer Wahrscheinlichkeit glatt als große. Daher nutzten Morrison und Brillhart [10] die Kettenbruchentwicklung zur Bestimmung genügend vieler glatter quadratischer Reste $z_i = (-1)^i Q_i$ modulo N:

Kettenbruchalgorithmus.

(0) Bestimme eine geeignete Schranke S und eine kleine natürliche Zahl k. Setze $j := 1$.

(1) Bestimme die Kettenbruchentwicklung von $\sqrt{kN}$.

(2) Teste jedesmal, ob Q_i eine S-glatte Zahl ist durch Trial Division durch die Primzahlen $p_1, \ldots, p_r \leq S$.

(3) Falls Q_i aus (2) S-glatt ist, so schreibe die Exponenten von $z_j := (-1)^i Q_i = A_i^2 - B_i^2 kN$ modulo 2 als eine neue Zeile der Matrix E und setze $x_j := A_i$ und $j := j + 1$.

(4) Teste, ob E einen Kern hat: Ist $\sum_{j\in I} e_{jl} \equiv 0 \pmod 2$ für alle $l = 0, \ldots, r$, so setze $y = \sqrt{\prod_{j\in I} z_j}$ und $x := \prod_{j\in I} x_j$ und teste, ob $\mathrm{ggT}(x - y, N)$ ein nichttrivialer Teiler von N ist.
(5) Ist die Periode der Kettenbruchentwicklung von $\sqrt{kN}$ erreicht, so wähle ein neues k in Schritt (0).

4.3 Das Quadratische Sieb

Ein Schwachpunkt beim Kettenbruchalgorithmus ist, daß ein Glattheitstest teuer ist und man in Schritt (2) viele quadratische Reste vergeblich auf Glattheit testet. 1982 hat C. Pomerance [13] einen Algorithmus veröffentlicht, der die Erzeugung der quadratischen Reste und damit auch den Glattheitstest vereinfacht. Das *Quadratische Sieb* erzeugt quadratische Reste modulo N als Werte eines Polynoms. Sei also $f(X) := X^2 - N \in \mathbf{Z}[X]$ und setze $z_i := f(x_i) = x_i^2 - N$ für $x_i \in [\sqrt{N} - M, \sqrt{N} + M] \cap \mathbf{N}$. Um die S-glatten (oder S-semiglatten) quadratischen Reste unter den z_i zu finden, geht man wie beim Sieb des Eratosthenes vor. Ist nämlich p ein Teiler von $f(x_i)$, so teilt p auch alle $f(x_i + k \cdot p)$ mit $k \in \mathbf{Z}$. Um Divisionen zu vermeiden, speichert man die Werte $R_i := \log|f(x_i)|$ ab. Für alle Primzahlen $p \leq S$ berechnet man ein $x(p)$ mit $p \mid f(x(p))$ und subtrahiert $\log(p)$ von allen R_i, für die $x_i \equiv \pm x(p) \pmod p$ ist. Ist nach dem Durchlaufen aller Primzahlen

$$R_i = \log(|f(x_i)|) - \sum_{\substack{p\leq S,\ p \text{ prim} \\ x_i \equiv \pm x(p) \pmod p}} \log(p)$$

kleiner als eine vorgegebenen Schranke, so ist z_i ein guter Kandidat für eine S-glatte Zahl. Man testet nur solche z_i auf Glattheit und bestimmt gleichzeitig die Exponentenvektoren und damit die Matrix E analog zu Schritt (2)-(4) des Kettenbruchalgorithmus.

Da Sieben sehr viel schneller ist als Trial Division, ist das Quadratische Sieb dem Kettenbruchalgorithmus überlegen. Ein Problem beim Quadratischen Sieb ist, daß die Werte $f(x_i)$ schnell groß werden und deshalb schlechte Chancen haben, glatt zu sein. Deshalb werden i. a. gleich mehrere Polynome betrachtet [20], damit M und folglich die Zahlen z_i klein gehalten werden können. Das so entstehende Verfahren, das sogenannte *Multiple Polynomial Quadratic Sieve*, ist im Moment einer der besten allgemeinen Faktorisierungsalgorithmen. Mit ihm können z. B. 67- bis 88-stellige Zahlen in 0,4 bis 12 CPU-Stunden faktorisiert werden [1].

4.4 Das Zahlkörpersieb

Rekorde im Faktorisieren hat man mit dem *Zahlkörpersieb* [8] erzielt. Dabei wird in Teilringen algebraischer Zahlkörper gerechnet, die $\mathbf{Z}/N\mathbf{Z}$ als ein homomorphes Bild haben. Man bestimmt zwei irreduzible, der Einfachheit halber hier als normiert vorausgesetzte, Polynome $f(X), g(X) \in \mathbf{Z}[X]$ vom Grad n bzw. l und ein $m \in \mathbf{Z}$ mit $f(m) \equiv 0 \pmod N$ und $g(m) \equiv 0 \pmod N$. Weiter seien $\alpha, \beta \in \mathbf{C}$ Nullstellen von f bzw. g, $f(\alpha) = g(\beta) = 0$. Dann induziert die Abbildung $\alpha \mapsto m$ (bzw. $\beta \mapsto m$) einen Ringhomomorphismus von $\mathbf{Z}[\alpha] \to \mathbf{Z}/N\mathbf{Z}$ (bzw. $\mathbf{Z}[\beta] \to \mathbf{Z}/N\mathbf{Z}$). Man sucht Zahlen $v_i, w_i \in \mathbf{Z}$ mit $\mathrm{ggT}(v_i, w_i) = 1$, so daß gewisse Teilpro-

dukte

$$(*) \quad \prod_{i\in I}(v_i - w_i\alpha) = \gamma^2 \ (\gamma \in \mathbf{Z}[\alpha]) \text{ und } \prod_{i\in I}(v_i - w_i\beta) = \delta^2 \ (\delta \in \mathbf{Z}[\beta])$$

Quadrate sind. Ist nämlich $\gamma = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}$ und $\delta = d_0 + d_1\beta + \ldots + d_{l-1}\beta^{l-1}$, so erfüllen $x := \sum_{i=0}^{n-1} c_i m^i$ und $y := \sum_{j=0}^{l-1} d_j m^j$ die Kongruenz

$$x^2 \equiv \prod_{i\in I}(v_i - w_i m) \equiv y^2 \pmod{N}.$$

Um geeignete Quadrate wie in $(*)$ zu finden, sucht man $v_i, w_i \in \mathbf{Z}$ für die $(v_i - w_i\alpha)$ und $(v_i - w_i\beta)$ „glatte" Zahlen sind. Dabei will man möglichst das Rechnen im Zahlkörper $\mathbf{Q}[\alpha]$ (bzw. $\mathbf{Q}[\beta]$) vermeiden. Eine notwendige Bedingung für $(*)$ ist, daß die Normen $\prod_{i\in I}\mathrm{Norm}(v_i - w_i\alpha) = \mathrm{Norm}(\gamma)^2$ und $\prod_{i\in I}\mathrm{Norm}(v_i - w_i\beta) = \mathrm{Norm}(\delta)^2$ Quadrate in $\mathbf{Z}$ sind.

Nun ist $\mathrm{Norm}(v - w\alpha) = w^n f(v/w)$ ein ganzzahliges Polynom in v und w. Hält man z. B. w fest, so kann man Zahlen v, für welche $\mathrm{Norm}(v - w\alpha)\cdot \mathrm{Norm}(v - w\beta)$ glatt ist, durch Sieben der Polynome $w^n f(X/w)$ und $w^l g(X/w) \in \mathbf{Z}[X]$ analog wie im Quadratischen Sieb bestimmen.

Das Aufstellen der Matrix E aus den Exponentenvektoren der glatten $v_i - w_i\alpha$ (und $v_i - w_i\beta$) muß verfeinert werden. Die Spalten von E werden mit Primidealen von $\mathbf{Z}[\alpha]$ indiziert. Teilt eine rationale Primzahl p die Norm $\mathrm{Norm}(v - w\alpha)$, so gibt das $r \in \{0, \ldots, p-1\}$ mit $v \equiv wr \pmod{p}$ das Primideal $\wp_r$ in $\mathbf{Z}[\alpha]$ über p an, welches das Ideal $(v - w\alpha)$ teilt. Anstelle von nur einer Spalte für jedes p hat die Matrix E also für jedes vorkommende (p, r) eine Spalte. Jedes Element aus dem Kern von E entspricht nun einem Produkt $\prod_{i\in I}(v_i - w_i\alpha)$, das Quadrat eines Ideals in $\mathbf{Z}[\alpha]$ ist. Auch beim Kettenbruchalgorithmus hatten wir noch eine zusätzliche Spalte für das Vorzeichen eingeführt. In $\mathbf{Z}[\alpha]$ muß man sehr viel mehr Einheiten als nur ± 1 berücksichtigen. Außerdem ist im allgemeinen nicht jedes Ideal in $\mathbf{Z}[\alpha]$ von einem Element erzeugt. Beide Probleme kann man gleichzeitig, ohne viel Rechnen in $\mathbf{Z}[\alpha]$, mit Hilfe von sogenannten quadratischen Charakteren erschlagen: Dazu wählt man z. B. Primideale $\mathcal{Q}$ in $\mathbf{Z}[\alpha]$, deren Norm eine Primzahl größer als S ist. Damit ist sichergestellt, daß die S-glatten $v - w\alpha$ auf Einheiten modulo $\mathcal{Q}$ abgebildet werden. Für jedes dieser Primideale $\mathcal{Q}$ erhält die Matrix E eine weitere Spalte, in die man einträgt, ob $(v_i - w_i\alpha)$ auf ein Quadrat in $\mathbf{Z}[\alpha]/\mathcal{Q}$ abgebildet wird (Eintrag 0) oder auf ein Nichtquadrat (Eintrag 1). Wählt man genügend viele solche Ideale $\mathcal{Q}$, so entspricht jedes Element aus dem Kern von E mit großer Wahrscheinlichkeit einem Quadrat in $\mathbf{Z}[\alpha]$. Analog verfährt man mit den $(v - w\beta)$, was ungefähr ebensoviele Spalten in E liefert. Um ein Element aus dem Kern von E zu finden, braucht man jetzt sehr viel mehr Paare (v_i, w_i), für die $\mathrm{Norm}(v_i - w_i\alpha)\mathrm{Norm}(v_i - w_i\beta)$ glatt ist. Die Wahrscheinlichkeit, solche glatten Zahlen zu finden, ist jedoch so viel größer, daß der Nachteil der zusätzlichen Spalten in E und auch der zusätzliche Rechenaufwand in Zahlkörpern für große Zahlen N aufgewogen werden. Wie auch schon beim Quadratischen Sieb ist der zeitaufwendigste Teil des Algorithmus, das Sieben, sehr leicht parallelisierbar und kann problemlos auf mehrere Rechner verteilt werden.

Der aktuelle Rekord im Faktorisieren nichtspezieller Zahlen wurde am 22. August 1999 mit dem Zahlkörpersieb aufgestellt. H. te Riele und andere fanden in

Gemeinschaftsarbeit die Faktorisierung einer 155-stelligen Zahl aus der RSA-challenge-list (Internetseite [RSA]) als Produkt von zwei 78-stelligen Primzahlen. Die Auswahl des Polynoms f (vom Grad 5) benötigte 100 MIPS Jahre, also weniger als ein halbes Jahr CPU-Zeit auf modernen Prozessoren. Es soll kleine Werte im Siebbereich annehmen und ungewöhnlich viele Nullstellen modulo kleiner Primzahlen haben. g wurde als $X - m$ gewählt. Die Gesamtzeit beim Sieben betrug 8000 MIPS Jahre (35,7 CPU Jahre) jedoch nur 3 1/2 Monate Kalenderzeit, da auf sehr vielen Rechnern gleichzeitig gesiebt wurde. Das Aufstellen der Matrix E, die Berechnung von Elementen aus dem Kern und das Wurzelziehen gingen im Vergleich zum Sieben sehr schnell.

Dies ist aber noch nicht die größte Zahl, die mit dem Zahlkörpersieb faktorisiert wurde. Am 8. April 1999 wurden der 93-stellige und der 118-stellige Primteiler der Zahl $N = 10^{211} - 1$ gefunden. Dazu wurde die spezielle Form von N zur geschickten Wahl der Polynome $f(X) = 10X^6 - 1$ und $g(X) = X - 10^{35}$ ($m = 10^{35}$) benutzt.

5 Wie schnell kann Faktorisieren sein?

Die meisten Methoden zum Faktorisieren einer Zahl N benutzen glatte Zahlen. Dabei ist die Häufigkeit glatter Zahlen nicht nur für eine Komplexitätsanalyse des Algorithmus von Bedeutung, sondern auch für die optimale Auswahl der Schranken. Sei $\psi(M, S)$ die Anzahl S-glatter Zahlen $\leq M$. Um T verschiedene S-glatte Zahlen zu finden, muß man also in etwa $MT/\psi(M, S)$ zufällige Zahlen $\leq M$ erzeugen. Definiert man

$$L_M[v, c] := \exp(c \cdot \ln(M)^v \ln(\ln(M))^{1-v}),$$

so ist nach [2, Theorem 10.1]

$$\frac{MT}{\psi(M, S)} \geq L_M[1/2, \sqrt{2} + o(1)]$$

für $M \to \infty$, falls $T = S^{1+o(1)}$, wobei Gleichheit nur für $S = L_M[1/2, \sqrt{2}/2 + o(1)]$ gilt. Der Kettenbruchalgorithmus und auch das Quadratische Sieb erzeugen quadratische Reste modulo N in der Größenordnung $M \sim \sqrt{N}$. Da man in etwa so viele S-glatte Zahlen benötigt, wie es Primzahlen $\leq S$ gibt (also $S/\ln(S) \sim S^{1+o(1)}$), ist die optimale Schranke also $S = L_{\sqrt{N}}[1/2, \sqrt{2}/2 + o(1)]$. Da die übrigen Operationen vernachlässigt werden können, ist unter der Annahme, daß die erzeugten quadratischen Reste sich bezüglich der Glattheit wie zufällige Zahlen benehmen, die erwartete Laufzeit für den Kettenbruchalgorithmus und das Quadratische Sieb $L_N[1/2, 1 + o(1)]$. Auch die Elliptische-Kurven-Methode findet, unter einer plausiblen Annahme, den kleinsten Primteiler p von N mit $L_p[1/2, 2 + o(1)]$ arithmetischen Operationen [7]. Wegen der Verteilung glatter Zahlen hat man bis zur Entdeckung des Zahlkörpersiebs angenommen, daß der Exponent $\frac{1}{2}$ nicht unterboten werden könne. Unter gewissen Annahmen läßt sich jedoch zeigen, daß die heuristische Laufzeit des Zahlkörpersiebs $L_N[1/3, (64/9)^{1/3} + o(1)]$ ist [2].

Bis heute kennt man noch keinen deterministischen Faktorisierungsalgorithmus mit subexponentieller Laufzeit. Setzt man die verallgemeinerte Riemann-

sche Vermutung voraus, so ist Shanks Klassengruppenalgorithmus [18] ein deterministisches Faktorisierungsverfahren mit Komplexität $O(N^{1/5+o(1)})$ ($O(N^{1/4+o(1)})$ ohne diese Voraussetzung). Dabei wird in der Idealklassengruppe von $\mathbf{Q}[\sqrt{-N}]$ mit Hilfe der Bijektion zwischen eigentlichen Idealklassen und reduzierten binären definiten quadratischen Formen gerechnet. Elemente der Ordnung 2 in dieser Gruppe liefern Zerlegungen von N, vgl. [14, Section 5.6.4].

Eine sehr interessante Plausibilitätsbetrachtung, die durch den Primzahlsatz motiviert ist und die Existenz einer Faktorisierungsmethode, deren Laufzeit polynomial in der Länge $\log(N)$ der eingegebenen Zahl ist, nahezulegen versucht, findet man in [16, S. 221 ff]. Die Entwicklung eines polynomialen Faktorisierungsalgorithmus ist zum einen praktisch interessant, da man damit das weitverbreitete Kryptographieverfahren RSA [17] angreifen kann, zum anderen ist es komplexitätstheoretisch von fundamentaler Bedeutung, wenn man zeigen kann, daß es keinen solchen polynomialen probabilistischen Algorithmus gibt, der mit herkömmlichen Computern auskommt.

P. Shor hat nämlich einen solchen Algorithmus für Quantencomputer entworfen [19]. Momentan ist der Quantencomputer zwar nicht mehr als ein theoretisches Modell, jedoch widerspricht es keinem physikalischen Gesetz, daß solche Computer in hinreichender Größe gebaut werden könnten. Anstelle der gewöhnlichen bits 0/1 gibt es im Quantencomputer sogenannte qubits $|0\rangle$ und $|1\rangle$, die einen 2-dimensionalen komplexen Vektorraum erzeugen. Die Zustände sind nicht mehr 0-1-Folgen der Länge n, sondern Vektoren $\sum_{s=0}^{2^n-1} a_s V_s$ in $\mathbf{C}^{2^n}$, wobei V_s das der Binärdarstellung von s entsprechende Tensorprodukt der qubits $|0\rangle$ und $|1\rangle$ ist. Die Zahlen $a_s \in \mathbf{C}$ erfüllen $\sum_{s=0}^{2^n-1} |a_s|^2 = 1$, und $|a_s|^2$ gibt die Wahrscheinlichkeit an, den Zustand V_s zu beobachten. Die elementaren Operationen sind Multiplikationen mit *Elementarmatrizen*; das sind gewisse unitäre $2^n \times 2^n$-Matrizen, die bis auf einen 4×4 Block die Identität sind. Ein Bestandteil des Shorschen Faktorisierungsalgorithmus ist die *Quantum Fourier Transformation*

$$\mathrm{QFT}_n : \mathbf{C}^{2^n} \to \mathbf{C}^{2^n}; V_s \mapsto \frac{1}{2^{n/2}} \sum_{r=0}^{2^n-1} \exp\left(\frac{2\pi i s r}{2^n}\right) V_r.$$

QFT_n kann als Produkt von $\binom{n}{2}$ Elementarmatrizen geschrieben werden. Zum Faktorisieren von N benutzt man wieder die alte Fermatsche Idee. Man wählt ein zufälliges $x \in \{2, \ldots, N-2\}$. Der Algorithmus bestimmt die Ordnung g von x in $(\mathbf{Z}/N\mathbf{Z})^*$. Ist g gerade und $x^{g/2} \not\equiv -1 \pmod{N}$, so ist $\mathrm{ggT}(x^{g/2}-1, N)$ ein nichttrivialer Teiler von N. Dazu wird in einem 2^{3L}-dimensionalen Vektorraum, d.h. mit qubits der Länge $3L$ gearbeitet, wobei $L := \lceil \log_2(N) \rceil$. Der Anfangszustand ist

$$\frac{1}{2^L} \sum_{s=0}^{2^{2L}-1} V_s \otimes V_0$$

wobei der zweite Tensorfaktor L qubits lang ist. Mit $O(L^3)$ elementaren Operationen berechnet man daraus

$$\frac{1}{2^L} \sum_{s=0}^{2^{2L}-1} V_s \otimes V_{x^s \pmod{N}}$$

und führt dann QFT_{2L} auf den ersten $2L$ qubits aus, was

$$\frac{1}{2^{2L}} \sum_{s=0}^{2^{2L}-1} \sum_{r=0}^{2^{2L}-1} \exp\left(\frac{2\pi irs}{2^{2L}}\right) V_r \otimes V_{x^s \pmod N}$$

liefert. Dieser Zustand wird gemessen. Dabei ist die Wahrscheinlichkeit, $V_r \otimes V_{x^j}$ zu beobachten, gleich

$$\frac{1}{2^{4L}} \left| \sum_{s \equiv j \pmod g} \exp\left(\frac{2\pi irs}{2^{2L}}\right) \right|^2 .$$

Falls die Einheitswurzeln in der Summe in verschiedene Richtungen zeigen, ist diese Zahl sehr klein. Also beobachtet man mit großer Wahrscheinlichkeit solche r mit $gr \sim d2^{2L}$ für ein $d \in \mathbf{N}$. Daraus läßt sich die Ordnung g von $x \in (\mathbf{Z}/N\mathbf{Z})^*$ durch Runden von $\frac{r}{2^{2L}}$ ermitteln. Der Algorithmus benötigt asymptotisch $O(L^3)$ elementare Operationen und ist damit polynomial in der Anzahl der Ziffern von N.

References

[1] *H. Boender, H. J. J. te Riele:* Factoring integers with large-prime variations of the quadratic sieve. Experiment. Math. **5** (1996), 257–273.

[2] *J. P. Buhler, H. W. Lenstra, Jr, C. Pomerance:* Factoring integers with the number field sieve. [8], 50–94.

[3] *R. P. Brent:* Parallel algorithms for integer factorisation. in J. H. Loxton (Hrsg.): Number theory and cryptography, Cambridge University Press (1990), 26–37.

[4] *H. Cohen:* A course in computational algebraic number theory. Springer Graduate Text in Mathematics **138** (third printing 1996)

[5] *R.-M. Elkenbracht-Huizing:* Historical background of the number field sieve factoring method. Nieuw archief voor wiskunde, Vierde serie Deel 14 no 3 (1996), 375–389

[6] *C. F. Gauß:* Disquisitiones arithmeticae. Yale university Press, New Haven, 1966

[7] *H. W. Lenstra, Jr:* Factoring integers with elliptic curves. Ann. of Math. **126** (1987), 649–673.

[8] *A. K. Lenstra, H. W. Lenstra, Jr. (Hrsg.):* The development of the number field sieve. Springer Lecture Notes in Math. **1554** (1993)

[9] *P. L. Montgomery:* A survey of modern integer factorization algorithms. CWI Quaterly, Volume 7 (4) (1994), 337–365

[10] *M. A. Morrison, J. Brillhart:* A method of factoring and the factorization of F_7. Math. Comp. **29** (1975), 83-205.

[11] *J. Pollard:* Theorems of factorization and primality testing. Proc. Cambridge Philos. Soc. **76** (1974), 521–528.

[12] *J. Pollard:* Monte Carlo method for factorization. BIT 15 (1975), 331–334.

[13] *C. Pomerance:* Analysis and comparison of some integer factoring algorithms. In H. W. Lenstra, Jr. and R. Tijdeman (Hrsg.) Computational Methods in Number Theory, Part I, Mathematisch Centrum Amsterdam (1982), 89–139.

[14] *C. Pomerance, R. Crandall:* Primes. A computational perspective. Springer (2000)

[15] *P. Ribenboim:* The NEW book of prime number records. Springer (1996)

[16] *H. Riesel:* Prime numbers and computer methods of factorization. Second edition, Birkhäuser (1994)

[17] *R. L. Rivest, A. Shamir, L. Adleman:* A method of obtaining digital signatures and public-key cryptosystems. Comm. Assoc. Compu. Mach. **21** (1978), 120–126.

[18] *D. Shanks:* Class number, a theory of factorization and genera. Proc. Symp. Pure Math. **20** A.M.S. Providence, R.I. (1969), 415–440.

[19] *P. W. Shor:* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Computing **26** (1997), 1484-1509.
[20] *R. D. Silverman:* The multiple polynomial quadratic sieve. Math. Comp. **48** (1987), 329-339.
[21] *H. C. Williams:* A $p+1$ method of factoring. Math. Comp. **39** (1982), 225-234.

Einige interessante Internetseiten

The number theory web http://www.maths.uq.oz.au/~krm/web.html
Auf dieser Seite findet man unter anderem viele homepages von Zahlentheoretikern. Alle weiteren hier aufgeführten Internetseiten sind von dieser Seite aus gelinkt.

The prime pages [PRIME]: http://www.utm.edu/research/primes
Eine sehr ansprechende Seite mit vielen Links. Natürlich findet man dort Informationen über Primzahlrekorde, Primzahltests, Mersenne-Primzahlen, Software und eine lange Literaturliste. Aber man kann auch Primzahlen hören, sehen oder raten. (z. B. unter „Aesthetics of the Prime Numbers Sequence")

Faktorisieren Eine informative Internetseite zum Faktorisieren mit elliptischen Kurven ist
[ECM]: http://www.loria.fr/~zimmerma/records/ecmnet.html
Dort findet man Literatur zum Faktorisieren mit elliptischen Kurven sowie Links zu anderen Seiten, unter anderem den Link NFSNET, wo man auch einige Literatur zum Zahlkörpersieb bekommen kann.
Eine Liste von schwer zu faktorisierenden Zahlen erhält man unter
[RSA]: http://www.rsa.com/rsalabs/html/factoring.html
Über den aktuellen Stand der Faktorisierung von Fermat-Zahlen informiert
[FERMAT]: http://vamri.xray.ufl.edu/proths/fermat.html

Gabriele Nebe
Lehrstuhl B für Mathematik
RWTH Aachen
Templergraben 64
D-52062 Aachen
gabi@math.rwth-aachen.de

(*Eingegangen 28.10.1999*)

Jber. d. Dt. Math.-Verein. 102 (2000) 15–41

On the Milnor Conjectures: History, Influence, Applications

A. Pfister, Mainz

0 Introduction

Let F be a field, let $n \geq 0$ be an integer.
The "Milnor Conjectures" concern a set of triangles

$$\begin{array}{ccc} & k_nF & \\ {\scriptstyle s_n}\swarrow & & \searrow{\scriptstyle h_n} \\ \bar{I}^nF & \dashrightarrow \bar{e}_n & H^nF \end{array}$$

where the groups $\bar{I}^n = I^n/I^{n+1}$, H^n and k_n come from quadratic form theory, cohomology theory and algebraic K-theory respectively. s_n, h_n and hopefully $\bar{e}_n$ are homomorphisms. Proper definitions will be given later (the letter F is omitted whenever possible).

Very roughly the necessary foundation of quadratic form theory began with Witt (1937) and was extended by myself (1966), general cohomology theory was introduced by Cartan-Eilenberg (1956), Galois cohomology by Serre (1962, 1964).

The intimate connection between quadratic forms and Galois cohomology turned up in a paper of Springer (1959), Stiefel-Whitney invariants of quadratic forms were introduced by Delzant (1962) and further investigated by Scharlau (1967).

In a fundamental paper Milnor (1970) introduced his (big) K-groups K_n and (small) K-groups $k_n = K_n/2K_n$ of a field and constructed the homomorphisms s_n and h_n. The existence of homomorphisms e_n was known only for $n \leq 2$ at that time, e_0, e_1, e_2 being the "classical invariants" of quadratic forms in a modern version.

Furthermore Milnor asked the following questions:

Q 0: Is the intersection of the ideals I^n equal to zero?
(This question occurred already in my and Scharlau's paper)
Q 1: Is s_n bijective for all n and fields F?
Q 2: Is h_n bijective for all n and fields F?
(This question is implicitly contained in the remark on p 340, l 5 of his paper).

It soon became clear that these questions were of utmost importance and interest for the three theories involved (corresponding to the three corners of our

triangle). As Q 0 had been solved in the short joint paper of Arason and myself (1971) even before we got to know Milnor's paper there remained Q 1 and Q 2. They entered into the literature as the "Milnor Conjectures".

After Milnor, some important historical steps were the following: Arason (1975) proved the existence of the third invariant e_3, Merkurjev showed that h_2 (and therefore s_2 and $\bar{e}_2$) is always an isomorphism, Jacob-Rost (1989) and independently Merkurjev-Suslin (1990) proved the existence of e_4 and the bijectivity of $\bar{e}_3$.

Finally Q 2 was "solved"[1] by Voevodsky (1996) and Q 1 was "solved" by Orlov-Vishik-Voevodsky but many other mathematicians also contributed to this impressive work. The final result can be phrased as follows: There exists a natural triangle

$$\begin{array}{ccc} & k_*F & \\ s_* \swarrow & & \searrow h_* \\ \widehat{W}F & \xrightarrow{\widehat{e}} & H^*F \end{array}$$

of $\mathbb{N}_0$-graded commutative rings k_*, $\widehat{W}$, H^* with isomorphisms s_*, $\widehat{e}$, h_* (of graded rings) such that $h_* = \widehat{e} \cdot s_*$. Here $k_* = \sum_{n \geq 0} k_n$ is the (small) k-ring, $H^* = \sum_{n \geq 0} H^n$ is the cohomology ring and $\widehat{W} = \sum_{n \geq 0} \bar{I}^n$ is the "graded Witt ring" of the field F.

There are already some applications of the positive solution of the Milnor Conjectures which are described in the last section. In addition there is great hope that more applications are to follow, in particular a better understanding of the original Witt ring W and of the absolute Galois group Γ of F.

As this is a survey for non-experts I have tried to keep the text as simple as possible. A preliminary version appeared in May 1999, it contains 6 appendices on some technical details the headings being:

Central simple algebras and the Brauer group;
Clifford algebras and classical invariants;
Multiplicativity of Pfister forms;
Cohomology groups;
Witt-Grothendieck ring and Stiefel-Whitney invariants;
Kato's work in characteristic 2.

These appendices were intended to outline that the necessary background for a full understanding of the Milnor Conjectures (not the proof of them!) is purely algebraic in nature and in fact rather elementary. To save space these appendices are not reproduced here.

During and after conferences in Paris (March 99), Oberwolfach (May 99) and Dublin (July 99) many people have given me their advice and comments on the preliminary version of the paper and thereby improved the present final version. My special thanks go to J. Arason, B. Kahn, A. Quéguiner, M. Rost, J.-P. Serre and M. Szyjewski.

[1] More about the meaning of the word "solved" will be said in section 5.

1 Quadratic Forms

Classically quadratic forms were considered as a part of number theory until the proof of the Hasse-Minkowski-Theorem which classifies quadratic forms over a number field K by invariants (Minkowski 1890 for $\mathbb{Q}$, Hasse 1923 for general K).
The "Algebraic Theory of Quadratic Forms" over an arbitrary field F was created in the famous paper of Witt [W, 1937]. For obvious reasons the case *char $F = 2$ is excluded* in his paper and most publications since, hence also here. But it is essentially known how to change things in this special case, and the analogues of the Milnor Conjectures have been formulated *and proved* by Kato [Kat 1, 1982] long before the conjectures could be solved for *char $F \neq 2$*.

1.1 Part A

The essential points of Witt's theory are:

(1) Let F be the given field. One considers quadratic forms q of any finite dimension $m \geq 0$ over F. In geometric language q is a quadratic map $V \to F$ where V is an m-dimensional F-vectorspace. The pair (V, q) is then called "quadratic space" over F. An F-linear change of variables (resp. a base change in V) leads to an "equivalent" or "isometric" form q' resp. quadratic space (V', q'). If necessary such an equivalence is denoted by $q \cong q'$ but otherwise the letter q always stands for the equivalence (or isometry) class of the quadratic form q.
Since char $F \neq 2$ it is immediately clear that q can be "diagonalized", i. e. the underlying vectorspace V possesses an orthogonal (with respect to q) basis $e_1, \cdots, e_m$ such that

(a) $q(v) = q(\sum_1^m v_i e_i) = \sum_1^m a_i v_i^2$

for $v = \sum_1^m v_i e_i \in V\ (v_i \in F)$. The $a_i \in F$ are called the (diagonal) coefficients of q. As a quadratic form, i. e. as a homogeneous polynomial of degree 2, q is then given by

(b) $q(x) = \sum_1^m a_i x_i^2 \quad \in F[x] := F[x_1, \cdots, x_m]$.

Instead of (a) or (b) we just write:

$q =< a_1, \cdots, a_m >$.

Clearly the ordering of the coefficients $a_1, \cdots, a_m$ plays no role if we consider q only up to equivalence.
Also we can and will always suppose that all

$a_i \in \dot{F} = F \setminus \{0\}$

otherwise m could be reduced. q is then called "regular" or "non-degenerate".

(2) (Classes of) Regular quadratic forms

$q^{(1)} =< a_1, \cdots, a_{m_1} >$, $q^{(2)} =< b_1, \cdots, b_{m_2} >$

can be added (direct orthogonal sum of quadratic spaces)

$q^{(1)} + q^{(2)} =< a_1, \cdots, a_{m_1}, b_1, \cdots, b_{m_2} >$

and multiplied (tensor product of quadratic spaces)

$q^{(1)} \cdot q^{(2)} =< a_i b_j >_{i=1,\ldots,m_1;\, j=1,\ldots m_2}$

Together with the zero element $0 =< \emptyset >$ (of dimension $m = 0$) and the unit element $1 =< 1 >$ (of dimension $m = 1$) we get the commutative semiring $S := SF$ of (classes of regular) quadratic forms q over F.

(3) The cancellation law holds in S, i. e. we have:

$q^{(0)} + q^{(1)} = q^{(0)} + q^{(2)} \Rightarrow q^{(1)} = q^{(2)}$

This is a fundamental and non-trivial result of Witt.

(4) A quadratic form q is called "isotropic over F" if there exists a non-trivial vector $0 \neq v \in V$ with $q(v) = 0$, otherwise q is "anisotropic". Clearly (regular) forms of dimension 0 or 1 are anisotropic. It is easy to see that every isotropic binary (= 2-dimensional) form is equivalent to the

"hyperbolic plane" $\mathbb{H} := < 1, -1 >$

Furthermore every quadratic form q has a unique decomposition

$$q = i(q) \times \mathbb{H} + q_0 = \underbrace{\mathbb{H} + \cdots + \mathbb{H}}_{i(q)} + q_0$$

where the "Witt index" $i(q) \in \mathbb{N}_0$ is uniquely determined by q and where the form q_0 (sometimes called the kernel form of q) is anisotropic and unique up to equivalence. We have: $\dim q = 2i(q) + \dim q_0$.

The case $q_0 = 0$ is allowed, in this case q is called "hyperbolic".

(5) **Definition** (Witt) Let $q^{(1)}, q^{(2)} \in SF$ with anisotropic kernels $q_0^{(1)}, q_0^{(2)}$. We write

$q^{(1)} \sim q^{(2)} :\Longleftrightarrow q_0^{(1)} = q_0^{(2)}$ in S

$q^{(1)}$ and $q^{(2)}$ are then called "Witt equivalent".

The set $W = WF := SF/\sim$ of Witt equivalence classes is called the "Witt ring of F". It is easily seen that addition and multiplication are well-defined on WF and that $-q :=< -a_1, \cdots, -a_m >$ is the additive inverse of $q =< a_1, \cdots, a_m >$ modulo $\sim$ since $q + (-q) = m \times \mathbb{H}$ in S.

If there is no danger of confusion we identify $q \in S$ with its Witt equivalence class $\tilde{q} \in W$, i. e. we simply write $q \in W$.

(6) Clearly W is additively generated by the unary (= 1-dimensional) forms $< a >$ with $a \in \dot{F}$. These generators satisfy the following relations:

(a) Unary relations:

$< a >=< b > \Longleftrightarrow a\dot{F}^2 = b\dot{F}^2$ in the "square class group" $\dot{F}/\dot{F}^2$

$< a > \cdot < b >=< ab >$ for all $a, b \in \dot{F}$

(b) Binary relations: $< a_1 > + < a_2 >=< a_1, a_2 >$ satisfies :

$$< a_1, a_2 >=< b_1, b_2 > \Longleftrightarrow \begin{cases} a_1 a_2 = b_1 b_2 \text{ in } \dot{F}/\dot{F}^2 \\ < a_1, a_2 > \text{ represents } b_1 \text{ over } F \end{cases}$$

$$\Longleftrightarrow \begin{cases} a_1 a_2 = b_1 b_2 \text{ in } \dot{F}/\dot{F}^2 \\ (a_1, a_2) = (b_1, b_2) \text{ in } Br_2 F \end{cases}$$

Furthermore:
$< a_1, a_2 >=< 1, -1 >= \mathbb{H} \Longleftrightarrow < a_1, a_2 >$ is isotropic over F.
(The definition of the "quaternion symbol" (a_1, a_2) and the group Br_2F is given below, see (10a)).

(7) Witt's "Chain Equivalence Theorem" tells us that all relations in W between the generators $< a >$ follow from the ring axioms and the "elementary relations" given in (6).

(8) Let E/F be any field extension. The embedding $i : F \to E$ induces natural maps $SF \to SE$ and $i_{E/F} : WF \to WE$. $i_{E/F}$ is a ring homomorphism but not injective in general since an anisotropic form q over F can become isotropic over E.
Example: $E = F(\sqrt{a})$, $q =< 1, -a >$ with $a \in \dot{F} \setminus \dot{F}^2$.
Then $q_E := i_{E/F}(q) =< 1, -1 >= 0$ in WE.

(9) There are some "classical invariants" of a quadratic form $q =< a_1, \cdots, a_m > \in S$. Very easy are the "dimension" $\dim q = m$ and the "determinant" $\det q = a_1 \cdot \ldots \cdot a_m \cdot \dot{F}^2 \in \dot{F}/\dot{F}^2$.
(Note that only the square class of $\prod_1^m a_i = a_1 \cdots a_m$ is well-defined on S). In order to get invariants of the element $\tilde{q} \in W$ dim and det have to be modified in the following obvious way:
dim is replaced by $\dim \mathit{mod}\, 2 : W \to \mathbb{Z}/2\mathbb{Z}$
det is replaced by the "discriminant" (or "signed" determinant) $d(q) = (-1)^{\binom{\dim q}{2}} \det q = (-1)^{m(m-1)/2} \Pi_1^m a_i \in \dot{F}/\dot{F}^2$
Next there are "signatures". They correspond to orderings α of the field F (if any). Then $sgn_\alpha q :=$ number of positive entries a_i minus number of negative entries a_i with respect to α.
(By Sylvester's inertia law $sgn_\alpha q \in \mathbb{Z}$ is well-defined on S and on W). Except for one application we do not need signatures in this article and omit any further details.

(10) The most complicated classical invariant is the "algebra class" $c(q)$ or an intimately related invariant with the name "Hasse invariant". For $F = \mathbb{Q}$ (and similarly for a number field K) this invariant consists of a set of local invariants $c_p(q) \in \{1, -1\}$ where p runs through the prime numbers and the symbol ∞ (corresponding to the archimedean valuation of $\mathbb{Q}$). But the "Local-Global-Principle" of number theory tells us that the set $\{c_p(q)\}$ of local invariants is essentially equivalent to one "global invariant", namely the
algebra class $c(q) \in Br_2F$.
This invariant then works for any field F, it is well-defined on S and even on W. Very briefly there are two ingredients for the definition and the properties of the invariant $c(q)$:
(a) One considers (finite-dimensional, associative) central simple algebras A over the base field F. By a famous theorem of Wedderburn (1906) A is then isomorphic to a full matrix ring $M_r(D)$ where D is a "division algebra" (= skew-field) over F. Two such algebras A_1, A_2 are called (Brau-

er-)equivalent if their underlying division algebras D_1, D_2 are isomorphic. The equivalence classes $[A]$ of all central simple algebras A over F together with the product $[A] \cdot [B] := [A \otimes_F B]$ form a commutative group BrF, the "Brauer group of F". This group structure was discovered by R. Brauer (1932). Notice the intimate similarity between the construction of WF and BrF!

Since the dimension (over F) of any central simple algebra A is always a square number the "simplest" elements of BrF are the unit element $1 = [F]$ (represented by $A = F$) and the elements $[Q]$ which are represented by four-dimensional "quaternion algebras". Such an algebra Q has an F-basis $1, i, j, k$ with multiplication determined by

$$i^2 = a_1 \cdot 1\,,\ j^2 = a_2 \cdot 1\,,\ ij = -ji\ = k$$

for some $a_1, a_2 \in \dot{F}$. We then write $[Q] = (a_1, a_2) \in BrF$. This is the definition of the "quaternion symbol" used in (6b). The "standard involution" $i \to \bar{i} = -i, j \to \bar{j} = -j$ of Q shows that Q is isomorphic to its opposite algebra Q^{op}, hence (a_1, a_2) lies in the subgroup

$$Br_2F := \{[A] \in BrF : [A]^2 = 1\}$$

of elements of order ≤ 2 in the Brauer group.

(b) To any (regular) quadratic space (V, q) one can attach its Clifford algebra

$$C(q) = TV/I(q).$$

Here TV is the tensor algebra of V (which is of infinite dimension unless $m = \dim V = 0$) and $I(q)$ is the two-sided ideal of TV generated by all elements of the form

$$v \otimes v - q(v) \cdot 1 \quad (v \in V)$$

$C(q)$ is a $\mathbb{Z}/2\mathbb{Z}$-graded algebra of dimension 2^m.

Let $C_0(q)$ be the subalgebra of $C(q)$ consisting of all even elements. It turns out that $C(q)$ resp. $C_0(q)$ is a central simple algebra over F if $\dim q$ is even resp. odd. Furthermore $C(q)$ resp. $C_0(q)$ is always equivalent to a tensor product of quaternion algebras. The definition of the "algebra class" $c(q)$ is then as follows:

$$c(\tilde{q}) = c(q) := \left\{ \begin{array}{ll} [C(q)] & \text{even} \\ \text{if } \dim q \text{ is} & \\ [C_0(q)] & \text{odd} \end{array} \right\} \in Br_2F$$

For computations it is often more convenient to use the so-called "Hasse invariant" of a quadratic form $q = < a_1, \ldots, a_m >$ which is defined by

$$s(q) := \Pi_{1 \leq i < j \leq m}(a_i, a_j) \in Br_2F\,.$$

It can be shown that $s(q)$ is well-defined on the isometry class $q \in S$ but not on the Witt class $\tilde{q} \in W$. There are formulas for computing $s(q)$ from $c(q)$ or conversely (depending on $\dim q$ and $d\,q$). For more details see the standard books [L] of Lam or [Sc 2] of Scharlau.

Historical remarks:

1. It is interesting to note that Witt was the first who introduced the "Clifford algebra" $C(q)$ for a general quadratic form $q =< a_1, \ldots, a_m > \in S$. Clifford himself considered only the case $a_1 = \ldots = a_m = -1$ [Cl, 1878]. Of course Clifford, Witt and many other European mathematicians used the term "hypercomplex system" (up to ca. 1945) instead of "algebra" for a vectorspace with additional ring structure. The first systematical treatment of Clifford algebras can be found in the books of Eichler (1952) and Chevalley (1954).

2. It is also remarkable that Witt did not use the invariant $c(q)$ in his paper. Instead, he replaced

$q =< a_1, \ldots, a_m >$ by $q_e =< a_1, \ldots, a_m, \underbrace{-1, \ldots, -1}_{m} >$

(presumably in order to deal with even-dimensional forms only and to avoid the dichotomy in the definition of $c(q)$) and defined his "system invariant" $S(q)$ by $S(q) := c(q_e)$. But $S(q)$ is not invariant under adding a hyperbolic plane to q, hence does not give an invariant of the Witt class $\tilde{q} \in W$, too bad!

1.2 Part B

In the sixties I continued Witt's theory by investigating the properties of the Witt ring WF. The decisive role for this is played by special quadratic forms of dimension $m = 2^n$ $(n = 0, 1, \cdots)$, namely

(11) $<< a_1, \cdots, a_n >> := < 1, -a_1 > \cdot \cdots \cdot < 1, -a_n > \quad (a_i \in \dot{F})$

I called these forms "multiplicative", Witt called them "round", and later they were called "n-fold Pfister forms" by Elman-Lam [EL 1, 1971] and Knebusch [Kn 1, 1971].

Note the slightly different notation in the books of Lam [L, 1973], Scharlau [Sc 2, 1985] and myself [P 3, 1995].

Let $q =<< a_1, \cdots, a_n >>$ be as in (11), let x be an indeterminate vector of dimension 2^n, let $F(x)$ be the rational function field corresponding to x, let v be any vector of dimension 2^n with components in F.

Then we have the following main properties:

(12) a) $< q(x) > \cdot q \; = q$ over the field $F(x)$

b) $< q(v) > \cdot q \; = q$ over F if $q(v) \neq 0$

c) $0 =< q(v) > \cdot q \sim q$ over F if $q(v) = 0$

d) The set $\dot{D}_F(q) := \{a \in \dot{F} : \exists v \text{ with } q(v) = a\}$ (of elements $a \in \dot{F}$ which are "represented" by q over F) is a subgroup of $\dot{F}$.

In particular (12c) shows that q is either anisotropic over F or hyperbolic over F, i. e. $q \sim 0$, $q = 0$ in WF.

My original proof of (12) (see [P 1, 1966] or [P 3, p. 26]) used matrices. Later Witt found a shorter proof which is based on the properties of binary forms (see e.g. [P 3, p. 27]). Variations of this proof can be found in [Sc 2, ch. 2, §10] or [L, ch. X].

Many further properties of WF can be derived by using the multiplicative forms, e. g. the description of the torsion subgroup W_tF, the radical R and nilradical N, the prime ideals, units, zero-divisors and signatures of WF. But we do not need these things here.

The (Witt classes of) forms of even dimension clearly constitute a maximal ideal $I = IF$ of WF. I is the kernel of the surjective ring homomorphism

$$e_0 : W \to \mathbb{Z}/2\mathbb{Z} \qquad \text{where } e_0(q) := \dim q \ \ mod\ 2$$

Hence $\bar{e}_0 : W/I \to \mathbb{Z}/2\mathbb{Z}$ is a natural isomorphism.

I is called the "fundamental ideal" of W.

Since $< a, b >=< 1, -(-a) > - < 1, -b >=<< -a >> - << b >>$ the ideal I is additively generated by the 1-fold forms $<< a >>$, $a \in \dot{F}$. Therefore the n-th power I^n of I is generated by the n-fold forms $<< a_1, \cdots, a_n >>$ for every $n > 0$ (put $I^0 := W$). The factor groups

$$\bar{I}^n := I^n/I^{n+1}$$

are elementary abelian 2-groups.

(13) **Definition:** The $\mathbb{N}_0$-graded commutative ring

$$\hat{W} := \hat{W}F := \bigoplus_{n=0}^{\infty} \bar{I}^n$$

(whose multiplication is induced by the product in W) is called the "graded Witt ring" of F.

The discriminant $d(q)$ obviously satisfies the rules $d(<< a >>) = a$, $d(<< a >> + << b >>) = ab$,
$d(<< a, b >>) = d(<< a >> \cdot << b >>) = 1$,

hence d induces a surjective group homomorphism

$$d_I : (I, +) \to (\dot{F}/\dot{F}^2, \cdot)$$

with $I^2 \subset \ker(d_I)$. By induction on $\dim q$ it is easy to show that $q \in I$ and $d(q) = 1$ imply $q \in I^2$.

Hence we have a group isomorphism

$$\bar{d} : (I/I^2, +) \xrightarrow{\cong} (\dot{F}/\dot{F}^2, \cdot)$$

induced by the map d_I.

(Note that the discriminant $d : W \to \dot{F}/\dot{F}^2$ - though well defined on W - is not a group homomorphism!)

Similarly it can be shown that the algebra class $c(q)$ of $q \in W$ induces a homomorphism

$$\bar{c} : (I^2/I^3, +) \longrightarrow (Br_2F, \cdot)$$

Furthermore it turns out that the seemingly unrelated target groups for the maps $\bar{e}_0, \bar{d}, \bar{c}$ are indeed isomorphic to cohomology groups H^0, H^1, H^2 (see section 2). From this it follows that the "classical invariants" lead to group homomorphisms

$$\bar{e}_i : \bar{I}^i \longrightarrow H^i \qquad \text{for } i = 0, 1, 2$$

which appear in the bottom side of Milnor's triangle.

Finally I asked in my paper [P 1]:

$\underline{Q0}$: $\bigcap_n I^n = 0$ (for every field F)?

For a recent historical survey on quadratic forms which in particular exhibits many early connections to topology see the article [Sc 3] of W. Scharlau (1999).

2 Galois Cohomology

Homology and cohomology theories have their origin in topology and group theory. The first unified and purely algebraic treatment was given in the famous book "Homological Algebra" by Cartan-Eilenberg [CE, 1956]. Nowadays there are a lot of related but different cohomology theories like group-, sheaf-, etale, motivic cohomology etc. but we need only some elementary facts about cohomology of groups and Galois cohomology as presented in the two books "Corps Locaux" (1962) and "Cohomologie Galoisienne" (1964) of Serre [Se 1, Se 2]. Many of the results presented there are originally due to J. Tate.

Let Γ be a group, let $\Lambda = \mathbb{Z}[\Gamma]$ be its integral group ring and let A be an abelian group (usually written additively). We say that Γ acts on A if there is a map $\Gamma \times A \to A$, $(\gamma, a) \mapsto \gamma a$, with the following properties:

$$1a = a \ , \ \gamma(a_1 + a_2) = \gamma a_1 + \gamma a_2 \ , \ (\gamma_1\gamma_2)a = \gamma_1(\gamma_2 a)$$

for all $\gamma, \gamma_1, \gamma_2 \in \Gamma$, $a, a_1, a_2 \in A$.
In other words: A is a Λ-(left) module in the ring-theoretic sense, we also call it "Γ-module".
Under these conditions the cohomology groups $H^n(\Gamma, A)$ are defined for all $n \geq 0$, they are additive abelian groups. If A and B are two Γ-modules then their tensor product $A \otimes B$ (over $\mathbb{Z}$) becomes a Γ-module if we define

$$\gamma(a \otimes b) := \gamma a \otimes \gamma b$$

for $\gamma \in \Gamma$, $a \in A$, $b \in B$ and extend this Γ-action to $A \otimes B$ by linearity. In this situation the cohomology groups attached to A, B and $A \otimes B$ are related by a bilinear product

$$\cup : H^p(\Gamma, A) \times H^q(\Gamma, B) \longrightarrow H^{p+q}(\Gamma, A \otimes B) \ ,$$

called the "cup product".
In our case Γ is always the absolute Galois group of the field F, i. e. $\Gamma = Gal\,(F_s/F)$ where F_s is a separable closure of F. Γ is a profinite group (= projective limit of finite groups). In such a case one considers only "discrete" Γ-modules A which means that A has the discrete topology and Γ acts continuously on A. Furthermore all cochains are also assumed to be continuous. In this way one gets modified cohomology groups, the

"Galois cohomology" groups $H^n(\Gamma, A)$.

Alternatively Γ is the projective limit of the finite groups $\Gamma_E = Gal\,(E/F)$ where E runs over all finite Galois extensions of F with $E \subset F_s$, and $H^n(\Gamma, A)$ is the inductive limit of the groups $H^n(\Gamma_E, A)$. It is a matter of taste which description is "simpler".

The intimate connection between quadratic forms and Galois cohomology was discovered in a short paper of Delzant [De, 1962] and further investigated in the dissertation of Scharlau [Sc 1, 1967] and a paper of Belskii [Be, 1968]. The fundamental facts are the following:

Let $\mu_2 = \{1, -1\}$ be the group of second units of F (note that char $F \neq 2$). Γ acts trivially on μ_2.

The short exact sequence of multiplicative groups

(0) $1 \to \mu_2 \to \dot{F}_s \overset{x \mapsto x^2}{\longrightarrow} \dot{F}_s \to 1$

induces a long exact sequence of cohomology groups

(1) $$\begin{aligned} 1 &\to H^0(\Gamma, \mu_2) \to H^0(\Gamma, \dot{F}_s) \to H^0(\Gamma, \dot{F}_s) \\ &\to H^1(\Gamma, \mu_2) \to H^1(\Gamma, \dot{F}_s) \to H^1(\Gamma, \dot{F}_s) \\ &\to H^2(\Gamma, \mu_2) \to H^2(\Gamma, \dot{F}_s) \to H^2(\Gamma, \dot{F}_s) \to \dots \end{aligned}$$

From Hilbert's Theorem 90 we know that $H^1(\Gamma, \dot{F}_s) = 1$ and from the cohomological description of the Brauer group by means of 2-cocycles (see e. g. [Se 1, chap. X]) we know that $H^2(\Gamma, \dot{F}_s) \cong BrF$. Together with the trivial statements $H^0(\Gamma, \dot{F}_s) = \dot{F}$, $H^0(\Gamma, \mu_2) = \mu_2$ sequence (1) then reduces to the isomorphisms

$$H^1(\Gamma, \mu_2) \cong \dot{F}/\dot{F}^2 \ , \ H^2(\Gamma, \mu_2) \cong Br_2F = \ker (BrF \overset{x \mapsto x^2}{\longrightarrow} BrF)$$

Other useful treatments of the Brauer group and/or Galois cohomology can be found in the books of Draxl (Part II), Kersten (Kap. III), Knus-Merkurjev-Rost-Tignol (ch. VII) and in a paper of Tate for the 50th birthday of Serre, see the references.

Since we want to write Γ-modules and cohomology groups additively we replace the multiplicative group μ_2 by the additive group $\mathbb{Z}/2\mathbb{Z}$. (Remark: For $m > 2$ the group μ_m of m-th units in $\dot{F}_s$ is not always trivial as a Γ-module. Then it cannot be replaced by $\mathbb{Z}/m\mathbb{Z}$). In this way we get additive cohomology groups

(2) $H^n := H^nF := H^n(\Gamma, \mathbb{Z}/2\mathbb{Z})$ (for $n \geq 0$)

They appear in the right lower corner of Milnor's triangle. Clearly all H^n are elementary-abelian 2-groups. For $n \leq 2$ we have:

$H^0 = \mathbb{Z}/2\mathbb{Z}$ (trivial), H^1 is an additive version of $\dot{F}/\dot{F}^2$, H^2 is an additive version of Br_2F.

Remark: It is of great advantage that the cohomology groups H^n (and the K-groups of the next section) are written additively. If not, how could we write a cup-product (see below)?

The three classical invariants e_0, d, c of section 1 are now transformed into group homomorphisms

(3) $e_n : I^n \to H^n$ for $n = 0, 1, 2$

e_0 and e_1 induce isomorphisms

$\bar{e}_0 : W/I = \bar{I}^0 \to H^0 = \mathbb{Z}/2\mathbb{Z}$, $\bar{e}_1 : I/I^2 = \bar{I}^1 \to H^1$,

e_2 induces a homomorphism

(4) $\bar{e}_2 : I^2/I^3 = \bar{I}^2 \to H^2$

A natural question which first turned up in [De] and again in [P 1] is of course:

Is $\bar{e}_2$ an isomorphism?

It was solved in Merkurjev's famous paper [Me 1, 1981]. This was one of the most important steps towards the Milnor Conjectures (see section 4).
Since $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$ the cup-product introduced above induces bilinear maps

$$\cup : H^p \times H^q \to H^{p+q}$$

This product is commutative because the general cup-product is commutative up to sign.

Definition: The commutative graded ring

(5) $H^* := \bigoplus_{n=0}^{\infty} H^n$

is called the (small) cohomology ring of our field F.

Notation: Let $(a) \in H^1$ be the element which corresponds to the square class $a\dot{F}^2 \in \dot{F}/\dot{F}^2$ under the canonical isomorphism $(H^1, +) \cong (\dot{F}/\dot{F}^2, \cdot)$. Then we have the rules

(6) $(a) + (b) = (ab) \in H^1$ (trivial), $(a) \cup (b) = (a, b) \in H^2$ (easy)

where $(a, b) \in H^2$ is the element which corresponds to the "quaternion class" $(a, b) = c(< a, b >) \in Br_2 = Br_2F$ under the canonical isomorphism $(H^2, +) \cong (Br_2, \cdot)$ (see section 1, part (10)). For a proof of (6) see e.g. [KMRT, Prop. 30.4]

Remark: Before Merkurjev it was not known that the group H^2 is generated by cup-products $(a) \cup (b)$ with $(a), (b) \in H^1$. Before Voevodsky it was not known that H^* as a ring is generated by H^1.

The main work of Delzant and Scharlau consists in the construction and study of the so-called "Stiefel-Whitney invariants" $w_n(q)$ of quadratic forms $(n = 1, 2, \ldots)$. w_1 is just the determinant and w_2 is the Hasse invariant which was mentioned in section 1 part (10). Unfortunately the higher Stiefel-Whitney invariants $w_3, w_4, \ldots$ are not independent of one another, and - what is worse - they vanish on I^3 if $(-1) = 0 \in H^1$ (i. e. - $1 \in \dot{F}^2$) or (more generally) on I^t for large t if (-1) is nilpotent in H^* (i. e. - 1 is a sum of squares in F).

A further smaller problem with the Stiefel-Whitney invariants is that they do not live on the Witt ring $W = WF$ but on the "Witt-Grothendieck ring" $\tilde{W} = \tilde{W}F$ (for the definition see e.g. [Sc 2]) and that they take values in the (big) cohomology ring $\tilde{H} = \prod_{n=0}^{\infty} H^n$. For the Milnor Conjectures the higher invariants w_i $(i \geq 3)$ play no role. For all these reasons I have decided to omit more details about $\tilde{W}$, $\tilde{H}$ and Stiefel-Whitney invariants.

3 Milnor K-Theory

Like cohomology theory K-theory has its origins in topology, mainly in the work of Grothendieck on vector bundles (1957). See the early book [At, 1967]. In an algebraic setting vector bundles correspond to projective modules over the structure sheaf of the underlying topological space. This observation opened the door for introducing an "algebraic K-theory" over rings (commutative or not), see [SW,

1968]. The main foundations are due to Milnor [Mi 3, 1971] and Quillen [Q, 1973]. It is a non-trivial fact that the algebraically defined Milnor K-groups K_n^M and the topologically defined Quillen K-groups K_n^Q coincide for $n \leq 2$ (but not for $n > 2$). In this article we need only Milnor K-groups and omit the upper index M. Important further work on the K-theory of fields F is due to Suslin [Su 1-3].

It is well-known that J. Milnor (born 1931) worked in algebraic and differential topology and won the Fields Medal in 1962 for his discovery of exotic 7-spheres. But like many really great mathematicians he was interested in other topics as well, e. g. in geometry, algebra and (since 1975) dynamics. For about 8 years (1965–1973) he worked mainly in algebra. His algebraic work began with a paper on Whitehead torsion, then turned to the congruence subgroup problem (a famous paper with Bass and Serre) and finally led him to algebraic K-theory (see the book mentioned above) and quadratic forms, culminating in the book with Husemoller on "Symmetric Bilinear Forms" [MH, 1973]. Quadratic forms over $\mathbb{Z}$ turned up even much earlier in his work, for instance in the paper [Mi 1] on 4-manifolds.

There is a fine article by Bass [Ba, 1993] in the Symposium Volume in honor of Milnor's 60th birthday. He writes: "Milnor has had a deep and affectionate interest in quadratic form theory, as is evident from the beautiful book with Husemoller, based on Milnor's lectures. His paper "Algebraic K-theory and quadratic forms" [Mi 2, 1970] continues to guide much of the current research in the algebraic theory of quadratic forms".

Indeed, it is this paper which we have to discuss in some detail now because it provides the top of our triangle and the maps s_n, h_n. Let F be our field, let $K_1 = K_1F$ be its multiplicative group but written additively. This means that we have a one-to-one map (a kind of "logarithm"):

$$l : \dot{F} \to K_1 \ , \ l(ab) = l(a) + l(b)$$

Let T be the tensor-algebra of the $\mathbb{Z}$-module K_1,

$$\text{i.e.} \quad T = \mathbb{Z} \oplus K_1 \oplus (K_1 \otimes K_1) \oplus (K_1 \otimes K_1 \otimes K_1) \oplus \dots$$

Let J be the homogeneous two-sided ideal of T which is generated by the elements

$$l(a) \otimes l(1-a) \in K_1 \otimes K_1 \qquad (a \in \dot{F} \, , \, a \neq 1)$$

Then

(1) $$K_*F := T/J =: (\mathbb{Z} \oplus K_1 \oplus K_2 \oplus K_3 \oplus \dots)$$

is called the (big) "Milnor ring" of F. In other words each K_n $(n \geq 2)$ is the quotient of the n-fold tensor product $K_1 \otimes \dots \otimes K_1$ by the subgroup generated by all $l(a_1) \otimes \dots \otimes l(a_n)$ such that $a_i + a_{i+1} = 1$ for some $i \leq n-1$. K_*F is a non-commutative $\mathbb{N}_0$-graded ring (for $\xi \in K_m$, $\eta \in K_n$ one has $\eta\xi = (-1)^{mn}\xi\eta \in K_{m+n}$)

(2) $$k_* = k_*F := K_*F/2K_*F =: (k_0 \oplus k_1 \oplus k_2 \oplus \dots)$$

is called the (small) Milnor ring of F. It is a commutative $\mathbb{N}_0$-graded ring. Clearly we have:

$$k_0 = \mathbb{Z}/2\mathbb{Z} = H^0 \, , \, k_1 = K_1/2K_1 = H^1 \ (\cong \dot{F}/\dot{F}^2) \, , \, k_2 = K_2/2K_2, \dots$$

Bass writes about the definition of the groups K_n: "Milnor's results and questions revealed that K_*F, which at first looks somewhat naive for $n > 2$, carries a great deal of arithmetic information about the field F."
Let me repeat some details of Milnor's paper:
§1 contains some elementary consequences of the definitions, e. g.

(3) $l(a)\,l(-a) = 0 \quad , \quad l(a)^2 = l(a)\,l(-1) \quad \text{in} \quad K_*F \qquad (a \in \dot{F})$

(4) $l(a)\,l(b) + l(b)\,l(a) = 0 \qquad\qquad (a, b \in \dot{F})$

(This implies the anticommutativity of K_*F mentioned above).

(5) $l(-1)$ nilpotent in $K_*F \iff -1$ is a sum of squares in F

In §4 Milnor studies the relation between the (small) K-groups $k_n = k_nF$ and quadratic forms over F. Let

(6) $\{a\} := l(a) \bmod 2 \qquad \in k_1 \qquad (a \in \dot{F})$

be the generators of k_1 and hence of the ring $k_* = k_*F$ (as a $\mathbb{Z}/2\mathbb{Z}$-algebra). Define a map

(7) $s_n : k_n \to \bar{I}^n \qquad (n = 0, 1, 2, \ldots)$

by $s_n(\{a_1\} \cdot \ldots \cdot \{a_n\}) := \prod_{i=1}^{n} << a_i >> = << a_1, \ldots, a_n >> \bmod I^{n+1}$

s_n is well-defined since for $a_i + a_{i+1} = 1$ we have
$<< a_i, a_{i+1} >> = < 1, -a_i, -a_{i+1}, a_i a_{i+1} > = 0 \qquad \in WF$
s_n is n-linear since

$<< a >> + << b >> \equiv << ab >> \qquad \bmod I^2$, i.e.

$< 1, -a > + < 1, -b > - < 1, -ab > \sim < 1, -a, -b, ab > \in I^2$

Hence s_n is a group homomorphism which is clearly surjective.
Since $s_n(\{a_1\} \cdot \ldots \cdot \{a_n\}) = s_1\{a_1\} \cdot \ldots \cdot s_1\{a_n\}$ the maps s_n can be combined to a graded ring homomorphism $s_* : k_* \to \widehat{W}$.

$s_0 : \mathbb{Z}/2\mathbb{Z} = k_0 \longrightarrow \bar{I}^0 = W/I = \mathbb{Z}/2\mathbb{Z}$ is the identity

$s_1 : \dot{F}/\dot{F}^2 \cong k_1 \longrightarrow \bar{I}^1 = I/I^2 \;,\; a\dot{F}^2 \mapsto \{a\} \mapsto << a >> \bmod I^2$

is the inverse map of the discriminant map $\bar{d}$ (see the end of section 1), hence s_1 is an isomorphism.

(8) $s_2 : k_2 \to \bar{I}^2 = I^2/I^3$ is also an isomorphism.

This is non-trivial but there is a short proof. s_2 is the inverse of a map $w_2^M : I^2/I^3 \to k_2$ which is intimately related to the second Stiefel-Whitney invariant w_2.
Finally Milnor introduces the question
Q1: Is s_n bijective for all n (and fields F)? [Mi 1, §4, Question 4.3]
The other sections of Milnor's paper are also very interesting and important. §2 contains the study of discrete valuations $v : F \longrightarrow \mathbb{Z} \cup \infty$, residue homomorphisms ∂_π and the computation of the groups $K_nF(t)$ of the ra-

tional function field $F(t)$ from the groups $K_m E$ of finite algebraic extension fields E/F:
There is a split exact sequence:

$$(9) \qquad 0 \longrightarrow K_n F \longrightarrow K_n F(t) \xrightarrow{(\partial_\pi)} \bigoplus_\pi K_{n-1}(F[t]/(\pi)) \longrightarrow 0$$

where the sum extends over all monic prime polynomials $\pi \in F[t]$.
§3 contains the construction and some properties of the Milnor-Stiefel-Whitney invariants w_n^M which take values in k_n instead of H^n.
In §5 Milnor derives an exact sequence for the Witt group of a rational function field $F(t)$ which is very similar to the above sequence, namely

$$(10) \qquad 0 \to I^n F \to I^n F(t) \to \ominus_\pi I^{n-1}(F[t]/(\pi)) \to 0$$

As we do not need further details of these sections here, let me turn to §6 of Milnor's paper where he constructs the "norm residue homomorphisms".

$$(11) \qquad h_n : k_n \longrightarrow H^n \qquad (n = 0, 1, 2, \ldots).$$

This is the last thing we need for a complete definition of the "Milnor triangles" in the Introduction.
The h_n are the homogeneous components of the following natural graded ring-homomorphism (attributed to Bass-Tate):

$$(12) \qquad h_* = h_F : k_* F \longrightarrow H^* F$$

which is induced from the isomorphism

$$h_1 : k_1 \longrightarrow H^1 \quad , \quad \{a\} \mapsto (a) \qquad (\text{for } a \in \dot{F})$$

Since k_* is generated by k_1 the map h_1 can be extended to a (graded) ring-homomorphism $h_* : k_* \to H^*$ if we can show that it respects the defining relations of k_*.
This is almost trivial:
Let $a, b \in \dot{F}$ be such that $a + b = 1$, i. e. $\{a\} \cdot \{b\} = 0$ in k_2.
Then $h_2(\{a\} \cdot \{b\}) := h_1(\{a\}) \cup h_1(\{b\}) = (a) \cup (b) = (a, b) \in H^2$.
But the quaternion algebra $(a, 1 - a)$ splits, i. e. we have $(a, b) = 0 \in H^2$.
It is also immediate that

$$(13) \qquad \bar{e}_n \circ s_n = h_n \qquad \text{for } n = 0, 1, 2.$$

Near the end of his paper (on p. 340, l. 5) Milnor states: "I do not know of any examples for which the homomorphism h_F fails to be bijective." Using the results of the previous sections he can show that s_n and h_n are actually bijective (for all n) for all (finite, local, global) fields occurring in number theory, and for $F(t)$ and $F((t))$ whenever bijectivity holds for F and its algebraic extensions E/F. This provides enough background for raising the question

Q2 : Is h_n bijective for all n(and fields F)?

Let me finish this section with some metamathematical observations about the rings W, $\tilde{W}$, $\hat{W}$, H^*, k_*. They shed perhaps more light on the significance and influence of the Milnor conjectures. We look at these things with the eyes and the knowledge of the years 1970/71. Only occasionally I risk a view on the future development.

The Witt ring W is the most *concrete* object because we believe to know what quadratic forms are. However, if we want to find invariants of quadratic forms over a suitably general field F we soon get into trouble. Except for the "classical invariants" described in section 1 no further invariants had been found and even for the discriminant $d(q)$ resp. the algebra class $c(q)$ it was necessary to restrict q to I resp. I^2 in order to get group homomorphisms. (In fact, the next invariant e_3 which was found by Arason in 1975, is defined only on I^3 and not on I^2, see section 4).

This fact forced us to introduce some modifications of W like the graded Witt ring $\widehat{W}$ or the Witt-Grothendieck ring $\widetilde{W}$ or the "reduced Witt ring" $W_{red} := W/R$ (which plays no role in this survey) which hopefully are easier to handle. However again, this change has some drawback. For W we have seen in section 1 (6) that W can be "presented" by generators $< a >$ and a certain set of defining relations between them. This induces the generators $<< a_1, \ldots, a_n >>$ of the subgroup $I^n \subset W$ and also some relations between them coming from the binary relations of (6). But nobody can tell us that there are no further "hidden relations" in I^n. (This is a well-known problem in group theory.) Therefore we do not know whether I^n or the factor group $\bar{I}^n = I^n/I^{n+1}$ are "presented" by the generators $<< a_1, \ldots, a_n >>$ (or their classes in $\bar{I}^n$) and the induced relations between them. Hence we also cannot tell whether Milnor's maps s_n (left side of the triangle) are injective.

The cohomology ring H^* is the most *formal* object. By definition it depends only on the absolute Galois group Γ of F and not on other properties of F whereas W and $\widehat{W}$ depend in a complicated manner on the addition and multiplication of F. Another good property of H^* resp. its homogeneous components H^n is that these groups satisfy good exact sequences under a change of the field F or the exponent n. But the drawback of the cohomology groups H^n is the lack of any good understanding of the elements $\eta \in H^n$. For $n = 1$ η can be interpreted as a "crossed homomorphism", for $n = 2$ as a "crossed product" but for $n > 2$ no concrete description is known. For instance the question whether H^n is generated by n-fold cup-products from H^1 seems completely hopeless. Considering Milnor's triangle this implies that we know nothing about the maps h_n (whether they are injective or surjective).

Finally, Milnor's small ring k_* is the most *generic* object. This is the reason for the existence (and easy proof) of the homomorphisms s_n and h_n. At first it seems that the definition of K_* and k_* involves only the multiplicative group $\dot{F}$ of our field F (and this is true concerning the generators) but a careful look at the defining relations

$$l(a) \otimes l(b) = 0 \quad \text{for} \quad a + b = 1$$

shows that the addition of F also plays a role, even though the equation $a + b = 1$ is very special. As in the case of W or $\widehat{W}$ the Galois group Γ of F does not show up in the definition of k_*.

In contrast to the situation for H^n, I^n and (less complete) $\bar{I}^n$ practically nothing was known for k_n concerning exact sequences even in the simplest case of a quadratic extension $E = F(\sqrt{a})$. It is this case which was solved in 1981 by Mer-

kurjev (see section 4) and which turned out to be a milestone for the complete solution of the Milnor Conjectures by Voevodsky (see section 5).

Nevertheless it still looks like a miracle to me that the 3 corners of the Milnor triangles are isomorphic. This reveals deep connections between the additive and multiplicative structure of a field F, the Galois group Γ, quadratic forms on F and the more modern and abstract notions of cohomology and K-groups.

4 The time after Milnor

4.1 Invariants of quadratic forms

As already mentioned in the Introduction Arason and myself proved the intersection theorem, i. e. the positive answer to Question Q 0, in our paper [AP, 1971] without knowing Milnor's work at that time. Our main result reads:

(1) Let $q \neq 0$ be an anisotropic quadratic form over F such that $q \in I^n$. Then $\dim q \geq 2^n$.
The idea of the proof is as follows: Write $q = \sum_{i=1}^{r} \pm q_i$ where each q_i is an n-fold Pfister form. We use induction on r and the "transcendental method". Let $F(q_r)$ be the function field of q_r defined below. Over $F(q_r)$ we have $q_r = 0$, hence the induction hypothesis applies, i. e. we have either $\dim(q \otimes F(q_r))_{an} \geq 2^n$ or $q \otimes F(q_r) = 0$. In the latter case it can be shown that (up to a scalar factor) q_r is a subform of q over F, so again $\dim q \geq 2^n$.

(2) **Definition:** Let $q \neq \mathbb{H}$ be a quadratic form of dimension $m \geq 2$ over F. The polynomial $q(x) \in F[x]$ is then irreducible and defines the "quadric" $Q \in \mathbb{P}^{m-1}(F)$ given by $q(x) = 0$. The function field $F(q) := F(Q)$ of Q is then (also) called "function field of q over F".
It is a field of transcendence degree $m - 2$ over F.
For $q = \mathbb{H}$ or $\dim q \leq 1$ we define $F(q) := F$.
Example: $q = <1, -a> = <<a>> \Rightarrow F(q) = F(\sqrt{a})$.
In the early seventies Elman and Lam started their productive work on quadratic forms and K-theory, let me in particular mention the papers [EL 1, EL 2] and Lam's fine text-book [L]. The most important paper of this time however, at least with respect to the Milnor Conjectures, is the dissertation of Arason [A1, 1975].
Arason undertakes a systematic study of the rings W, $\widehat{W}$ and H^* and their behaviour under the maps which are induced from the field extension map $i_{E/F}$, the "Scharlau transfer" map $s_{E/F}$ (for the case of a finite extension E/F) and the (second) residue map $\partial : F \longrightarrow F/v$ (for the case of a field F with a discrete valuation v and residue field F/v). There are many exact sequences and commutative diagrams in his paper.
One of the main problems investigated by Arason is the existence of "higher invariants" for quadratic forms, i. e. group homomorphisms

$$e_n : I^n \longrightarrow H^n \qquad (n \geq 3)$$

Let $P_n := \{<<a_1, \ldots, a_n>> : a_i \in \dot{F}\} \subset I^n$ denote the set of all n-fold Pfister forms.

In paragraph 1, Satz 1.6 he shows:

(3) If a reasonably functorial map e_n exists then we must have

(*) $e_n(<< a_1, \ldots, a_n >>) = (a_1) \cup \ldots \cup (a_n)$

(4) e_n is well-defined on P_n

(5) For $q^{(1)}, q^{(2)} \in P_n$ with $q^{(1)} \equiv q^{(2)} \mod I^{n+1}$ we have $e_n(q^{(1)}) = e_n(q^{(2)})$.

The proof of this result is essentially elementary.
It uses a clever induction on n. But we have the
Existence Problem: Can e_n, if defined on P_n by (*), be extended to a well-defined group homomorphism $e_n : I^n \longrightarrow H^n$?
By property (5) e_n would then factor through I^{n+1} and induce the homomorphism
$\bar{e}_n : \bar{I}^n = I^n/I^{n+1} \longrightarrow H^n$
which we need for the lower side of Milnor's triangle.
Arason's last and deepest result is his Satz 5.7.
It says:

(6) $e_3 : I^3 F \to H^3 F$ is well-defined for all fields F (char $F \neq 2$).

For this he needs the following result which resembles very much some later discoveries of Merkurjev:

(7) For $\dim q > 8$ the map $i_{F(q)/F} : H^3 F \longrightarrow H^3 F(q)$ is injective.

In a final remark he also notes that e_3 (contrary to the classical invariants e_1, e_2) cannot be extended to a reasonable map
$b : I^2 \longrightarrow H^3$
even if it is not required that b be a homomorphism. This indicates that working with individual quadratic forms instead of elements of I^n becomes more and more difficult for growing exponent n. [Recent results of Hoffmann, Izhboldin, Karpenko, Esnault et.al. show that some properties one would like to hold for individual forms q with $\widetilde{q} \in I^n$ are just not true if the underlying field F is complicated enough. See the list of references.]

Next I have to mention the papers "Generic splittings of quadratic forms I, II" by Knebusch [Kn 2, 3 (1976/77)]. Let q_0 be an anisotropic form over $F = F_0$, let $F_1 = F(q_0)$ be its function field. If $\dim q_0 \geq 2$ then q_0 becomes isotropic over F_1. Let $q_1 := (q_0 \otimes F_1)_{an}$ be the anisotropic kernel of $q_0 \otimes F_1$ (i. e. q_0 considered as a form over F_1). Then $\dim q_1 < \dim q_0$ and $\dim q_1 \equiv$ and $\dim q_0 \bmod 2$.
Continuing this process we get fields $F = F_0 \subset F_1 \subset \ldots \subset F_h$ and quadratic forms q_i defined over F_i $(i = 0, \ldots, h)$. We stop if $\dim q_h \leq 1$. In particular we have $h = 0$ iff $\dim q_0 \leq 1$. The decreasing sequence $\dim q_0 > \dim q_1 > \ldots > \dim q_h$ stops at $\dim q_h = 1$ if $\dim q_0$ is odd and at $\dim q_h = 0$ (i. e. $q_h = 0$) if $\dim q_0$ is even. In this case the preceding form q_{h-1} is a scalar multiple of some Pfister form $\rho \in P_d(F_{h-1})$.

(8) **Definition**

(a) Let q be any quadratic form over F, let q_0 be its anisotropic kernel. The number $h(q) := h(q_0)$ is called the "height" of q (over F).

(b) If $\dim q$ is even and $h(q) > 0$ then the anisotropic Pfister form $\rho \in P_d(F_{h-1})$ is called the "leading form" of q.
(c) The (Knebusch) "degree" of q is defined as follows:
If $\dim q$ is odd then $\deg q := 0$.
If $q \neq 0$ and $\dim q$ is even then $\deg q$ is the number d occurring in part (b).
If $q = 0$ then $\deg 0 := \infty$.
We can now define the Knebusch ideals:

(9) $J_n := J_n F = \{q \in WF : \deg q \geq n\}$

The main result of Knebusch reads:

(10) The sets J_n $(n = 0, 1, 2, \ldots)$ are ideals of $W = WF$.
They satisfy $I^n \subset J_n$ and $I^m J_n \subset J_{m+n}$ for all $m, n \geq 0$. Furthermore we have:

$$J_1 = I^1 \ , \ J_2 = I^2 , J_3 = \{q \in W : e_0(q) = e_1(q) = e_2(q) = 0\}$$

More details can be found in the joint paper [AK, 1978] and in recent papers by Kahn and others. But before Voevodsky it was still open whether $J_n = I^n$ for all n and F. See section 6.1 for this result.

4.2 Progress in K-theory

The most influential paper after Milnor's own work is of course the 6 pages paper "On the norm residue symbol of degree 2" of Merkurjev [Me 1, 1981]. He proves:

(11) $h_2 : k_2 F \longrightarrow H^2 F$ is an isomorphism for all fields F of characteristic different from 2.
Essential steps for the proof are:
(i) A result of Suslin: If $h_2 F$ is bijective and $h_2 F(\sqrt{a})$ is surjective then $h_2 E$ is bijective for the function field $E := F(x, \sqrt{a(x^2 - b)})$ of the conic $q =< 1, -a, ab >$
(But Suslin used $K_2/2K_2$ where K_2 is Quillen's group K_2! So one has to know that this group coincides with our k_2)
(ii) The sequence $\dot{F} \xrightarrow{\nu} k_2 F \xrightarrow{\iota} k_2 F(\sqrt{a}) \xrightarrow{\mu} k_2 F$ is exact.
Here ν is the map $b \mapsto \{a\} \cdot \{b\}$ for $b \in \dot{F}$, ι is induced from the injection $i_{F(\sqrt{a})/F} : F \to F(\sqrt{a})$, and μ is induced from the norm map $N_{F(\sqrt{a})/F} : F(\sqrt{a}) \to F$ in the following non-trivial way:
If $t \in \dot{F}$, then $\mu(\{t, x + y\sqrt{a}\}) = \{t, x^2 - ay^2\}$, if $qy \neq 0$ then

$$\mu(\{p + q\sqrt{a}, x + y\sqrt{a}\}) = \left\{\tfrac{py - qx}{y}, x^2 - ay^2\right\} + \left\{p^2 - aq^2, \tfrac{xq - yp}{q}\right\}$$

The proof of this simple looking statement requires the use of function fields of high transcendence degree (in order to create a generic situation) and some ingenious specialization arguments.
Later Arason [A 2, 1984] gave a more elementary proof of the equivalent result that $\bar{e}_2 : \bar{I}^2 \to H^2$ is an isomorphism. It only uses the results of [A 1] and, of course, some specialization arguments similar to those of Merkurjev.

Further remarkable results of the eighties are the following:

(12) Kato's work for char $F = 2$ [Kat 1, 1982]:
Here one has to distinguish between symmetric bilinear forms over F which form a Witt ring $W = WF$ with fundamental ideal I, and (regular) quadratic forms over F which form a W-module W_q with subgroup $I_q = I \cdot W_q$ of index 2. Another change has to be made on the cohomological side since the ordinary cohomology groups $H^n F$ vanish for $n > 1$.
The H^n have to be replaced by certain factor groups which are derived from Ω^n, the n-th exterior power of the absolute differential module $\Omega = \Omega^1_{F/\mathbb{Z}}$.
For more details see [Kat 1] or [Ba].

(13) Existence of the invariants e_n for special fields F:
In a series of 6 joint papers published between 1984 and 1989 Arason-Elman-Jacob study the existence of the homomorphisms $e_n : I^n \longrightarrow H^n$ (for all n) under some additional assumptions on the ground field F. For instance they prove this and the bijectivity of the induced homomorphisms $\bar{e}_n : \bar{I}^n \longrightarrow H^n$ for all fields F which are of transcendence degree ≤ 4 over an algebraically closed subfield F_0 or of transcendence degree ≤ 3 over a real closed subfield F_0. See [AEJ 1] and [AEJ 2].

(14) Existence of e_4 and e_5 for all fields F:
Of course there have also been attempts to prove the bijectivity of $h_n : k_n \longrightarrow H^n$ and/or the existence of e_n for small $n = 3, 4, \ldots$ but without any assumptions on the field F. Let me state the results in chronological order without going into details:
Rost [R 1, 1986] and independently Merkurjev-Suslin [MS 2, 1990] (this paper was also written in 1986) proved that h_3 (hence also s_3 and $\bar{e}_3$) is an isomorphism. Jacob-Rost [JR, 1989] and independently Szyjewski [Sz, 1990] proved the existence of e_4 (Szyjewski calls this the "fifth invariant" of quadratic forms!).
In an unpublished paper Rost claims the existence of e_5 and the bijectivity of $\bar{e}_4$ for all fields F (char $F \neq 2$ of course). But he also points out that his methods are not powerful enough to go further.

5 Some remarks about Voevodsky's work and the Bloch-Kato Conjecture

As this is a survey for non-specialists and as I myself am not an expert for the modern development I can give only a very vague impression of the vast and powerful methods of Voevodsky. The main idea consists in the construction of a "homotopy theory for algebraic varieties". This includes:

- New categories, e. g. model category, homotopy category, triangulated categories
- New topologies, e. g. Nisnevich topology, qfh-topology

[The Nisnevich topology is finer than the "classical" Zariski topology of algebraic varieties but coarser than etale (= finite and everywhere unramified) topology, the qfh(= quasi-finite-henselian)-topology is finer than etale topology]

- Algebraic cobordism

- Motivic cohomologies (which were conjectured by Beilinson 1987) and their relation to etale cohomology
- "Rost motives" of "Pfister neighbors"

$$q := << a_1, \ldots, a_{n-1} >> + < -a_n >$$

[A motive is a pair (X, p) where X is an algebraic variety and $p \in End(X)$ is a projector: $p^2 = p$].
- Theorems à la "Hilbert 90" for various situations of K-groups and cohomology groups.

The "proof" of the second Milnor Conjecture $Q2$ is outlined in the preprint [V] of Voevodsky, the "proof" of the first Milnor Conjecture $Q1$ will be outlined in the preprint [OVV] of Orlov-Vishik-Voevodsky which was originally announced in 1996 and again announced under a more precise title in 1998 but which was not yet available in July 1999.
A word of warning must be said about these papers whence I put inverted commas on the word "solved" in the Introduction and the word "proof" above: They depend on some results which are not yet written or not yet checked carefully. [For instance it seems that they use a claim on the existence and expected properties of certain cohomology operations in motivic cohomology which have been proved in some other cohomology theory.]

For more details I refer in addition to the following excellent survey articles (written by experts and/or coauthors of Voevodsky): Levine [Le, 1997], Friedlander [F, 1997], Kahn [Kah2, 1997], Morel [Mo, 1998].

There is a very natural generalization of Milnor's second conjecture Q 2 which I want to describe shortly. Let F be an arbitrary field, let m be a (fixed) natural number prime to char F.
The exact sequence

$$1 \longrightarrow \mu_m \longrightarrow \dot{F}_s \overset{x \mapsto x^m}{\longrightarrow} \dot{F}_s \longrightarrow 1$$

and Hilbert's theorem 90 give isomorphisms

$$\dot{F}/\dot{F}^m \longrightarrow K_1 F/m K_1 F \longrightarrow H^1(\Gamma, \mu_m)$$

$$a \bmod \dot{F}^m \mapsto l(a) \bmod m \mapsto : (a)$$

The cup product in the cohomology theory of groups induces homomorphisms

$$h_{n,m} : K_n F/m K_n F \longrightarrow H^n(\Gamma, \mu_m^{\otimes n})$$

$$l(a_1) \cdot \ldots \cdot l(a_n) \bmod m \mapsto (a_1) \cup \ldots \cup (a_n)$$

for all $n \geq 0$ (norm residue maps mod m)

[Here $\mu_m = \{ x \in \dot{F}_s : x^m = 1 \}$ is the group of m-th roots of unity and $\mu_m^{\otimes n}$ is the n-fold tensor product of μ_m considered as a (multiplicative) Γ-module. By definition $\mu_m^{\otimes 0} = \mathbb{Z}/m\mathbb{Z}$]

Bloch-Kato Conjecture (1979)
$h_{n,m}$ is an isomorphism for all F, m (as above) and n.

It can be shown that this conjecture follows (for any m) if it could be proved for all prime numbers $m = p$ ($p \neq$ char F). Furthermore the following cases are known to be true: $n = 2$, m arbitrary [MS 1 and Me 2, 1983], n arbitrary, m = power of 2 [V, 1996]

For more details and some related results and conjectures see [Me 3, 1992]. It seems that the main problem for the case $m = p \neq 2$ is the lack of good varieties which could replace the Rost motives mentioned above. On the other hand the Bloch-Kato Conjecture would have many applications in number theory.

6 Applications

In this last section I describe some new results which rely at least partially on the positive solution of the Milnor Conjectures or on other statements in [V] or [OVV].

1. **The Knebusch Conjecture $J_n = I^n$** (see section 4.1)
   B. Kahn has shown me that this conjecture follows almost immediately from a result in [OVV]. The proof goes as follows:
   By induction on n we may assume that $J_k = I^k$ for $k \leq n$ and hence $J_{n+1} \leq I^n$. Let $q \in J_{n+1}$. Changing the form q modulo I^{n+1} we may assume $q = \sum_{i=1}^{r} \pm q_i$ with $q_i \in P_n F$ (compare (1) in section 4). Now we use induction on r. Then we can suppose
   $q \otimes F(q_r) \in I^{n+1} F(q_r)$.
   Let $q_r = \ll a_1, \ldots, a_n \gg$, let $\omega = \{a_1\} \cdot \ldots \cdot \{a_n\} \in k_n F$.
   By [OVV] we have $\ker(k_n F \to k_n F(q_r)) = \omega \cdot k_0 F$ and $\ker(\bar{I}^n F \to \bar{I}^n F(q_r)) = q_r \cdot \bar{I}^0 F$. Hence $q \equiv 0$ or $q \equiv q_r \ mod\ I^{n+1}$.
   But the second case is impossible since $deg\, q_r = n$ (if $q_r \neq 0$).
   Therefore $q \in I^{n+1}$ and $J_{n+1} = I^{n+1}$.
   Compare the paper [AB] of Aravire-Baeza (1999).
2. **The Marshall Conjecture and Lam's Open Problem *B***
   We need a few preliminary remarks about real fields and signatures:
   A field F is called (formally) *real* if -1 is not a sum of squares in F, otherwise F is called *nonreal* and the least number $s = s(F)$ such that
   $-1 = e_1^2 + \ldots + e_s^2$ with $e_i \in F$
   is called the *level* (in German: Stufe) of F.
   The *Pythagoras number* $p = p(F)$ of a field F is the least natural number such that every sum of squares in F can be rewritten as a sum of p squares (if such a number exists, otherwise we put $p(F) = \infty$). For nonreal fields the Pythagoras number of F is not very interesting because we have either
   char $F = 2$, $\sum_1^n a_i^2 = (\sum_1^n a_i)^2$ hence $s(F) = p(F) = 1$
   or *char* $F \neq 2$, $a = (\frac{a+1}{2})^2 + (-1)(\frac{a-1}{2})^2$ for every $a \in F$,
   hence $s(F) \leq p(F) \leq s(F) + 1$
   A real field F is called *pythagorean* if $p(F) = 1$.

Such fields can be rather complicated because they can have many orderings α. For a n-fold form $q = << a_1, \ldots, a_n >> = < 1, -a_1 > \cdot \ldots \cdot < 1, -a_n >$ over F we immediately see that

$$sign_\alpha q = \begin{cases} 0 & \text{at least one } a_i > 0 \\ \text{if} & \text{w.r.t. } \alpha \\ 2^n & \text{all } a_i < 0 \end{cases}$$

This implies that $2^n \mid sign_\alpha q$ for all $q \in I^n F$ and all orderings α of F. Marshall's conjecture asks for the converse:

(MC) Let F be a (real) pythagorean field, let $q \in WF$ be a quadratic form such that $2^n \mid sign_\alpha q$ for all orderings α of F. Then $q \in I^n F$. (See [Ma]).

The generalisation of this conjecture to an arbitrary real field F is known as Lam's Open Problem B:

(B) Let $q \in WF$ be such that $2^n \mid sign_\alpha q$ for all orderings α of F. Then $q \in I^n F + W_t F$ where $W_t F = \{q' \in WF : sign_\alpha q' = 0 \text{ for all } \alpha\}$ is the torsion subgroup of WF. (See [L 2])

(MC) has been proved by Dickmann-Miraglia [DM, 1998].

(B) has been proved by Monnier [Mon, 1999] under the additional assumption $v(F) \leq 3$ where the v-invariant is defined by $v(F) = \inf\{k : I^k F \cap W_t F = 0\}$.

A full proof of (B) which is easier than the proofs above has been shown to me by Arason. It will appear in a joint paper [AE] of Arason and Elman. Earlier results on (B) can be found in Krüskempers paper [Kr 1, 1990].

3. **Annihilators and presentation for I^n**

Let $0 \neq \omega \in P_k$ be a k-fold Pfister form ($k \in \mathbb{N}_0$). It is well known that the annihilator ideal $Ann\,\omega := \{q \in W : \omega \cdot q = 0\}$ is generated by binary forms $q = < 1, -t >$ with $t \in \dot{D}_F(\omega)$ (see [Sc 2, Ch 2, Thm 10.13]).

The corresponding question for the *ideal* I^n instead of the full Witt ring W amounts to the equality

(a) $\quad I^n \cap Ann\,\omega = I^{n-1} \cdot Ann\,\omega \qquad (n \geq 1)$

Similarly the question for a "natural presentation" of the *subgroup* $I^n \subset W$ by generators and relations which was already mentioned in section 3 leads to the following statements:

(b_1) I^1 is generated by the elements $\ll a \gg \in P_1 \quad (a \in \dot{F})$ with defining relations

$$\ll a \gg + \ll b \gg = \ll a + b \gg + \ll ab(a+b) \gg$$

(b_n) For $n \geq 2$ the subgroup I^n is generated by the elements $\ll a_1, \ldots, a_n \gg \in P_n$ with defining relations

$$\ll ab, c \gg \cdot\omega + \ll a, b \gg \cdot\omega = \ll ac, b \gg \cdot\omega + \ll a, c \gg \cdot\omega \qquad (a, b, c \in \dot{F}, \quad \omega \in P_{n-2})$$

Statement (b_1) was of course known before the work of Voevodsky and his coauthors. Results (a) and (b_n) will be proved in the forthcoming paper [AE]

mentioned just before. The clever proofs proceed in the following three steps:
1) We may suppose that the field F has finite transcendence degree d over its prime field F_0. Then $v(F) < \infty$, i.e. I^k is torsion-free for large k (see the next subsection 6.4). If F is real (which implies $F_0 = \mathbb{Q}$) then we also have

$$st(F) \leq d + 1 < \infty$$

where st is the "stability index" which was defined and studied in detail by L. Bröcker (1974).
2) Statements (a) and (b_n) are true in the so-called "stable range", i.e. for $n \geq \max\{v(F), st(F)\}$. This is trivial for nonreal F (since then $I^n = 0$) and relatively easy for real F. [Compare the interesting papers of Krüskemper (1990 and 1994) on these and similar questions around the Milnor Conjectures.]
3) Using results from [OVV] it is possible to do a "reverse induction" and thereby prove (a) and (b_n) successively for exponents

$$n\,(large),\ n-1,\ \ldots\ 2\,.$$

4. **Pythagoras numbers of finitely generated fields**

Let me start with a theorem which I proved in my paper [P 2, 1967]:
(a) Let F be a field of transcendence degree d over a real closed field R (e.g. $R = \mathbb{R}$). Then

$$p(F) \leq 2^d\,.$$

For a simplified proof see [Sc 2, Ch 4, Theorem 2.1] or [P 3, Ch 6, Theorem 3.3].
A much deeper question is whether the Pythagoras number $p(F)$ is finite for every field F which is finitely generated over its prime field F_0. This is clearly true if $F_0 = \mathbb{F}_p$ is finite since

$$s(F) \leq s(F_0) \leq 2, \text{ hence } p(F) \leq s(F) + 1 \leq 3\,.$$

For $F_0 = \mathbb{Q}$ the decisive step has been taken in a paper of Colliot-Thélène and Jannsen [CTJ, 1991]. They reduce the above problem to the Milnor Conjectures and a conjecture of Kato [Kat 2, 1986] which claims a certain higher-dimensional "Local-Global-Principle" for the cohomology group $H^{d+2}F$ where d is the transcendence degree of F over $F_0 = \mathbb{Q}$.
This conjecture of Kato has been proved by Kato for $d = 1$ and by Jannsen for $d = 2$ and "in principle" for all d (but Colliot-Thélène has informed me that details of the proof are missing for $d > 2$).
Fortunately Kato's conjecture can be totally avoided if we are satisfied with a slightly weaker estimate for $p(F)$. Such a proof has been shown to me by Arason. It runs as follows:
The field $F(\sqrt{-1})$ has cohomological dimension at most $d + 2$ (see [Se 2 (5th ed.)] ch. II, Propositions 11 and 13),

$$\text{hence } H^{n+1}F(\sqrt{-1}) = 0 \text{ for } n \geq d + 2\,.$$

By the Milnor Conjectures this implies

$$I^{n+1}F(\sqrt{-1}) = 0 \qquad \text{for } n \geq d + 2$$

From this result it follows that

(b) $p(F) \leq 2^{d+2}$

(See e.g. [P 3], ch. 6, Theorem 3.3]

This estimate is clearly sharp for $d = 0$ as we have $p(\mathbb{Q}) = 4$ by the theorem of Euler-Lagrange. For $d = 1$ Colliot-Thélène has shown that $p(F) \leq 7$ (see [CTJ]) and this has been improved to $p(F) \leq 6$ by Pop (unpublished). Presumably we have $p(F) \leq 5$ for $d = 1$, and this would be the best possible bound for $\mathbb{F} = \mathbb{Q}(t)$. For $d \geq 2$ we have the better estimate $p(F) \leq 2^{d+1}$ provided that Kato's conjecture holds.

For more details see [CTJ] and [P 3, ch. 7].

5. ***Mod* 2 cohomology**

The solution of the Milnor Conjecture $Q2$ allows the computation of the "*mod* 2 cohomology ring"

$$H^*G = \bigoplus_{n=0}^{\infty} H^n(G, \mathbb{Z}/2\mathbb{Z})$$

for some other groups G instead of Galois groups, e.g. for the "linear" groups

$$G = \mathbb{Z},\ GL(\mathbb{Z}),\ SL(\mathbb{Z}),\ St(\mathbb{Z}).$$

Here $GL(\mathbb{Z}) = \varinjlim GL(n, \mathbb{Z})$ is the infinite general linear group over $\mathbb{Z}$, and similar definitions hold for the special linear group $SL(\mathbb{Z})$ and the Steinberg group $St(\mathbb{Z})$. I refer to the papers of Rognes-Weibel (1997) and Arlettaz-Mimura-Nakahata-Yagita (1999).

Another interesting application of the Milnor Conjectures is given in the recent paper of Elman-Lum (1999). It concerns the cohomological 2-dimension $cd_2(F)$ of a field F.

Furthermore the Milnor Conjecture $Q2$ would imply that any (C_r)-field F in the sense of Tsen-Lang has cohomological 2-dimension $cd_2(F) = cd_2(\Gamma) \leq r$, see [Se 2, 5th ed., p. 89].

6. **Galois groups**

In contrast to the graded Witt ring $\widehat{W}F$ the original Witt ring WF of F is not fully determined by the absolute Galois group Γ of F. This can trivially be seen for finite fields $F = \mathbb{F}_q$ which all have $\Gamma = \widehat{\mathbb{Z}}$ whereas

$$\begin{aligned} WF &= \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} && \text{for } q \equiv 1 \ mod\, 4 \\ WF &= \mathbb{Z}/4\mathbb{Z} && \text{for } q \equiv -1 \ mod\, 4 \end{aligned}$$

(q is an odd prime power).

What else is needed from the Galois theory of F in order to determine the Witt ring WF (up to isomorphism)? A precise answer can be found in the paper [MiSp] of Mináč and Spira (1996): One has to know the level $s = s(F)$ and the Galois group Γ^3 of $F^{(3)}/F$ where $F^{(3)}$ is a specific extension of F which sits in between the composition of all quadratic extensions of F and the quadratic closure F_q of F.

Conversely one can also deduce results about generators and relations for pro-2-Galois groups Γ_E of fields E, $F \subset E \subset F_q$. See the paper of Gao-Mináč (1997).

References

[A1] *J.K. Arason:* Cohomologische Invarianten quadratischer Formen. J. Algebra **36**, 448–491 (1975).

[A2] *J.K. Arason:* A proof of Merkurjev's theorem. Can. Math. Soc. Conf. Proc, vol. **4**, 121–130 (1984).

[AE] *J.K. Arason, R. Elman:* Powers of the Fundamental Ideal in the Witt Ring. To appear.

[AEJ1] *J.K. Arason, R. Elman, B. Jacob:* The graded Witt ring and Galois Cohomology. I. Can. Math. Soc. Conf. Proc., Vol. 4, 17–50 (1984).

[AEJ2] *J.K. Arason, R. Elman, B. Jacob:* On quadratic forms and Galois cohomology. Rocky Mt. J. Math. **19**, 575–588 (1989).

[AK] *J.K. Arason, M. Knebusch:* Über die Grade quadratischer Formen. Math. Ann. **234**, 167–192 (1978).

[AP] *J.K. Arason, A. Pfister:* Beweis des Krullschen Durchschnittsatzes für den Wittring. Invent. math. **12**, 173–176 (1971).

[AB] *R. Aravire, R. Baeza:* A note on generic splitting of quadratic forms. Comm. in Algebra **27**, 3473–3477 (1999).

[AMNY] *D. Arlettaz, M. Mimura, K. Nakahata, N. Yagita:* The *mod* 2 cohomology of the linear groups over the ring of integers. Proc. AMS **127**, 2199-2212 (1999).

[At] *M.F. Atiyah:* K-theory. Benjamin, New York 1967.

[Ba] *H. Bass:* John Milnor the Algebraist, p. 45–84 in: *Topological Methods in Modern Mathematics.* A Symposium in Honor of John Milnor's Sixtieth Birthday. Publish or Perish Inc., Houston/USA 1993.

[Be] *A.A. Belskii:* Cohomological Witt rings. (in Russian) Math. USSR Izvestija **2**, 1101–1115 (1968).

[Br] *R. Brauer:* Über die algebraische Struktur von Schiefkörpern. J.r.a. Math **166**, 241–252 (1932) = Coll. Papers I, no 13.

[Brö] *L. Bröcker:* Zur Theorie der quadratischen Formen über formal reellen Körpern. Math. Ann. **210**, 233–256 (1974).

[CE] *H. Cartan, S. Eilenberg:* Homological Algebra. Princeton Univ. Press 1956.

[Ch] *C. Chevalley:* The algebraic theory of spinors. Columbia Univ. Press, New York 1954.

[Cl] *W.K. Clifford:* Application of Grassmann's extensive algebra. Am. J. Math **1**, 350–358 (1878) = Math. Papers XXX.

[CTJ] *J.-L. Colliot-Thélène, U. Jannsen:* Sommes de carrés dans les corps de fonctions. C.R. Acad. Sci. Paris **312**, 759–762 (1991).

[De] *A. Delzant:* Définition des classes de Stiefel-Whitney d'un module quadratique sur un corps de charactéristique différent de 2. C.R. Acad. Sci. Paris **255**, 1366–1368 (1962)

[DM] *M. Dickmann, F. Miraglia:* On quadratic forms whose total signature is zero mod 2^n. Solution to a problem of M. Marshall. Invent math. **133**, 243–278 (1998).

[Dr] *P.K. Draxl:* Skew Fields. Cambridge Univ. Press 1983.

[Ei] *M. Eichler:* Quadratische Formen und orthogonale Gruppen. Springer, Berlin 1952.

[EL1] *R. Elman, T.Y. Lam:* Pfister forms and K-theory of fields. Bull. AMS **77**, 971–974 (1971).

[EL2] *R. Elman, T.Y. Lam:* Quadratic forms over formally real fields and pythagorean fields. Amer. J. of Math. **94**, 1155–1194 (1972).

[ELum] *R. Elman, C. Lum:* On the cohomological 2-dimension of fields. Comm. in Algebra **27**, 615–620 (1999).

[EKLV] *H. Esnault, B. Kahn, M. Levine, E. Viehweg:* The Arason invariant and mod 2 algebraic cycles. J. AMS **11**, 73–118 (1998).

[F] *E.M. Friedlander:* Motivic complexes of Suslin and Voevodsky. Sém. Bourbaki 1996/97, exp. **833**, 355–378.

[GM] *W. Gao, J. Mináč:* Milnor's Conjecture and Galois Theory I. Fields Inst. Commun **16**, AMS 1997.

[H] *D.W. Hoffmann:* On the dimensions of anisotropic quadratic forms in I^4. Invent. math. **131**, 185–198 (1998).

[I] *O.T. Izhboldin:* On the nonexcellence of field extensions $F(\pi)/F$. Doc. Math. **1**, 127–136 (1996) (electronic).

[IK] *O.T. Izhboldin, N. Karpenko:* Some new examples in the theory of quadratic forms. Preprint ISSN 1435–1188 Univ. Münster 1998.

[JR] *B. Jacob, M. Rost:* Degree four cohomological invariants for quadratic forms. Invent. math. **96**, 551-570 (1989).

[Kah1] *B. Kahn:* A descent problem for quadratic forms. Duke Math. J. **80**, 139–155 (1995).

[Kah2] *B. Kahn:* La Conjecture de Milnor d'après V. Voevodsky. S. Bourbaki 1996/97, exp. **834**, 379–418.

[Kat1] *K. Kato:* Symmetric bilinear forms, quadratic forms and Milnor K-theory in characteristic two. Invent. math. **66**, 493–510 (1982).

[Kat2] *K. Kato:* A Hasse principle for two-dimensional global fields. J.r.a. Math. **366**, 142–181 (1986).

[Ke] *I. Kersten:* Brauergruppen von Körpern. Vieweg, Wiesbaden 1990.

[Kn1] *M. Knebusch:* Runde Formen über semilokalen Ringen. Math. Ann. **193**, 21–34 (1971).

[Kn2] *M. Knebusch:* Generic splittings of quadratic forms I. Proc. London Math. Soc. **33**, 65–93 (1976).

[Kn3] *M. Knebusch:* Generic splittings of quadratic forms II. ibid. **34**, 1–31 (1977).

[KMRT] *M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol:* The Book of Involutions. AMS Publ., Providence 1998.

[Kr1] *M. Krüskemper:* On real local-global principles. Math. Zeitschr. **204**, 145–151 (1990).

[Kr2] *M. Krüskemper:* On annihilators in graded Witt rings and in Milnor's K-theory. Contemp. Math. **155**, 307–320, AMS 1994.

[L1] *T.Y. Lam:* The algebraic theory of quadratic forms. Benjamin, Reading/Mass. 1973.

[L2] *T.Y. Lam:* Ten Lectures on Quadratic Forms over Fields. Queen's Papers in Pure and Appl. Math., No 46, 1–102. Kingston/Ont. 1977.

[Le] *M. Levine:* Homology of algebraic varieties: An introduction to the works of Suslin and Voevodsky. Bull. AMS **34**, 293–312 (1997).

[Ma] *M. Marshall:* A reduced theory of quadratic forms. Queen's Papers in Pure and Appl. Math., No. 46, 569–579. Kingston/Ont. 1977.

[Me1] *A.S. Merkurjev:* On the norm residue symbol of degree 2 (in Russian). Dokl. Acad. Nauk. SSSR **261**, 542–547 (1981). English transl.: Soviet Math. Doklady **24**, 546–551 (1981).

[Me2] *A. S. Merkurjev.* K_2 of fields and the Brauer group. AMS Contemp. Math. **55**, 529–546 (1983).

[Me3] *A.S. Merkurjev:* Algebraic K-Theory and Galois Cohomology. First European Congress of Math., Vol. II, 243–255 (1992). Birkhäuser, Basel 1994.

[MS1] *A.S. Merkurjev, A.A. Suslin:* K-cohomology of Severi-Brauer varieties and the norm-residue homomorphism (in Russian). Izv.Acad.Nauk. USSR **46**, 1011–1046 (1982). English transl.: Math. USSR Izv. **21**, 307–340 (1983).

[MS2] *A.S. Merkurjev, A.A. Suslin:* The norm residue homomorphism of degree 3 (in Russian). Izv. Acad. Nauk. SSSR **54**, 339–356 (1990). English transl.: Math. USSR Izv. **36**, 349–368 (1991).

[Mi1] *J. Milnor:* On simply connected 4-manifolds. Symp. Int. de Top. Alg. Mexico 1956, 122–128 (1958).

[Mi2] *J. Milnor:* Algebraic K-theory and quadratic forms. Invent. math. **9**, 318–344 (1970).

[Mi3] *J. Milnor:* Introduction to algebraic K-theory. Annals of Math. Studies **72**, Princeton Univ.Press 1971.

[MH] *J. Milnor, D. Husemoller:* Symmetric bilinear forms. Springer, Berlin 1973.

[MiSp] *J. Mináč*, M. Spira: Witt rings and Galois groups. Annals of Math. **144**, 35–60 (1996).

[Mon] *J.-P. Monnier:* On Lam's conjecture concerning signatures of quadratic forms. To appear in Archiv der Math.

[Mo] *F. Morel:* Voevodsky's proof of Milnor's Conjecture. Bull. AMS **35**, 123–143 (1998).
[OVV] *D. Orlov, A. Vishik, V. Voevodsky:* Motivic cohomology of Pfister quadrics and Milnor's conjecture on quadratic forms. Preprint.
[P1] *A. Pfister:* Quadratische Formen in beliebigen Körpern. Invent. math. **1**, 116–132 (1966).
[P2] *A. Pfister:* Zur Darstellung definiter Funktionen als Summe von Quadraten. Invent. math. **4**, 229–237 (1967).
[P3] *A. Pfister:* Quadratic Forms with Applications to Algebraic Geometry and Topology. Cambridge Univ. Press 1995.
[P4] *A. Pfister:* On the Milnor Conjectures. History, Influence, Applications. Preprint Nr. 8 (1999) FB Math., Univ. Mainz.
[Q] *D. Quillen:* Higher algebraic K-theory I. Springer Lecture Notes **341**, 85–147 (1973).
[RW] *J. Rognes, C. Weibel:* Two-primary algebraic K-theory of rings of integers in number fields. Preprint 1997, http://math.uiuc.edu/K-theory/0220/ .
[R1] *M. Rost:* Hilbert's theorem 90 for K_3^M for degree-two extensions. Preprint, Univ. Regensburg 1986.
[R2] *M. Rost:* Chow groups with coefficients. Doc. Math. **1**, 319–393 (1996) (electronic).
[R3] *M. Rost:* The motive of a Pfister form. Preprint 1998.
[Sc1] *W. Scharlau:* Quadratische Formen und Galois-Cohomologie. Invent. math. **4**, 238–264 (1967).
[Sc2] *W. Scharlau:* Quadratic and Hermitian Forms. Springer, Berlin 1985.
[Sc3] *W. Scharlau:* On the history of the algebraic theory of quadratic forms. To appear in: Proceedings of the Dublin Conference on Quadratic Forms and their Applications (July 5–9, 1999), AMS Contemporary Mathematics.
[Se1] *J.-P. Serre:* Corps locaux. Hermann, Paris 1962.
[Se2] *J.-P. Serre:* Cohomologie galoisienne. Springer Lecture Notes **5** (1964) [5th edition: Galois Cohomology. Springer, Berlin 1996].
[Sp] *T.A. Springer:* On the equivalence of quadratic forms. Indag. math. **21**, 241–253 (1959).
[Su1] *A.A. Suslin:* Algebraic K-Theory. In: Algebra, Topology, Geometry. vol. **20**, 71–152. Acad. Nauk SSSR, Moscow 1982 (in Russian).
[Su2] *A.A. Suslin:* On the K-theory of algebraically closed fields. Invent. math. **73**, 241–245 (1983).
[Su3] *A.A. Suslin:* Algebraic K-theory of fields. Proc.Int.Congr. Math. Berkeley 1986, vol. I, 222–244.
[Sw] *R. Swan:* Algebraic K-Theory. Springer Lecture Notes **76** (1968).
[Sz] *M. Szyjewski:* The fifth invariant of quadratic forms (in Russian). Algebra Anal. **2**, 213–234 (1990). English transl.: Leningrad Math. J. **2**, 179–198 (1991).
[T] *J. Tate:* Relations between K_2 and Galois Cohomology. Invent. math. **36**, 257–274 (1976).
[V] *V. Voevodsky:* The Milnor conjecture. Preprint 1996.
[W] *E. Witt:* Theorie der quadratischen Formen in beliebigen Körpern. J.r.a. Math. **176**, 31–44 (1937) = Coll. Papers, no 1.

Albrecht Pfister
Johannes-Gutenberg-Universität
Fachbereich Mathematik
Saarstraße 21
D-55099 Mainz
Germany
pfister@mat.mathematik.Uni-Mainz.de

(*Eingegangen 16.12.99*)

Buchbesprechungen

Bense, M., Ausgewählte Schriften in vier Bänden. Band 2: Philosophie der Mathematik, Naturwissenschaft und Technik, Stuttgart-Weimar: J. B. Metzler 1998, 480 S., DM 78,–

Die vierbändige Ausgabe der inzwischen vollständig erschienenen „Ausgewählten Schriften" Max Benses enthält in der Folge der Bände Benses frühere Beiträge zur Philosophie, Schriften zur Philosophie der Mathematik, Naturwissenschaft und Technik, ästhetische und semiotische Bücher sowie poetische Texte. Als Herausgeberin fungiert Elisabeth Walter; von ihr stammen auch die in den ersten Band mit aufgenommenen „Erläuterungen" zu den vier Bänden, die Gestaltung der Anmerkungen und der Register.

Der vorliegende Beitrag ist ausschließlich Band 2 gewidmet, in dem Benses Dissertation „Quantenmechanik und Daseinsrelativität" aus dem Jahre 1938, das zweibändige Werk „Konturen einer Geistesgeschichte der Mathematik", welches im Jahre 1951 abgeschlossen war, und die Abhandlung „Kybernetik oder die Metatechnik der Maschine" aus dem Jahre 1953, allesamt Publikationen, die seit Jahren vergriffen sind, einen Neudruck erfahren. Der Band wird von Elisabeth Emter eingeleitet, wobei die Autorin den biographisch anspielungsreichen Untertitel „Von Hause aus Physiker und Mathematiker. Der Philosoph Max Bense" wählt.

Bense war Philosoph und Wissenschaftstheoretiker. Platon folgend forderte er zeitlebens Mathematik als unersetzlichen Bestandteil des Philosophiestudiums. Er sah sich als Vermittler zwischen Natur- und Geisteswissenschaften, zwischen Technik und Philosophie. Diese Vermittlerrolle ist aus den drei Themen des Bandes ersichtlich. Im Blick auf neuere Entwicklungen in der wissenschaftstheoretischen Diskussion um die Mathematik, allgemeine Prinzipien der Quantisierung, mathematische Aspekte der Ästhetik sowie Ausmaß und Grenzen der Informatik betreffend gewinnen die „Daseinsrelativität", die „Konturen" sowie die „Metatechnik" an Bedeutung. Zum Zeitpunkt des Erscheinens dieser Schriften gab es noch keine Quantengruppen und -wahrscheinlichkeiten, keine informations- oder fraktaltheoretische Ästhetik, auch keine gruppentheoretische Musiktheorie; das berühmte Buch N. Wieners über „Cybernetics" war gerade erschienen. Umso interessanter ist es, bei Bense über den Stand des Einblicks in die diesbezügliche Forschung bis zum Jahre 1953 zu lesen.

In der Schrift über „Daseinsrelativität" beruft sich Bense bei der Einordnung der Welle-Teilchen-Theorie der modernen Physik auf die Schelersche Idee der gestuften Daseinsrelativität. Aus diesem Bezug folgert er, daß die Quantenmechanik durch Verfeinerung der Experimente eine neue Stufe der Daseinsrelativität der physikalischen Gegebenheiten erklommen habe und damit die moderne Physik phänomenologisch-ontologisch unmittelbar an die klassische Physik anschließe.

In der Schrift über „Metatechnik", die ganz wesentlich von L. Couffignals Buch „Les Machines à Penser" beeinflußt ist, begründet Bense sein Kredo zugunsten der Verpflichtung des denkenden Menschen, sich der technisch veränderten Welt zu stellen und die technische Intelligenz als für die geistige Entwicklung zuständig anzuerkennen. Bense plädiert für Abgrenzung gegenüber den sogenannten Bedrohungen durch die technischen Errungenschaften und für Hinwendung zu den „Segnungen"der Technik. Der Mensch als technische Existenz erscheint ihm als eines der wichtigsten Themen einer zukünftigen philosophischen Anthropologie.

Auf etwa 300 der insgesamt ungefähr 500 Seiten des Buches sind die „Konturen" abgedruckt, denen sich detaillierter zu widmen uns lohnend erscheint. Im ersten Teil über „Die Mathematik und die Wissenschaften" finden wir zunächst Gedanken zur Geistesge-

schichte der Mathematik, im Anschluß daran eine kleine Stilgeschichte der Mathematik. Es folgt ein Kapitel über Mathematik und Philosophie, sodann eine über die Mathematisierung der Gegenstände der (Natur)wissenschaften. Schließlich liest man über den Geist des Laplace (den Laplaceschen Dämon) und in einem Nachwort über die Antimathematica und den abstrakten Denker. Der zweite Teil der „Konturen" hat „Die Mathematik in der Kunst (in den Künsten)" zum Thema. Wiederum geht es in einem ersten Kapitel um den Begriff des Stils, danach um die Beziehungen der Mathematik zur Literatur. Ein zentrales Kapitel handelt von der Mathematik der Ornamente. Im Anschluß folgt in fünf aufeinanderfolgenden Kapiteln eine historische Darstellung des mathematischen Denkens und dessen Einfluß auf die künstlerische Gestaltung: von der Rezeption Euklids in der Renaissance über Mathematik und Kunst im Barock und in der nachklassischen Zeit, über D'Alemberts und Diderots Bedeutung für die Geistesgeschichte der Mathematik bis schließlich hin zu Goethes Farbenlehre und die Theorie des Impressionismus als mathematisch orientierte wissenschaftliche Erkenntnisprojekte. Im letzten Kapitel wird die mathematische Struktur musikalischer Kompositionen von der Antike bis zu Ernst Kreneck behandelt. Im Nachwort über ästhetische Fragen greift Bense noch einmal die Leibnizsche Reduktion der künstlerischen Formen auf mathematische Formen geometrischen oder arithmetischen Ursprungs auf und stützt seine These, daß es eine Ästhetik zu entwerfen gelte, die „Geist auf Form und Form auf Mathematik zurückführe".

Bei Lektüre der Benseschen Schriften fällt auf, daß der Autor auf frühere Arbeiten recht selten und nur dann zurückgriff, wenn ihn interessierende innovative Entwicklungen einsetzten. So hat er die „Daseinsrelativität" aus dem Jahre 1938 erst wieder gegen Ende seines Lebens zitiert, in dem posthum herausgegebenen Buch „Die Eigenrealität der Zeichen". In dieser Schrift besinnt er sich des Schelerschen Nachlasses und weist auf eine Analogie zwischen dessen ontologischer Theorie daseinsrelativer Gegenstandsarten und dem inzwischen aus der Peirceschen Perspektive entwickelten semiotischen System der dreistelligen Zeichenrelationen hin.

Hätte Bense in späteren Jahren das Bedürfnis gespürt, auch seine „Konturen" auf den Stand neuerer Forschungen anzuheben, so hätte ihn Weyls „Symmetrie" aus dem Jahre 1952 zu Gebote gestanden, wenn es um genauere gruppentheoretische Begründungen von Symmetrien in der bildenden Kunst gegangen wäre. Aktuelle Beiträge zu diesem Thema wurden von H. Götze und M. Koecher am Beispiel der Architektur des Castel del Monte geleistet. Eine launig gerahmte, in der Substanz maßgebende Veröffentlichung von K.H. Hofmann aus dem Jahre 1990 über Symmetrie und Homogenität zeigt anhand der Biographien von E. Galois (1811–1832) und S. Lie (1842–1899) auf, wie der in der Geometrie endlicher Konfigurationen entstandene Symmetriebegriff zu einer neuen analytisch-topologischen Denkweise führte: zur Theorie der Transformationsgruppen. Dieser Fortschritt in der mathematischen Forschung kommt auch dem Umgang mit ästhetischen Fragen zugute. Gegenüber der bildenden Kunst bedurfte es im Bereich der Musiktheorie nach den Arbeiten von H. L. F. Helmholtz (1885) der mathematisch ausgerichteten Beiträge von M. Babbitt (1972) und von G. D. Halsey und E. Hewitt (1978), um eine wesentliche Vertiefung des Einwirkens der Gruppentheorie auf die Ästhetik der Musik zu erkennen, eine Vertiefung, die die „Konturen" Benses aus heutiger Sicht zu aktualisieren vermag. Sowohl die „Daseinsrelativität" als auch die „Konturen" und die „Metatechnik" fügen sich in das Repertoire der Quellen ein, aus dem jede auf den gegenwärtigen Stand gebrachte „Geistesgeschichte der Mathematik" gespeist wird. Heute wird der Akzent des Historischen durch den des Faktischen zu ersetzen sein. Die Rolle der Mathematik als ordnende Kraft des Universums wird etwa bei A. Jaffee technisch detaillierter beschrieben als es zur Zeit der Entstehung der Benseschen Schriften möglich war. Bense war sich in seiner letzten Schaffensperiode der hier angesprochenen Entwicklungen bewußt. Er benützte die Sprache der algebraischen Topologen in der von ihm entwickelten Semiotik, er

kannte die Grundzüge der Fraktalgeometrie und wandte sie in der Analyse von malerischen bzw. bildhauerischen Arbeiten an. Auch über Grundlagenfragen der Mathematik hielt er sich informiert. Nachweise für diese neuen Aspekte seines mathematisch orientierten Denkens findet der Leser in den zwei Anschlußbänden, insbesondere in Band 3 über Informationsästhetik.

Im vorliegenden Band 2 der „Ausgewählten Schriften" ist der leitende philosophische bzw. wissenschaftstheoretische Grundgedanke, daß nämlich Geist im wesentlichen Form sei, dem Denken der Rationalisten entlehnt. Das klassische Zeitalter der mathesis universalis mit seinen herausragenden Vertretern Descartes, Pascal und Leibniz haben Benses Arbeit und damit auch seine Darstellung der Geistesgeschichte der Mathematik beeinflußt. Bei seinen früheren Studien war ihm die Geistesverwandtschaft und persönliche Freundschaft mit Heinrich Scholz von größter Bedeutung. In den Vorbemerkungen zu den „Konturen" spricht Bense von seiner enzyklopädischen Gesinnung, wobei er sich geradezu als Rationalisten vorstellt. Nach Ansicht des Referenten steht jedoch in den vorliegenden Schriften die essayistische Gesinnung im Vordergrund. Manche der Kapitel der hier abgedruckten Bücher sind in sich geschlossene Essays über die Varianten des mathematisch-naturwissenschaftlichen Geistes. Als Folge dieser Deutung werden Wiederholungen verständlich.

Dem interessierten Leser werden Einführung bzw. Vertiefung ins Bensesche Werk in mannigfacher Weise leicht gemacht: Längst Vergriffenes liegt wieder vor, Zurückliegendes kann neu eingeordnet werden. Dem forschenden Mathematiker bietet sich die Gelegenheit, den geistesgeschichtlichen Hintergrund seiner Resultate zu erkennen. Der Wissenschaftshistoriker bzw. -theoretiker mag eine angemessen fundierte Orientierung auf das mathematische Denken erhalten. Dem künstlerisch arbeitenden Menschen eröffnet sich die Einsicht, daß der intellektuelle Anteil seiner Ideen methodisch (sprachlich) und inhaltlich (strukturell) mathematische Züge trägt. Für den Philosophen und Ästhetiker wird es zu einer Herausforderung, ausgehend von der mathesis universalis Mathematik, Naturwissenschaft und Künste zusammenzudenken unter dem Stichwort „Geist ist wesentlich Form".

Herausgeberin und Verlag verdienen Anerkennung ihres Engagements für die gelungene Aufbereitung einiger besonders tragfähiger Schriften Benses, die von des Autors starker Neigung zur Mathematik künden und dessen gefestigte Überzeugung vermitteln, daß überall dort, wo geistige Schöpfung aufleuchtet und der Präzisierung harrt, Mathematik zur Hand sein sollte.

Babbit, M.: Three essays on Schoenberg. In: Perspectives on Schoenberg and Stravinsky, Rev. (Boretz, B; Cone, E.T., eds.), New York 1972

Bense, M.: Die Eigenrealität der Zeichen. Aus dem Nachlaß herausgegeben von Elisabeth Walther. Agis-Verlag Baden-Baden 1992

Couffignal, L.: Les Machines à Penser. Collection l'Homme et la Machine, Les Editions de Minuit, Paris 1952

Götze, H.: Castel del Monte. Prestel-Verlag 1984

Halsey, G. D.; Hewitt, E.: Eine gruppentheoretische Methode in der Musiktheorie. Jber.d.Dt.Math.-Verein. **80** (1978) 151–207

Helmholtz, H. L. F.: On the Sensations of Tone (Übers. v. A.J. Ellis). 2nd engl. ed. London 1885. Repr. New York 1954

Hofmann, K. H. Symmetrie und Homogenität. In: Symmetry of Discrete Mathematical Structures and Their Symmetry Groups, pp. 151–168. A Collection of Essays (K.H. Hofmann, R. Wille, eds.) Heldermann Verlag Berlin 1990

Jaffee, A.: Ordering the Universe: The Role of Mathematics. SIAM Review Vol. **26**, No. 4(1984), 473–500

Koecher, M.: Castel del Monte und das Oktogon. In: Miscellanea mathematica (P. Hilton, F. Hirzebruch, R. Remmert eds.), pp. 221–233. Springer-Verlag Berlin, Heidelberg 1991

Weyl, H.: Symmetry. Princeton University Press 1952

Wiener, N.: Cybernetics, or Conrol and Communication in the Animal and the Machine. Actualités Sci. Ind., no. 1053. Hermann et Cie, Paris 1948

Tübingen H. Heyer

Borel, A., Automorphic Forms on SL (2, $\mathbb{R}$),, Cambridge University Press 1997, 192 S., £ 32.50

Ursprünglich wurden automorphe Formen als holomorphe oder meromorphe Funktionen auf der (offenen) oberen Halbebene $X \subseteq \mathbb{C}$ betrachtet, die gewisse Transformationseigenschaften bzgl. einer diskreten Untergruppe $\Gamma \subseteq G := \mathrm{SL}(2, \mathbb{R})$ besitzen. Später wurden diese Konzepte durch H. Maass, A. Selberg und W. Roelcke derart verallgemeinert, daß man Funktionen einschloß, die nicht notwendigerweise holomorph, dafür aber Eigenfunktionen des Laplace-Beltrami-Operators sind. In den 50er Jahren hat sich ein darstellungstheoretischer Standpunkt durchgesetzt, der Verallgemeinerungen auf allgemeinere Gruppen zugänglicher ist, und automorphe Formen als glatte Funktionen φ auf $\Gamma\backslash G$ (bzw. Γ-linksinvariante Funktionen auf G) betrachtet, die folgende Bedingungen erfüllen: Ist $K = \mathrm{SO}(2, \mathbb{R})$ und $\mathcal{C}$ der Casimiroperator der Lie-Algebra $g = \mathfrak{sl}(2, \mathbb{R})$, so liegen sowohl die durch Elemente von K rechtsverschobenen Funktionen als auch die Funktionen $\mathcal{C}^n.\varphi$, $n \in \mathbb{N}$, in einem endlichdimensionalen Unterraum. Zusätzlich fordert man eine gewisse Wachstumsbedingung.

In diesem Sinne ordnet sich die Theorie der automorphen Formen der harmonischen Analysis des homogenen Raums $\Gamma\backslash G$ unter. Dies ist der Standpunkt des vorliegenden Buches, das aus mehreren Vorlesungen entstanden ist, die der Autor in den letzten drei Jahrzehnten gehalten hat, zuletzt am Mathematischen Institut der Academia Sinica im Frühjahr 1993. Im Vorwort des Buches schreibt der Autor hierzu „Introduction to some aspects of the analytic theory of automorphic forms on $\mathrm{SL}_2(\mathbb{R})$ and the upper half plane X" wäre ein Titel, der dem Inhalt des Buches gerechter würde. Das Ziel des Buches ist eine möglichst zugängliche und vollständige Darstellung von Selbergs Spektraltheorie der automorphen Formen auf $G = \mathrm{SL}(2, \mathbb{R})$, d.h. letztendlich der harmonischen Analyse der unitären Darstellung ρ der Gruppe G durch Rechtstranslationen auf dem Hilbertraum $H := L^2(\Gamma\backslash G)$. Durch die Voraussetzung, daß $\Gamma\backslash G$ bzgl. dem invarianten Maß endliches Volumen hat, d.h. daß die diskrete Untergruppe $\Gamma \subseteq G$ ein Gitter ist, enthält der Raum H alle beschränkten stetigen Funktionen und ist daher ein recht zugängliches Objekt. Bevor wir uns dem Aufbau des Buches zuwenden, geben wir einen kurzen Überblick über die Struktur der Darstellung ρ auf H. Diese Darstellung zerlegt man wie folgt in drei Blöcke, die man separat analysiert.

(1) Der cuspidale Anteil H^o: Eine unipotente Untergruppe $N \subseteq G$ ist eine Untergruppe, die zu der Gruppe N_0 der Matrizen der Gestalt $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$, $x \in \mathbb{R}$, konjugiert ist. Ist $N \cap \Gamma \neq \{e\}$, so nennen wir N cuspidal bzw. eine Spitze von Γ. In diesem Fall ist $\Gamma_N := N \cap \Gamma \cong Z$ und $N/(N \cap \Gamma) \cong \mathbb{R}/Z$ kompakt. Ist nun φ eine lokal integrable Funktion auf G, die links Γ_N-invariant ist, so heißt die lokal integrable Funktion

$$\varphi_N(g) := \int_{N/\Gamma_N} \varphi(ng)\, dn$$

konstanter Term von φ entlang N. Wir nennen φ cuspidal, wenn die konstanten Terme für alle Γ-cuspidalen unipotenten Untergruppen verschwinden. Es stellt sich heraus, daß

der Raum H^o der cuspidalen Elemente in H ein abgeschlossener G-invarianter Unterraum ist, der in eine direkte Summen irreduzibler Darstellungen mit jeweils endlichen Vielfachheiten zerfällt (Theorem 16.2). Durch Poincaréreihen (Mittelung von Funktionen bzgl. Γ auf der linken Seite), erhält man Einbettungen von integrablen Darstellungen der diskreten Reihe in H^o.

Der Orthogonalraum $(H^o)^\perp$ in H zerfällt in den Unterraum H_{rs}, der erzeugt wird von allen irreduziblen Unterdarstellungen von $(H^o)^\perp$, und sein Komplement H_{ct}. Insgesamt haben wir also

$$H \cong H^o \oplus H_{\mathrm{rs}} \oplus H_{\mathrm{ct}}.$$

(2) Der diskrete nichtcuspidale Anteil H_{rs}: Dieser Unterraum wird erzeugt von den konstanten Funktionen und endlich vielen irreduziblen Darstellungen der Komplementärreihe. Welche Darstellungen hier auftreten, ist bestimmt durch die Pole der meromorphen Fortsetzungen von Eisensteinreihen, deren Konstruktion wir kurz skizzieren.

Eine parabolische Untergruppe P ist der Normalisator einer unipotenten Untergruppe N, d.h. $P = N_G(N)$. Man nennt P cuspidal, wenn N cuspidal ist. In diesem Fall haben wir eine Zerlegung $P = MAN$, wobei A die Gruppe der positiv definiten symmetrischen Matrizen in P ist und $M = Z_K(A)$. Weiterhin haben wir die zugehörige Iwasawazerlegung $G = NAK$, für die die Multiplikationsabbildung $N \times A \times K \to G$ bijektiv ist.

Auf der Gruppe $K = \mathrm{SO}(2, \mathbb{R})$ betrachten wir die Charaktere

$$\chi_m\left(\begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}\right) = e^{im\varphi} \quad \text{für} \quad m \in Z.$$

Für die Gruppe $P_0 = N_G(N_0)$ der oberen Dreiecksmatrizen und $s \in \mathbb{C}$, $m \in Z$ erhalten wir eine Funktion

$$\varphi_{P_0,m,s}\colon G = N_0 A_0 K \to \mathbb{C}, \quad nak = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{\chi_m(k)}{(c^2+d^2)^{\frac{1+s}{2}}}.$$

Ist P beliebig und $k \in K$ mit $P = kP_0k^{-1}$, so setzen wir $\varphi_{P,m,s}(g) := \varphi_{P_0,s,m}(k^{-1}gk)$. Ist nun P cuspidal und zusätzlich $\varphi_{P,s,m}$ linksinvariant bzgl. Γ_N (das ist für $\Gamma_N = \Gamma_P := P \cap N$ oder $m \in 2Z$ der Fall), so betrachten wir die Eisensteinreihe

$$E(P,m,s)(g) := \sum_{\gamma \in \Gamma_P \backslash \Gamma} \varphi_{P,m,s}(\gamma g).$$

Für $m = 0$ und $P = P_0$ erhalten wir mit $z = g.i \in X$ die Relation

$$E(P_0,0,s)(g) = \text{const.} \cdot (\operatorname{Im} z)^{\frac{1+s}{2}} \sum_{(0,0)\neq(c,d)\in Z^2} \frac{1}{|cz+d|^{1+s}},$$

also klassische Eisensteinreihen für $\Gamma = \mathrm{SL}(2, Z)$ auf der oberen Halbebene X.

Die Eisensteinreihen konvergieren absolut auf G für $\operatorname{Re} s > 1$ und sind für festes s analytische Eigenfunktionen des Casimiroperators $\mathcal{C}$ zum Eigenwert $\frac{1}{2}(s^2-1)$. Darüberhinaus besitzen sie meromorphe Fortsetzungen auf ganz $\mathbb{C}$. Das zentrale Ergebnis über den Raum H_{rs} ist nun, daß er erzeugt wird von den Residuen der meromorphen Fortsetzungen der Eisensteinreihen $E(P,m,s)$ an den Polen im Intervall $]0,1]$ (Theorem 16.6). Hierbei gehören die konstanten Funktionen zum Residuum an der Stelle $s = 1$. Ist $\Gamma \subseteq \mathrm{SL}(2,Z)$ eine Kongruenzuntergruppe, so liegt bei $s = 1$ der einzige Pol, so daß H_{rs} in diesem Fall eindimensional ist.

(3) Der stetige Anteil H_{ct}: Der Raum H_{ct} ist eine Summe direkter Integrale von Hauptreihendarstellungen (Theorem 17.7). Um diese Zerlegung zu beschreiben, benötigt man

den Spektraltyp der meromorphen Fortsetzungen der Eisensteinreihen $E(P, m, s)$ für $s \in i\mathbb{R}$.

Für die Existenz der meromorphen Fortsetzungen der Eisensteinreihen folgt Borel einer Beweisstrategie, die auf J. Bernstein und Selberg zurückgeht und die Existenz aus den entsprechenden Eigenschaften der Resolvente eines kompakten Operators gewinnt. Dieser Beweis funktioniert für allgemeine Gitter Γ in G und vereinfacht Selbergs ursprünglichen Beweis wesentlich.

Das Buch besteht aus 4 Kapiteln, die insgesamt in 18 Abschnitte unterteilt sind. Das erste Kapitel (Abschnitte 1–4) enthält grundlegendes Material zu diskreten Untergruppen von $\mathrm{SL}(2, \mathbb{R})$ und der Wirkung auf der oberen Halbebene. Abschnitt 1 enthält allgemeine Notation und in Abschnitt 2 werden einige Fakten über invariante Differentialoperatoren auf G und X zusammengestellt. In Abschnitt 3 wird die Reduktionstheorie für Gitter $\Gamma \subseteq G$ diskutiert. Hier findet man zum Beispiel einen Beweis des Siegelschen Satzes über die Existenz eines Fundamentalpolygons mit endlich vielen Seiten für den Fall, daß $\Gamma \backslash G$ endliches Volumen besitzt. Abschnitt 4 beschreibt das Kreisscheibenmodell von $\mathrm{SL}(2, \mathbb{R})/\mathrm{SO}(2, \mathbb{R})$.

In Kapitel II (Abschnitt 5–9) werden automorphe Formen und Spitzenformen eingeführt. In Abschnitt 7 werden konstante Terme in einer Spitze definiert und Abschätzungen für die Differenz einer automorphen Form und ihres konstanten Terms in der Nähe der Spitze bewiesen, die es schließlich in Abschnitt 8 erlauben zu zeigen, daß der Raum der automorphen Formen, die zu einem festen Charakter von K gehören und von einem festen Polynom $p(C)$ im Casimiroperator C annulliert werden, endlichdimensional ist. In Abschnitt 9 wird gezeigt, daß Faltung mit einer glatten Funktion mit kompaktem Träger auf dem Raum H^o zu einem Hilbert-Schmidt-Operator führt.

Die Theorie der Eisensteinreihen wird in Kapitel III (Abschnitt 10-12) entwickelt. Die Konvergenz von Eisensteinreihen wird in Abschnitt 10 untersucht, ihre meromorphe Fortsetzung in Abschnitt 11 und ihr Bezug zu automorphen Formen, die orthogonal zu Spitzenformen sind, in Abschnitt 12. Hier ist die Information über die Pole in der rechten Halbebene $\mathrm{Re}\, s \geq 0$ relevant. Für $\mathrm{Re}\, s > 0$ wird sie aus den sogenannten Maass-Selberg-Relationen abgeleitet.

Kapitel IV (Abschnitt 13–18) enthält die Spektralzerlegung von H. In Abschnitt 13 wird zunächst die Spektralzerlegung derjenigen Unterräume von H, auf denen K mit einem festen Charakter operiert, bzgl. dem Casimiroperator C beschrieben. Abschnitte 14 und 15 enthalten schließlich diejenigen Informationen über unendlichdimensionale unitäre Darstellungen von G, die für das weitere Vorgehen benötigt werden. In Abschnitt 14 werden allgemeine Fakten zusammengestellt und in Abschnitt 15 die irreduziblen Darstellungen von G vorgestellt. Ab Abschnitt 14 werden die Anforderungen an den Hintergrund des Lesers dementsprechend höher, aber es ist ein wesentlicher didaktischer Vorteil des Buches, daß dieser Punkt möglichst weit hinten liegt. Die Hauptresultate findet man schließlich in den Abschnitten 16 und 17, die jeweils dem diskreten bzw. kontinuierlichen Teils in H gewidmet sind. Das Bild, das sich hier bietet, haben wir oben bereits vorgestellt.

Das Buch schließt mit Abschnitt 18, in dem erklärt wird, in welchem größeren Kontext das Buch steht. Insbesondere bemerkt der Autor an dieser Stelle, daß das Ende des Buches eigentlich erst der Anfang der Theorie ist. Auch im übrigen Teil des Buches sind die eingestreuten Bemerkungen, Hinweise und Referenzen sehr hilfreich für den Leser, dem sie ermöglichen, den roten Faden ständig im Auge zu behalten. Die Beweise sind sehr sorgfältig ausgeführt und man findet nur wenige Druckfehler.

Die Voraussetzungen, die das vorliegende Buch von seinen Lesern erwartet, sind durch die exzellente Darstellung minimal gehalten. Es werden Grundkenntnisse in Funktionalanalysis (kompakte Operatoren) und einige wenige Grundbegriffe der Lieschen

Theorie erwartet, die allerdings nur für sehr explizite Untergruppen von $SL(2, \mathbb{R})$ benötigt werden. Ein wesentliches Anliegen des Buches ist die Unabhängigkeit von der elaboraten Struktur- und Darstellungstheorie allgemeiner reduktiver Gruppen. Die Darstellung ist sehr gelungen und sollte einem Leser, der nicht über diesen Hintergrund verfügt, zugänglich sein.

Das Buch ist jedem, der sich für automorphe Formen und ihre Anwendungen in Darstellungstheorie, Zahlentheorie und algebraischer Geometrie interessiert, wärmstens zu empfehlen.

Darmstadt K.-H. Neeb

Gonchar, A. A., Havin, P., Nikolski, N. K., Complex Analysis I (Encyclopaedia of Math. Sci. 85), Berlin u. a.: Springer 1997, 261 S., DM 148,–

Dieser Band ist die Übersetzung eines im Jahr 1991 in russischer Sprache erschienenen Buches und enthält zwei voneinander unabhängige Teile. Der Teil I, von A.A. Goldberg, B. Ya. Levin und I. V. Ostrovskii, trägt den Titel „Entire and Meromorphic Functions"; der Teil II ist von M.B. Balk mit dem Titel „Polyanalytic Functions and Their Generalizations".

Es wird auf sehr beschränkter Seitenzahl eine Fülle von Resultaten aus dem Bereich der Theorie der ganzen und meromorphen Funktionen bzw. der polyanalytischen Funktionen dargestellt. Dies gelingt, indem weitgehend auf eine ausführliche Beweisführung verzichtet wird und nur gelegentlich Beweisideen kurz geschildert werden.

Dafür hat man mit diesem Buch einen sehr kompakten Überblick, nicht nur über einen großen Teil der Arbeiten der beteiligten Autoren und deren Schüler und Mitarbeiter, sondern auch über historische Zusammenhänge und Verbindungen zu anderen Arbeitsgruppen in Händen.

Daraus ergibt sich natürlich schon vorneweg, daß dieses Buch in erster Linie den Forscher auf einem der genannten Gebiete anspricht, der darüber hinaus mehr Einblick in bisher vielleicht weniger bekannte Arbeiten russischer Autoren bekommen möchte.

Eine ausführliche Diskussion des Inhaltes ist hier nicht möglich, deshalb werde ich zunächst einmal, um einen ersten Überblick zu geben, die Kapitelüberschriften von *Teil I* auflisten und danach auf die dazugehörigen Inhalte näher eingehen.

Die Kapitel sind:

1. General Theorems on the Asymptotic Behavior of Entire and Meromorphic Functions
2. The Connection Between the Growth of an Entire Function and the Distribution of Its Zeros
3. Limit Sets of Entire and Subharmonic Functions
4. Interpolation by Entire Functions
5. Distribution of Values of Meromorphic Functions
6. Entire and Meromorphic Solutions of Ordinary Differential Equations
7. Some Applications of the Theory of Entire Functions

Im *1. Kapitel* werden Wachstumsmaße, wie Ordnung (verallgemeinerte Ordnung) Typ, Indikator ganzer Funktionen eingeführt und grundlegende Eigenschaften diskutiert. Pólya-peaks, Wiman-Valiron Theorie von Maximalglied und Zentralindex (auch für Dirichlet-Reihen) gehören ebenso dazu, wie der Zusammenhang von Indikator und Borel-transformierter.

Im *2. Kapitel* wird auf Zusammenhänge zwischen Wachstum und Nullstellenverteilung spezieller Klassen ganzer Funktionen eingegangen; insbesondere auf Funktionen von vollständig regulärem Wachstum. Beispielsweise werden Funktionenklassen unter-

sucht, deren Nullstellenverteilung in Winkelräumen eine zweistellige asymptotische Darstellung besitzen, oder auch der Zusammenhang zwischen Nullstellenverteilung und Fourierkoeffizienten.

Das *Kapitel 3* befaßt sich mit Limit-sets ganzer Funktionen endlicher Ordnung. Für eine ganze Funktion der Ordnung $\rho < \infty$ versteht man unter dem Limit-set die Menge jener Elemente des Distributionenraumes $\mathcal{D}'(\mathbf{C})$, die als Grenzwert der Familie $\{\log|f(z)|t^{-\rho}\}_{t>0}$ für $t \to \infty$ auftreten.

Zahlreiche Anwendungen, zusammen mit grundlegenden Eigenschaften von Limit-sets werden aufgeführt. Interessant ist hier u.a. der Zusammenhang mit dynamischen Systemen.

Im *Kapitel 4* werden verschiedene Interpolationstechniken, wie z.B. Newton- oder Lagrangeinterpolation, mit Hilfe Ganzer Funktionen von endlicher Ordnung beschrieben.

Das *Kapitel 5* beschäftigt sich nun mit meromorphen Funktionen und deren Wertverteilung. Dies geschieht im Rahmen der Nevanlinna-Theorie meromorpher Funktionen. Es werden verschiedene Defekte (Nevanlinna, Valiron, Petrenko) behandelt und das „Umkehrproblem", welches 1974 von D. Drasin gelöst wurde, sowie damit verwandte Probleme beschrieben. Desweiteren werden Ergebnisse über asymptotische Kurven und asymptotische Werte, sowie über Julia- und Borelrichtungen angegeben. Die Wertverteilung bei speziellen Klassen meromorpher Funktionen, etwa im Umfeld der sogenannten cos $\pi\rho$-Sätze, gehört hier ebenso dazu, wie die Wertverteilungstheorie ganzer Kurven.

Das *Kapitel 6* ist der Untersuchung gewöhnlicher Differentialgleichungen gewidmet und zwar insbesondere der Existenz ganzer oder meromorpher Lösungen. Typischerweise betrachtet man algebraische Differentialgleichungen und insbesondere auch lineare Differentialgleichungen. Die benutzten Methoden stammen hier meist aus der Nevanlinna-Theorie oder der Zentralindexmethode nach Wiman und Valiron, wie sie im 1. Kapitel eingeführt wurde. Insgesamt wird hier nur eine recht beschränkte Auswahl aus den bis heute auf diesem Gebiet erzielten Ergebnissen angesprochen.

Das letzte *Kapitel 7* bringt dann noch einige Anwendungen der Theorie auf Riemannsche Randwertprobleme mit unendlichem Index oder auf ganze charakteristische Funktionen einer Wahrscheinlichkeitsverteilungsfunktion.

Allein die mehr als 460 Literaturzitate, welche den ersten Teil beschließen, belegen, welch umfangreiches und inhaltsreiches Werk hier vorliegt. Deshalb ist auch eine detailliertere Beschreibung auf so begrenztem Raum nicht möglich.

Im *Teil II* werden polyanalytische Funktionen behandelt. Diese Funktionenklasse ist insofern eine Verallgemeinerung der holomorphen Funktionen, als sie den Kern einer Potenz des Cauchy-Riemann Operators bildet. Eine polyanalytische Funktion f (der Ordnung n) ist also in der Form

$$f(z) = \sum_{k=0}^{n-1} h_k(z)\bar{z}^k$$

darstellbar, wobei $h_k, k = 0, 1, \ldots, n-1$, holomorphe Funktionen sind.

Wie man am Beispiel der bianalytischen Funktion $f(z) = 1 - z\bar{z}$ erkennt, gilt z.B. der Satz über die Isoliertheit der Nullstellen nicht mehr, was die Möglichkeit einer Verallgemeinerung von Sätzen aus der klassischen Funktionentheorie erheblich einschränkt. Dennoch gilt beispielsweise, daß jede ganze n-analytische Funktion die n verschiedene Werte nicht annimmt ein *polyanalytisches Polynom* ist. Bis n=3 gilt dann, daß diese Polynome eine entartete Abbildung darstellen, d.h. $\mathbf{C}$ auf eine gewisse Kurve abbilden. Für $n > 3$ ist diese Frage bisher unbeantwortet.

Der Satz von Picard gilt hier völlig analog zum klassischen Fall und besagt, daß eine ganze transzendente polyanalytische Funktion höchstens einen Wert ausläßt; er gilt aber nicht mehr für polymeromorphe Funktionen.

Sehr interessant ist eine angepaßte Verallgemeinerung des Begriffs der Normalen Familie, so daß das Montelsche Normalitätskriterium wieder gilt.

Obwohl es auch eine schwache Form des Maximumprinzips gibt, sind Randwertaufgaben i.a. nicht eindeutig lösbar; man kann die eindeutige Lösbarkeit durch gewisse Zusatzvoraussetzungen jedoch erzwingen. Es gelten auch Sätze über nichttangentielle Grenzwerte. Bemerkenswert ist dabei, daß für die Existenz eines nichttangentiellen Grenzwertes die Beschränktheit von f und f_z ausreichen. Ein Ausblick über mögliche Verallgemeinerungen und eine explizite Darstellung des Bergmankerns für den Einheitskreis beschließen diesen Teil.

Zusammenfassend kann gesagt werden, daß dieser Abschnitt eine umfassende Darstellung der Theorie der polyanalytischen Funktionen bis zum Jahre 1991 ist. Er beinhalted ein reichhaltiges Literaturverzeichnis über eine Theorie, welche zwischen der Theorie von Funktionen mehrerer komplexer Veränderlicher und der Theorie der ganzen (meromorphen) Kurven angesiedelt werden kann.

Aachen G. Jank

Bergeron, F., Labelle, G., Leroux, P., Combinatorial Species and Tree-like Structures (Encycl. of Math. and its Appl. 67), Cambridge University Press 1997, 457 S., £ 55,–

Das aus der Analysis stammende Werkzeug der erzeugenden Funktionen (im Sinne von formalen Potenzreihen) hat eine lange Tradition bei der Behandlung von kombinatorischen Zählproblemen; Namen wie Euler, MacMahon, Pólya bezeugen das. Auch heute kommen aus in den verschiedensten Bereichen (von der Statistischen Mechanik bis zur Komplexitätsanalyse von Algorithmen) mannigfache Aufgaben, die sich auf kombinatorische Zählprobleme reduzieren lassen. Obwohl es immer wieder Versuche der Systematisierung gegeben hat, wurden und werden Lösungsmethoden oft ad-hoc (wieder-)erfunden.

Im Jahr 1981 erschien in den Advances of Mathematics (Band 42, pp. 1–82) ein Artikel von André Joyal (Montréal) mit dem Titel *Une théorie combinatoire des séries formelles.* Dabei wurde Ansatz präsentiert, wie man die üblichen Operationen auf (formalen) Reihen, wie Addition, Cauchy- und Hadamard-Multiplikation, Ableitung, Integration, Substitution, Inversion, usw. auf das Niveau von kombinatorischen Objekten, oder besser noch: von Konstruktionsvorschriften für solche Objekte, „liften" kann. Diese Objekte (bzw. Vorschriften) werden als „kombinatorische Spezies" bezeichnet, und wie man so etwas präzise definiert und damit konzeptuell umgeht, dafür liefert in diesem Ansatz die Sprache der Kategorientheorie die Anleitung. Auf ganz anschaulichem Niveau geht es um Objekte wie: Permutationen, Bäume, Funktionen, Listen, usw., aber eben nicht nur um isolierte Objektklassen dieser Art, sondern um Aussagen der Art: „eine Abbildung einer endlichen Menge in sich ist (auf kanonische Weise) eine Permutation von gewurzelten Bäumen". Nicht diese (sehr simple) Aussage für sich alleine ist von Interesse, sondern die Frage, wie man numerische Information über Symmetrietypen von Abbildungen aus entsprechenden Informationen über deren Komponenten (Permutationen, Bäume) erhalten kann. Bei diesem Ansatz sollen also auch die Symmetrieeigenschaften dieser Objekte systematisch erfasst werden, und das bedeutet, dass zu den üblichen Werkzeugen der numerischen Buchhaltung, nämlich der exponentiellen erzeugenden Funktion (für Konstruktionen auf Basismengen mit unterscheidbaren Elementen) und der gewöhnlichen erzeugenden Funktion (bei ununterscheidbaren Basis-Elementen, also bei der Enumeration

von Isomorphietypen), als wesentliches Instrument die sogenannte Zykelindexreihe kommt. Die Idee zu diesem Konstrukt ist natürlich in der Abzähltheorie à la Pólya beheimatet, sie wird hier systematisch untersucht und eingesetzt. Letztlich hat man es dann mit drei verschiedenen Niveaus zu tun: den kombinatorischen Konstruktionen, den Zykelindexreihen, sowie den üblichen erzeugenden Funktionen. Im Studium der Beziehungen zwischen diesen Niveaus liegt, neben den konkreten Anwendungen, der Reiz dieser Theorie der kombinatorischen Spezies.

Obwohl A. Joyal in der Folgezeit noch einige wichtige Beiträge zu speziellen Fragestellungen geliefert hat, war es vorwiegend die Sache seiner Kollegen an der Université du Québec à Montréal (darunter in erster Linie den drei Autoren des vorliegenden Buches), dieses „Programm" auszuführen und dessen Potential nach allen Richtungen auszuloten. Dabei zahlte sich aus, dass diese Mitarbeiter zwar alle in erster Linie an kombinatorischen Fragestellungen interessiert waren, aber ganz unterschiedlichen Hintergrund hatten: klassische Analysis, Algebra, Informatik, usw.; das wird beim Ausbau der Theorie und den Anwendungen deutlich.

Damit keine falschen Erwartungen geweckt werden: die Theorie der Spezies stellt keine fabelhaften neuen Techniken zur Behandlung bislang unzugänglicher Probleme bereit. Aber sie bietet ein schlüssiges Konzept und einen ausgefeilten begrifflichen und technischen Apparat zur Behandlung vieler (nicht aller!) Abzählprobleme. Wie gesagt, Ansätze zu solchen übergreifenden, systematisierenden Darstellungen kombinatorischer (Abzähl-)Technik hat es schon früher gegeben. Insofern ist natürlich nicht alles „neu", was die Theorie der Spezies zu bieten hat, aber es bedurfte – neben einer brauchbaren tragenden Idee – wohl eines solchen Gemeinschaftsunternehmens, einer „Schule", um die Vielfalt an Möglichkeiten und die kritische Masse von Anwendungsbeispielen zu erarbeiten, damit sich eine solche Theorie tatsächlich etabliert. Dass dies gelungen ist, bestätig das vorliegende Werk, die erste Monografie zu diesem Thema, auf überzeugende Weise. Eine fruchtbare Entwicklung über fast 20 Jahre hinweg kann natürlich nicht in einem Band vollständig dargestellt werden. Deshalb ist ein kurzer Abriss des Inhalts angezeigt.

Im ersten Kapitel werden Spezies in ihrer einfachsten Form eingeführt, nämlich mit einer Punktsorte und ohne spezielle Gewichtung. Die wichtigsten Operationen auf Spezies werden ebenso behandelt, ebenso wie die den Spezies zugeordneten erzeugenden Funktionen. Das zweite Kapitel behandelt weitere Operationen auf Spezies, wie Hadamard-Produkt und funktorielle Komposition, mit denen die Vielfalt der Anwendungsmöglichkeiten (beispielweise im Bereich der Graphentheorie) deutlich erhöht wird. Anschliessend werden auch Spezies mit mehreren Punktsorten und gewichtete Spezies definiert und untersucht. Der letzte Teil des zweiten Kapitels ist systematischen Fragestellungen gewidmet: wie kann man den „Ring der Spezies" als algebraisches Objekt beschreiben? Dazu muss man sog. virtuelle Spezies einführen, sowie additiv bzw. multiplikativ unzerlegbare Spezies untersuchen. Da Spezies aus algebraischer Sicht als spezielle Darstellungen der symmetrischen Gruppen aufgefasst werden können, überrascht es nicht, so manchem Konzept aus der Darstellungstheorie in neuem Gewand zu begegnen.

Der Inhalt des dritten Kapitels hat sehr stark mit Konzepten aus der klassischen Analysis zu tun. Es geht insgesamt um die Definition von Spezies durch kombinatorische Funktionalgleichungen und die Untersuchung der so definierten Objekte. Hier macht man Bekanntschaft mit kombinatorischen Versionen der Lagrange-Inversion, des Satzes über implizite Funktion, der Newton-Iteration. Speziell in diesem Kapitel spielen die im Titel genannten Baumstrukturen eine dominierende Rolle, sowohl als Objekte von eigenem Interesse, als auch als Hilfsmittel bei der iterativen Konstruktion von Lösungen von Funktionalgleichungen. Ein kurzer Abriss schlägt die Brücke zur asymptotischen Analysis.

Das vierte Kapitel ist einigen spezielleren Fragen im Zusammenhang mit der Abzählung von Isomorphietypen und asymmetrischen Strukturen gewidmet. Auch hier liegt

das Schwergewicht der Beispiele und Anwendungen im Bereich der Graphentheorie und Baumstrukturen. Der Zusammenhang mit der Abzähltheorie à la Pólya wird explizit gemacht, und der Beweis eines zentralen Resultats der ganzen Theorie, der (plethystischen) Substitutionsformel für die Zykelindexreihen von gewichteten Spezies, wird hier detailliert dargestellt.

Wählt man als Fundament des ganzen Gebäudes die Kategorie der totalgeordneten (endlichen) Mengen, anstelle der strukturlosen Mengen, so erhält man die sog. linearen Spezies. Diese verhalten sich in mancher Hinsicht (z.B. eindeutige Lösbarkeit von Gleichungen) ganz anders als die üblichen Spezies, sie sind viel näher an den formalen Reihen im klassischen Sinn. Interessante Anwendungen dieser Theorie, die im fünften Kapitel dargestellt wird, finden sich vor allem im Bereich der Differentialgleichungen.

Ein kurzer Anhang resümiert die Pólya-Theorie; weiterhin findet man Tabellen mit konkreten Spezies und ihren erzeugenden Funktionen, sowie ein Literaturverzeichnis mit 340 Einträgen. Das Buch enthält sehr viele Aufgaben, die allerdings nicht im Sinn der Übungsaufgaben eines Lehrbuchs zu verstehen sind. Es handelt sich vielmehr um weiterführendes Material, das in Aufgabenform dargeboten wird. Die Vielfalt des Beispielmaterials, die Bezüge zu den verschiedensten Fragestellungen in Anwendungsbereichen, die Ausbaumöglichkeiten und Varianten dieser Theorie, werden auf diese Weise eindrucksvoll dokumentiert. Ganz unberücksichtigt bleiben Aspekte der algorithmischen Umsetzung — aber das wäre wohl der Stoff für ein weiteres Buch.

Insgesamt ist dies ein sehr sorgfältig geschriebenes und gut lesbares Buch, das einen authentischen und adäquaten Überblick über die Theorie der kombinatorischen Spezies und die Vielfalt ihrer Anwendungen bietet.

Erlangen V. Strehl

Blum, L., Cucker, F., Shub, M., Smale, S., Complexity and Real Computation, Berlin u. a.: Springer-Verlag 1997, xvi + 453 S., DM 79,–

Seit einigen Jahrzehnten ist Komplexitätstheorie als interdisziplinäres Gebiet der Mathematik wie der Informatik wohletabliert. Vorrangig auf kombinatorische Entscheidungs- und Optimierungsprobleme bezogen, methodisch an der Tradition klassischer (Turingmaschinen) Berechenbarkeit orientiert, zielt die durch grundlegende Arbeiten von Cook und Karp begründete Theorie der *NP*-Vollständigkeit auf Fragen quantitativer Effizienz. Allerdings ist die Hauptvermutung $P \neq NP$, daß (z. B.) aussagenlogische Erfüllbarkeit nicht in polynomialer Zeit entscheidbar sei, immer noch unentschieden. Weiter gibt es, gängigen numerischen Verfahren näherstehend, den mittlerweile breiten Fundus der *Algebraischen Komplexitätstheorie*, wozu [BCS] als vorzügliche Quelle empfohlen werden kann.

Den Autoren des vorliegenden Buches [BCSS] geht es um eine (aus ihrer Sicht) adäquate Modellierung wissenschaftlichen Rechnens. Sie verallgemeinern, wie es R. Karp in einem begleitenden Vorwort treffend skizziert, die P/NP-Theorie auf beliebige Ringe R, wobei (wie der Titel andeutet) die Fälle $R = \mathbb{R}$ und $R = \mathbb{C}$ alias $\mathbb{R}^2$ im Vordergrund stehen, während $R = \mathbb{Z}_2$ die bisherige Theorie liefert und $R = \mathbb{Q}$ nebst $\mathbb{Z}$ als diskrete Varianten diskutiert werden. Die Relevanz solcher Unterscheidungen wird am Beispiel der linearen Optimierung deutlich: Seit 1979 (Ellipsoidmethoden) ist für *rationale* Eingabedaten polynomiale Bitkomplexität gesichert, also approximativ auch für den reellen Fall, während „streng" polynomische Verfahren (bei denen die Zahl reeller Operationen polynomial in den Dimensionen des Problems beschränkt bleibt) bisher nur für spezielle Problemklassen bekannt sind; vgl. dazu etwa [GLS, Kap. 1 und 6].

Im ersten der drei Teile des Buchs wird nach Vorstellung motivierender Probleme (wie z. B. Mandelbrot-Menge, Newton-Verfahren, Hilberts Nullstellensatz als Entschei-

dungsproblem) das vor neun Jahren von drei der Autoren vorgeschlagene „BSS-Modell" zur Formalisierung numerischen Rechnens eingeführt. Berechnungen mit (atomar, exakt gedachten) reellen oder komplexen Zahlen erfolgen durch „Maschinen", die mit Flußdiagrammen beschrieben werden (was allerdings teils recht umständlich wirkt). Operationen $+, -, *, /$ nebst Verzweigungen nach ≥ 0 Tests über $\mathbb{R}$ oder $= 0$ Tests über $\mathbb{C}$ führen bei Berechenbarkeits- und Entscheidbarkeitsfragen auf die Diskussion semi- bzw. quasi-algebraischer Mengen.

Aus der Fülle des gebotenen Materials hier nur ein Beispiel: Das Entscheidungsproblem HN/$\mathbb{C}$ (von den Autoren etwas daneben *Hilbert Nullstellensatz over* $\mathbb{C}$ genannt), ob endlich viele „gegebene" Polynome $f_j \in \mathbb{C}[z_1, \ldots, z_n]$ eine gemeinsame Nullstelle $\zeta \in \mathbb{C}^n$ haben, wird als $NP_{\mathbb{C}}$-vollständiges Problem identifiziert, wie im diskreten Fall bleibt aber auch hier $NP_{\mathbb{C}} \neq P_{\mathbb{C}}$ eine unbewiesene Vermutung. Daß andererseits HN/$\mathbb{C}$ zu $NP_{\mathbb{C}}$ gehört, beruht auf der Vorstellung, daß zusätzlich gegebenes ζ als gemeinsame Nullstelle durch Test der Bedingungen $f_j(\zeta) = 0$ in polynomialer Zahl von Schritten verifizierbar sei.

Hauptgegenstand des *zweiten Teils* ist das Newtonsche Iterationsverfahren in Anwendung auf Polynomgleichungen über $\mathbb{C}$, womit 5 jüngere Arbeiten *Complexity of Bezouts theorem, I–V* von Shub und Smale eine zusammenfassende und vertiefte Darstellung finden. Aus Daten am Startpunkt werden (ähnlich den Kantorovich Kriterien) hinreichende a priori Bedingungen für (quadratische) Konvergenz gegeben und in Homotopieverfahren auf einzelne Polynomgleichungen und Systeme solcher angewandt. Naturgemäß ist das jeweils auf die Approximation *einfacher* Nullstellen beschränkt, die anderen Fälle werden als „ill-posed problems" eingestuft. Bestechend elegant ist andererseits die unitär invariante Formulierung für projektive Räume. Besondere Erwähnung (auch für den Fachmann) verdienen die Kapitel 11–13, in denen die *Kondition* solcher Probleme analysiert und im Mittel nach oben abgeschätzt wird.

Im Kapitel 15 (Lineare Optimierung) findet Newton-Iteration bei einem Barriereverfahren Verwendung. Daß solche „inneren" Methoden anderen (polynomialen) Verfahren überlegen sind, wird aber nicht hinreichend deutlich, weil die Behandlung weiterer hier benötigter Algorithmen (z. B. exaktes Invertieren rationaler Matrizen) weit hinter heutigem Stand des Wissens zurückbleibt. Einschlägige Teile aus [GLS] – im Buch übrigens nicht zitiert – bilden hier eine lohnende Alternative.

Im *dritten Teil* behandeln die Autoren Komplexitätsklassen über $\mathbb{R}$ nach den heute in der theoretischen Informatik üblichen (und weiteren) Spielarten, z. B. Entscheidungsbäume, probabilistische Algorithmen, Parallelität, und früher schon diskutierte Maschinen nun unter variierten Kostenmaßen. Häufige Paradigmenwechsel lassen diesen Teil weniger kohärent erscheinen. So erhellend dieser Streifzug hier und da auch sein mag, manches kommt dabei leider doch zu kurz. Wer sich z. B. über die unteren Schranken bei Entscheidungsbäumen, die man aus oberen Schranken (Milnor, Thom) für die Zahl der Zusammenhangskomponenten semi-algebraischer Mengen herleiten kann, gründlicher informieren will, sollte statt Kap. 16 [BCSS] besser in Kap. 11 [BCS] lesen – ebenfalls bei Springer!

Im Gesamtbild erscheint dieses Buch nicht ausgewogen. Die Auswahl der Themen wie auch der zitierten Literatur wirkt sehr selektiv. Das mathematische Niveau der Darstellung schwankt, indem z. B. hier Einsicht in die Integration auf Mannigfaltigkeiten erwartet wird, dort in trivialer Manier alle Regeln eines inneren Produkts erklärt werden. Bei genaueren Leseproben findet man (neben verzeihlichen technischen Pannen) viele Ungenauigkeiten, oft auch im Begrifflichen, so bei Definitionen und deren (un)pünktlicher Befolgung, was die Lektüre erschwert. So kann man diesen Text auch kaum als Lehrbuch empfehlen.

Alles in allem ein kontroverses Buch, das spannende Fragen und Resultate bietet, bei seinen Modellierungen aber auch erhebliche Zweifel an deren Adäquatheit weckt. Im

Deutschen ist das „Real Computation" des Titels sicher als *reelles Rechnen*, aber wohl nicht als *reales Rechnen* zu lesen. Diese Diskrepanz wird z. B. sichtbar, wenn die Autoren im Text formal beweisen, daß die Mandelbrotmenge (im Sinne des BSS-Modells) nicht entscheidbar ist, andererseits aber Seite 9 wie auch der Buchdeckel ein schönes farbiges Bild dieser Menge zeigen.

[BCS] Bürgisser, P.; Clausen, M.; Shokrollahi, M. A.: *Algebraic Complexity Theory.* Springer, 1997.

[GLS] Grötschel, M., Lovász, L., Schrijver, A.: *Geometric Algorithms and Combinatorial Optimization.* 2nd ed., Springer, 1993.

Bonn A. Schönhage

O'Malley, R., Thinking about Ordinary Differential Equations, Cambridge Univ. Press 1997, $ 24.95

In meiner Vorlesung über gewöhnliche Differentialgleichungen werde ich oft von Studenten nach ergänzender Literatur gefragt, und das vorliegende Buch kommt einem solchen Bedürfnis entgegen. Der Autor ist als Experte für singuläre Störungstheorie bekannt und hat den Text nach eigenem Bekunden zum Selbststudium für Leser mit Vorkenntnissen verfaßt, ohne dabei Anspruch auf Originalität zu erheben.

Das Buch kommt fast ohne Beweise aus, denn sein erklärtes Ziel ist nicht die Darlegung von Theorien sondern die Vertiefung des Verständnisses anhand von vielen elementaren Beispielen und Übungsaufgaben mit ausführlichen Anleitungen. Der Vorteil des Buches liegt also darin, anhand von Beispielen Struktur zu erkennen und die Neugier auf die zugehörige Mathematik zu wecken. Die Beispiele sind jedoch bei weitem nicht so plump gewählt und so breit ausgewalzt wie etwa in Martin Brauns: Differential equations and their Applications, Springer (1975).

Inhaltlich werden folgende Themen angesprochen: 1. Gleichungen erster Ordnung, zu denen z.B. exakte Gleichungen oder spezielle Gleichungen zweiter Ordnung gezählt werden, 2. Lineare Gleichungen zweiter Ordnung, 3. Potenzreihenansätze und spezielle Funktionen, 4. Systeme linearer Differentialgleichungen, 5. Stabilitätskonzepte inklusive Ljapunovfunktionen, 6. Singuläre Störungsmethoden.

Diese Themen werden nicht erschöpfend behandelt sondern stets nur angerissen. Das Buch soll zum Nachdenken anregen und kommt diesem Ziel in mannigfacher Weise nach. Nachdenklich macht zum Beispiel schon das Titelbild, auf dem sich bei näherer Betrachtung das Phasenporträt des mathematischen Pendels von Seite 186 wiederfindet. Leider enthält es einen Fehler, denn die Linien durch die Sattelpunkte schneiden sich in der Graphik nicht, wie von der Differentialgleichung gefordert, transversal sondern berühren einander tangential. Auch Abbildung 19 auf Seite 223 ist nicht korrekt, denn die Lösung ist bis auf die Randschichten konstant 2 und nicht 0. Wie mir der Autor erklärte, sollen diese Fehler in der zweiten Ausgabe behoben werden.

Ich empfehle dieses Buch dennoch jedem der eine einführende Vorlesung über gewöhnliche Differentialgleichungen hört oder liest zum vergnüglichen Selbststudium. Nicht jeder wird darüber glücklich sein, daß das übliche Schema von Voraussetzung, Behauptung, Beweis, Definition usw. weitgehend aufgehoben ist, doch fast jeder wird nach dem aktiven Lesen des Büchleins eine Menge über das Lösen von Differentialgleichungen gelernt haben und hoffentlich mehr lernen wollen.

Köln B. Kawohl

Meyer, Y., Coifman, R., Wavelets, Calderón-Zygmund and Multilinear Operators (Cambridge Studies in Advanced Mathematics 48), Cambridge University Press 1997, 314 S., £ 40,–)

Dieser Band ist die (fachlich einwandfreie) Übersetzung des Titels „Ondelettes et Opérateurs", Vol. II (Opérateurs de Calderón-Zygmund) von Yves Meyer und Vol. III (Opérateurs multilinéaries) von R. Coifman und Yves Meyer ins Englische, die die Übersetzung von „Ondelettes" (Wavelets and Operators; Cambridge Univ. Press 1992) ergänzt. Die in der Übersetzung zu einem Band zusammengefassten Kapitel 7-16 des Werkes von Y. Meyer und R. Coifman beschäftigen sich im wesentlichen mit neueren Ergebnissen aus der Theorie der singulären Integral- und Calderón-Zygmund-Operatoren und damit verbundenen Pseudodifferential-Operatoren (dies entspricht den Kapiteln 7-11 der französischen Originalausgabe) und verallgemeinerten Hardy-Räumen, multilinearen Operatoren in L^p-Räumen, Quadratwurzeln akkretiver Differentialoperatoren, Potentialtheorie in Lipschitz-Gebieten und Paradifferential-Operatoren.

Das wesentliche Ziel des Gesamtwerkes ist es, einen Zusammenhang herzustellen zwischen der Theorie der Wavelets und solchen linearen Operatoren T, die sich zu stetigen Operatoren auf Standard-Räumen wie $H = L^2(\mathbf{R}^n)$ oder $H = L^2[0, 2\pi]$ forsetzen lassen und die diagonal bezüglich einer Orthogonalbasis von H sind, die aber nicht „pathologisch" sind in folgendem Sinn; wird eine Funktion f aus H in der gegebenen Orthogonalbasis dargestellt, so sollen die Eigenschaften von $g = Tf$ in möglichst einfacher, stabiler und robuster Weise aus der Darstellung von g ablesbar sein, und umgekehrt, die von f aus der Darstellung von g. Dies ist etwa bei der Zuordnung von $f \in L^2[0, 2\pi]$ zu ihrer Fourier-Reihe (und umgekehrt) nicht in natürlicher Weise der Fall: Eigenschaften von f übertragen sich nicht in sehr durchsichtiger Weise auf ihre Fourier-Koeffizienten, und es ist nicht immer möglich, korrespondierende Aussagen über f aus denen über die Fourier-Koeffizienten zu gewinnen. Die Autoren versuchen nun gerade in den hier übersetzten Kapiteln der französischen Originalausgabe die bemerkenswerte Tatsache zu erhellen und präzise darzustellen, daß bei der Wahl von Wavelet-Orthogonalbasen für H (oder andere Standard-Funktionen- und Distributionen-Räume) die Wavelet-Koeffizienten die Eigenschaften der dargestellten Funktion in einfacher und natürlicher, aber gleichzeitig genauer und stabiler Weise widerspiegeln, wohingegen die trigonometrischen Orthonormalbasen für das geschilderte Programm nicht sehr geeignet sind. Im wesentlichen sind es nun die in der Monographie behandelten Calderón-Zygmund-Operatoren und verwandte Pseudodifferential-Operatoren die bezüglich Wavelet-Orthogonalbasen diagonal oder approximativ diagonal sind und die den obigen „nicht-pathologischen" Eigenschaften entsprechen.

Eine kurze Vorstellung der hier dargestellten tiefliegenden Ergebnisse könnte wie folgt aussehen: Die Kapitel 7–11 dienen der allgemeinen Darstellung der Calderón-Zygmund-Operatoren und derem Beschränktheitseigenschaften als Abbildungen diverser Funktionsräume (wie $L^p(\mathbf{R}^n)$, Hardy-Räumen, BMO-Räumen [= Räume von Funktionen beschränkter mittlerer Oszillation], etc.); es werden notwendige und hinreichende Bedingungen bewiesen, die die Beschränktheit von Calderón-Zygmund-Operatoren nach sich ziehen; ein typisches hier bewiesenes Resultat ist der sogenannte $T(1)$-Satz von David und Journe, der besagt, daß ein gewisser singulärer Integraloperator T beschränkt nach $L^2(\mathbf{R}^n)$ fortgesetzt werden kann, falls u.a. $T(1) \in BMO$ ist. Es werden verschiedene Verallgemeinerungen solcher Aussagen unter Verwendung von Methoden der Wavelet-Theorie bewiesen. In den Kapiteln 12-16 werden zunächst verallgemeinerte Hardy-Räume definiert, und wichtige Resultate von Calderón, Kenig und David über die Struktur von Hardy-Räumen nachgewiesen; hierbei werden teilweise die vorher mit Hilfe von Wavelet-Analysis gezeigten $T(1)$-Theoreme und deren Verallgemeinerungen verwendet. Ferner werden Ergebnisse über Bedingungen dargestellt, die es erlauben, gewisse multilineare

Pseudodifferential-Operatoren beschränkt auf $BMO \times L^2(\mathbf{R}^n)$ fortzusetzen. Eine Vermutung von Kato über den Definitionsbereich der Quadratwurzel von maximal akkretiven Differentialoperatoren wird im Kapitel 14 in einem Spezialfall positiv beantwortet (wobei wieder $T(1)$-Theoreme herangezogen werden). Im Kapitel 15 wird die tiefliegende Calderón-Methode behandelt, die ein allgemeines Verfahren liefert, wie elliptische Randwertprobleme mit irregulärem Rand mit Hilfe von Pseudodifferential-Gleichungen oder allgemeineren Operator-Gleichungen auf dem Rand gelöst werden können; dies wird im Fall untersucht, wenn der Rand höchstens Lipschitzsch ist. So wird hier das Dirichlet- und das entsprechende Neumann-Problem mit der Calderón-Methode aus den vorhergehenden Kapiteln vollständig gelöst. Schließlich werden im letzten Kapitel des Bandes die von Bony eingeführten Paradifferential-Operatoren untersucht; es wird ein Approximationsresultat für diese Klasse von Operatoren gezeigt, die die Wavelet-Skalen benutzt.

Es sei noch erwähnt, daß die Autoren in einem Vorwort zur englischen Ausgabe einige neuere Resultat aufführen, die die wachsende Bedeutung der Verbindung von Wavelet-Theorie mit dem Bereich der linearen und nichtlinearen Differential- und Operator-Gleichungen aufzeigen (die aber noch nicht in eine entsprechende Monographie eingehen konnten). Der Band ist wegen der großen technischen Schwierigkeiten und der Tiefe der Resultate nicht leicht zu lesen, kann aber doch sehr für alle auf den Gebieten der harmonischen Analysis und Partiellen Differentialgleichungen Arbeitende oder an diesen Bereichen Interessierte empfohlen werden.

Köln H. Lange

Kröner, D., Numerical Schemes for Conservation Laws (Wiley-Teubner Series in Adv. Num. Math.) Stuttgart-Leipzig: Teubner 1997, 508 S., DM 78,–

Die nichtlinearen hyperbolischen Erhaltungsgleichungen stellen heutzutage immer noch eine große Herausforderung an die Mathematik dar. Sie stehen einerseits im Zentrum vielfältiger Anwendungen, wobei die Strömungsmechanik das wichtigste Gebiet darstellt. Andererseits sind eine Fülle fundamentaler mathematischer Probleme im Zusammenhang mit diesen Gleichungen noch offen. Eine globale Existenztheorie für Systeme in mehr als einer Raumdimension ist zum Beispiel nicht vorhanden. Zeitlich lokale Aussagen vom Cauchy-Kowalewskaja-Typ sind hier nicht von so großem Interesse, da man besonders an unstetigen schwachen Lösungen interessiert ist.

Dieses Teilgebiet der nichtlinearen partiellen Differentialgleichungen ist durch ein besonders enges Zusammenspiel von Analysis und Numerik geprägt. Einige analytische Meilensteine der Existenztheorie beruhen auf Konvergenzbeweisen für numerische Verfahren. So verwendete Oleinik 1957 für skalare Gleichungen das Lax-Friedrichs-Verfahren. Der erste Existenzsatz für Systeme in einer Raumdimension wurde für kleine Daten von Glimm 1965 mit Hilfe des nach ihm benannten numerischen Verfahrens gezeigt. Diese Analysis ist in dem Buch von Smoller [11] ausführlich dargestellt. Umgekehrt ist es eine Binsenweisheit, daß eine zufriedenstellende Theorie der Existenz und Eindeutigkeit von Lösungen generell eine notwendige Grundlage der Numerischen Analysis ist, um zum Beispiel Konvergenzgeschwindigkeiten oder a posteriori Fehlerabschätzungen, zum Einsatz in adaptiven Verfahren, mathematisch abzusichern.

Das vorliegende Buch stößt in eine bisher vorhandene Lücke der Lehrbuchliteratur zur Numerik von Erhaltungsgleichungen. Es gibt viele Darstellungen der Differenzenverfahren und der klassischen Stabilitätstheorie sowie Bücher, die hauptsächlich algorithmisch orientiert sind, sich an Anwender richten. Etwa in den Büchern von Hirsch [3, 4] und LeVeque [8] werden vor einer Übersicht über numerische Verfahren auch einige der mathematischen Grundlagen dargestellt, die zum Verständnis der Numerik notwendig

sind. Besonders das Buch von LeVeque [8] ist als kurzer Einstieg in das Thema sehr gut geeignet und findet dafür vielfältig Verwendung. Aber Resultate, die eine umfangreichere Analysis benötigen, wurden nur erwähnt und nicht ausgearbeitet. Ein der vertieften Numerischen Analysis zuzuordnendes Werk auf diesem Gebiet, wie wir es aus der mathematischen Finite-Element-Literatur für elliptische Gleichungen kennen, fehlte bisher. Das hat seinen Grund darin, daß vergleichbare Resultate für skalare Erhaltungsgleichungen erst in jünster Zeit erzielt werden konnten. Daß nun die Zeit für ein derartiges Lehrbuch reif war, sieht man daran, daß nur ein Jahr vorher ein ähnlich ausgerichtetes, aber völlig anders gestaltetes Werk von Godlewski und Raviart [2] erschienen ist.

In der inhaltlichen Auswahl der numerischen Verfahren und der Darstellungsweise setzt sich das Buch von Kröner deutlich von anderen Werken auf dem betrachteten Gebiet ab. Es hält sich nicht mehr als nötig mit Grundlagen auf, die bereits in anderen Büchern ausführlich und verständlich abgehandelt sind. Dafür wird sehr zügig eine Einführung in diejenigen numerischen Verfahren gegeben, deren Analysis im Mittelpunkt des Buches steht. Es wird die Konvergenzanalysis der Stromlinien-Diffusions-Methode und der Finite-Volumen-Verfahren in mehreren Raumdimensionen behandelt. Zentral ist Darstellung des Einsatzes von Resultaten aus Theorie der kompensierten Kompaktheit für Erhaltungsgleichungen, die von Tartar [12] und DiPerna [1] entwickelt wurde, auf die Konvergenzanalysis für die Stromlinien-Diffusions-Methode und die bei Praktikern sehr gebräuchlichen Finite-Volumen-Verfahren. An dieser Entwicklung bei letzteren Verfahren war der Autor [7, 6] maßgeblich beteiligt.

Das vorliegende Buch ist die Ausarbeitung von Vorlesungen, in denen der Autor seine Studenten von den Anfängen bis an aktuelle Probleme und Methoden der numerischen Löser und der Numerischen Analysis heranführt. Es stellt somit eine sehr aktuelle und von der wissenschaftlichen Arbeit des Autors geprägte Stoffauswahl dar. Besonders positiv hervorzuheben ist, daß Eigenschaften der behandelten numerischen Verfahren und auch Aussagen der Analysis, zum Beispiel zu Fehlerordnungen, anhand von Rechenergebnissen aus seiner Arbietsgruppe veranschaulicht und erläutert werden. Allerdings wäre es besonders für Studenten wünschenswert, wenn die dargestellten numerischen Lösungen im Text noch eingehender erläutert würden.

Den Einstieg in das Buch bilden einige motivierende Beispiele, wobei auch das Phänomen der Stoßentstehung erläutert wird. Im zweiten Kapitel werden anhand der skalaren Erhaltungsgleichung in einer Raumdimension die wesentlichen Konzepte und Probleme der numerischen Approximation dieser Gleichungen mittels Differenzenverfahren dargestellt. Dazu gehören die Entropiebedingungen an die Lösungen, die wichtigen Verfahrenseigenschaften der Konservativität, der Stabilität, der Monotonie sowie die TVD-Bedingung, der Satz von Lax-Wendroff und Ansätze höherer Ordnung für numerische Verfahren. Abschließend wird mit der Stromliniendiffusionsmethode ein Finite-Element-Ansatz für diese Gleichungen betrachtet. Die üblichen Finite-Element-Ansätze führen auf instabile zentrale Differenzen und benötigen deshalb einer upwind-Stabilisierung in irgendeiner Form. Die Stromliniendiffusionsmethode erreicht dieses durch Modifikation der Testfunktionen. Für diese Methode erzielten Johnson und Szepessy [5] einen Konvergenzbeweis mit der Methode der kompensierten Kompaktheit, der im vorliegenden Buch vorgestellt wird.

Das dritte Kapitel behandelt die in der Anwendungspraxis sehr wichtigen Finite-Volumen-Verfahren für skalare Erhaltungsgleichungen in zwei Raumdimensionen. Hier ist auch der oben erwähnte Konvergenzbeweis für gewisse Finite-Volumen-Verfahren zu finden.

In Kapitel vier werden die Verfahren für Systeme für den mathematisch noch etwas beherrschbaren Fall einer Raumdimension eingeführt, insbesondere werden die für Berechnung von Anwendungsproblemen unumgänglichen approximativen Riemann-Lö-

ser diskutiert. Die im fünften Kapitel betrachteten Systeme in mehr als einer Raumdimension sind zwar der Fall, den man in den Anwendung zumeist numerisch berechnen will, für den es aber noch so gut wie keine Theorie gibt. Deshalb mußte die Darstellung zwangsläufig überwiegend auf algorithmische Fragen beschränkt bleiben. Das sechste Kapitel enthält eine kurze Einführung in das schwierige und weitläufige, für die numerische Praxis aber sehr wichtige, Thema der Randbedingungen.

Den Abschluß bildet eine äußerst kurze Darstellung der konvektionsdominierten Diffusionsgleichungen, der singulär gestörten linearen Advektion und den kompressiblen Navier-Stokes-Gleichungen. Zu diesem Thema sind ein Jahr vorher sehr umfangreiche Darstellungen von Morton [9] sowie von Roos, Stynes und Tobiska [10] erschienen. Der Bezug des Kapitels zum Gesamtthema ist zwar klar, das Kapitel wirkt wegen seiner Kürze am Ende aber trotzdem etwas verloren und eher als Anhängsel.

Insgesamt stellt das Buch eine sehr interessante Ergänzung der Lehrbuchliteratur zu diesem noch sehr heterogenen Gebiet der Numerischen Mathematik dar.

[1] DiPerna, R. J.: Measure-valued solutions to conservation laws. *Arch. Rat. Mech. Anal.*, 88, 223–270, 1985
[2] Godlewski, E., Raviart, P. A.: *Hyperbolic Systems of Conservation Laws.* Ellipses, Paris, 1991
[3] Hirsch, C.: *Numerical Computation of Internal and External Flows. Volume 1: Fundamentals of Numerical Discretization.* Wiley, Chichester – New York, 1989
[4] Hirsch, C.: *Numerical Computation of Internal and External Flows. Volume 2: Computational Methods for Inviscid and Viscous Flows.* Wiley, Chichester - New York, 1990
[5] Johnson, C., Szepessy, A.: On the convergence of a finite element method for a nonlinear hyperbolic conservation law. *Math. Comp.*, 49, 427–444, 1987
[6] Kröner, D., Noelle, S., Rokyta, M.: Convergence of higher order upwind finite volume schemes on unstructured grids for scalar conservation laws in several space dimensions. *Numer. Math.*, 71, 527–560, 1995
[7] Kröner, D., Rokyta, M.: Convergence of upwind finite volume schemes for scalar conservation laws in two dimensions. *SIAM J. Numer. Anal.*, 31, 324–343, 1994
[8] LeVeque, R.: *Numerical Methods for Conservation Laws.* Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel – Boston – Berlin, 1990
[9] Morton, K. W.: *Numerical Solution of Convection-Diffusion Problems.*, Band 12 von *Applied Mathematics and Mathematical Computation.* Chapman & Hall, London, 1996
[10] Roos, H.-G., Stynes, M. Tobiska, L.: *Numerical Methods for Singularly Perturbed Differential Equations.*, Band 24 von *Springer Series in Computational Mathematics.* Springer Verlag, Berlin – Heidelberg – New York, 1996
[11] Smoller, J. A.: *Shock Waves and Reaction-Diffusion Equations.*, Band 258 von *Grundlehren der mathematischen Wissenschaften.* Springer-Verlag, New York – Heidelberg – Berlin, 1983
[12] Tartar, L.: The compensated compactness method applied to systems of conservation laws. In: J.M. Ball, Hrsg. , *Systems of Nonlinear Partial Differential Equations.*, Seiten 263–285, Doordrecht, 1983. Reidel-Publ.

Magdeburg G. Warnecke

Fulford, G., Forrester, P., Jones, A., Modelling with Differential and Difference Equations (Math. Soc. Lect. Series 10), Cambridge University Press 1997, 405 S., paperback, £19.95

Den Autoren geht es darum, mathematisches Modellieren anhand spezieller Beispiele aus verschiedenen Disziplinen dem Anfänger näher zu bringen. Dabei wird aus diesen Disziplinen genügend Hintergrundwissen bereitgestellt, so daß auch der Laie den *gesamten* Modellierungsvorgang erfassen kann.

Zu ergänzen ist, daß auch praktisch das gesamte mathematische Rüstzeug (Differentiation und Integration im $\mathbf{R}^1$, letzteres durch Beispiele als Umkehrung der Differentiation eingeführt, lineare und einfache nichtlineare gewöhnliche Differentialgleichungen, lineare Systeme gewöhnlicher Differentialgleichungen, Elementarstes zu Phasenportraits, reelle Folgen, lineare Differenzengleichungen, Linearisierung von Differential- bzw. Differenzengleichungen einschließlich entsprechender Motivationen) in sehr informeller Form bereitgestellt und geübt wird, so daß zumindest die im Buch angesprochenen praktischen Situationen wie auch sehr einfache Erweiterungen vom Anfänger verstanden werden können.

Insgesamt braucht man zum *mathematischen* Verständnis also nur sehr geringe Vorkenntnisse.

Im einzelnen werden u. a. behandelt: Probleme der klassischen Punktmechanik, Rollen und Rollensysteme, gedämpfte und ungedämpfte Hookesche Federn, eindimensionale Wärmeleit- und Diffusionsprobleme (z. B. Isolations- und Mischungsprobleme), Zinses-Zinsprobleme, Bewegungen in viskosen Flüssigkeiten, einfache Modelle der Populationsdynamik (z. B. diskrete und kontinuierliche logistische Gleichungen und Erweiterungen, einfache Räuber-Beute-Situationen), epidemische Modelle (z. B. Verbreitung von Masern in einer Bevölkerung), populationsgenetische Probleme (z. B. Mutation, natürliche Auswahl), (weitere) medizinische Probleme (z. B. Diabetes-Erkennung, Stoffwechsel in der Plazenta). Die gern angeführten Kriegs- und Schlachtenmodelle fehlen leider nicht. Nicht erwähnt werden im jeweiligen Kontext weiterführende bzw. schwierigere verwandte Situationen, die dann fortgeschrittenere mathematische Hilfsmittel erforderten, wie z. B. *räumliche* Diffusion.

Die Autoren gehen folgendermaßen vor: Zunächst schildern sie die allgemeine Situation des zu Modellierenden, fassen die wesentlichen Fakten, auch graphisch ansprechend, zusammen und entwickeln das Modell. Die entsprechenden Argumentationen sind meist, insbesondere für den lernenden Laien, ausreichend motiviert, so daß der Aufmerksame auch imstande sein sollte, zumindest analoge Situationen gleichen Schwierigkeitsgrades selbst modellieren zu können.

Zum Abschluß werden, in der Regel, einige Details des Modells diskutiert.

In der kapitelweise angegebenen weiterführenden Literatur ist dem zuvor erzielten Stand der Modellierfähigkeit entsprechendes Material enthalten, um sich als Modellierer auch an *etwas* komplizierteren Situationen mit Hoffnung auf Erfolg versuchen zu können. Durchgängiger etwas klarere Hinweise, was davon nun zum Selbststudium geeignet ist und was bloße Referenz bleibt, wäre dem Anliegen des Buches dienlich gewesen. Gleiches gilt für die Aufnahme von anspruchsvolleren Problemen in den Übungsteil.

Das Buch steht in einer Reihe mit beispielsweise den Lehrbüchern von Beltrami [1], Braun, Coleman und Drew [2], wobei [1] und [2] mathematisch anspruchsvoller sind. Verwandte genetische Fragestellungen werden, wesentlich weitergehender, in Hofbauer [3] behandelt. All dem steht gegenüber, daß „Modelling ..." dem nicht vorgebildeten Anfänger didaktisch leichter zugänglich sein wird.

Das Buch ist eine gute Ergänzung zu US-amerikanischen Calculus-I-Kursen. Es ist als Grundlage eines Mathematik- oder naturwissenschaftlichen Gymnasialleistungskurses der Klasse 12 sehr zu empfehlen. Das Englische sollte dem nicht allzu abträglich sein. Ebenfalls ist es, trotz oder gerade wegen seines geringen mathematischen Anspruches, für praktisch jedes Publikum, als Grundlage zum Selbststudium, eines Seminars oder als Ausgangspunkt einer allerersten Modellierungsvorlesung gut geeignet.

[1] Braun, Martin; Coleman, Courtney und Drew, Donald (ed.): Differential Equation Models, In: Modules in Applied Mathematics, Vol. 1, New York – Heidelberg – Berlin, Springer Verlag (1983)

[2] Hofbauer, Josef und Sigmund, Karl: The Theory of Evolution and Dynamical Systems, London Mathematical Society Student Texts 7, Cambridge University Press, Cambridge, New York, Rochelle, Melbourne, Sidney (1988)
[3] Beltrami, Edward: Mathematics for Dynamic Modeling, Academic Press (1987)

Essen M. Böhm

Musiela, M., Rutkowski, M., Martingale Methods in Financial Modelling, Theory and Applications (Appl. of Math. Stoch. Modelling and Appl. Probab., Vol. 36), Berlin u. a.: Springer 1997, 512 S., DM 118,-

Die stochastische Finanzmathematik hat in den vergangenen Jahren eine stürmische Entwicklung gesehen: Beginnend mit der bahnbrechenden Arbeit von F. Black, R. Merton und M. Scholes im Jahr 1973 zur Bewertung und Absicherung von Optionen (wofür der Ökonomie Nobel-Preis 1997 verliehen wurde) hat die Verwendung von stochastischen Modellen auf den Finanzmärkten große Bedeutung erlangt. Daran werden auch die spektakulären Miß-Erfolge von Hedge-Funds (z.B. die Krise von Long Term Capital Management im Sommer 1998) nichts ändern: der Einsatz der mathematischen Theorien ist inzwischen ein unverzichtbares Werkzeug für die Bewertung von Derivativen und zum Management und der Kontrolle von Risiko geworden.

Die zugrunde liegende mathematische Theorie ist durchaus anspruchsvoll und hat sich sehr rasch entwickelt. Allerdings existieren bisher nur wenige Monographien, die das Thema für einen breiteren Kreis von Lesern systematisch aufbauen. Ein beliebter Text für Lehrveranstaltungen auf diesem Gebiet ist das 1989 erstmals erschienene Buch von J. Hull [1]. Dieses Buch betont die praktischen Aspekte und versucht auch für Nicht-Mathematiker zugänglich zu sein.

In jüngster Zeit sind jedoch auch einige Text-Bücher erschienen, die mathematisch anspruchsvoller sind ([2], [3], [4]). Das vorliegende Werk von Musiela und Rutkowski enthält die bisher vollständigste Präsentation der mathematischen Theorie der Finanzmarkt Modelle. Auf über 500 Seiten wird in stringenter Weise ein umfassender Überblick geboten.

Im Zentrum der mathematischen Behandlung der Theorie der Finanzmärkte steht der Begriff des Martingals, i.e., der mathematischen Modellierung eines fairen Spiels. Dieser Begriff ist tatsächlich der Angelpunkt für die gesamte moderne stochastische Finanzmathematik. Der Grund liegt im sogenannten „Fundamental Theorem of Asset Pricing", das konzeptuell auf die Arbeiten von Harrisson, Kreps und Pliska um etwa 1980 zurückgeht. Vereinfachend formuliert sagt dieser Satz aus, daß für ein stochastisches Modell eines Finanzmarkts, das keine Arbitrage-Möglichkeiten bietet, ein äquivalentes Wahrscheinlichkeitsmaß gefunden werden kann, unter dem dieses Modell ein Martingal, also ein faires Spiel ist.

Das Buch gliedert sich in zwei große Abschnitte. Während der erste Teil die Bewertung und Absicherung von Derivaten (e.g. Optionen) auf stocks (e.g. Aktien, Fremdwährungen etc.) behandelt, wird im zweiten Teil die Theorie der Derivate auf bonds (i.e., festverzinsliche Wertpapiere) entwickelt. Während im ersten Teil das zugrunde liegende Modell ein reell-wertiger stochastischer Prozeß ist, der die Preisentwicklung des stocks beschreibt, ist der natürliche Rahmen für den zweiten Teil ein (möglicher Weise unendlichdimensionaler) vektorwertiger stochastischer Prozeß, der die zeitliche Entwicklung der Zinskurve beschreibt.

Die ersten 130 Seiten des Buchs sind der Entwicklung der Black-Scholes Formel gewidmet. Der Weg dorthin führt über das elementare Cox-Ross-Rubinstein Modell: durch Diskretisierung der Situation werden dabei alle analytischen und mathematischen

Schwierigkeiten umschifft und auf der Basis von einfacher linearer Algebra die grundlegenden ökonomischen Konzepte, wie z.B. der Begriff „Arbitrage", entwickelt.

Sodann folgen zahlreiche Varianten der Black-Scholes-Situation, insbesondere eine ausführliche Behandlung von Quanto-Optionen, die im Fremdwährungsbereich wesentlich sind, sowie amerikanischen und exotischen Optionen.

Während für Derivate auf stocks das Black-Scholes Modell nach wie vor eine dominierende Bedeutung hat, gibt es im Bereich der Derivate auf bonds kein Referenz-Modell mit einer ähnlichen Bedeutung. In diesem Bereich, in dem die Autoren auch wichtige Originalbeiträge geleistet haben, ist das vorliegende Buch von besonders großem Wert, da es beispielsweise ausführlich und verständlich die Methodologie von Heath-Jarrow-Morton beschreibt. Wir sprechen hier von Methodologie, da es sich nicht um ein spezielles Modell sondern um einen Rahmen für eine ganze Klasse von Modellen handelt. In diesem zweiten Abschnitt des Buchs – der für die Praxis wegen der hohen Liquidität der Bond-Märkte eminent wichtig ist – werden auch Spezialisten zahlreiche neue Informationen finden.

Das vorliegende Werk ist als ausgesprochen gelungen zu bezeichnen und schließt eine Lücke in der bisherigen Lehrbuch-Literatur. Es kann sowohl zum Selbststudium wie auch als Grundlage für ein Seminar über stochastische Finanz-Mathematik dienen. Abschließend weisen wir noch auf das sehr vollständige Literaturverzeichnis (über 700 Titel) hin, das ebenfalls in diesem Umfang erstmalig vorliegt.

[1] Hull, J., (1993) *Options, Futures, and other Derivative Securities.* 3rd ed. Prentice-Hall, Englewood Cliffs (New Jersey)
[2] Lamberton, D., Lapeyre, B. (1993) *Stochastic Calculus Applied to Finance.* Chapman & Hall, Padstow, Cornwall
[3] Karatzas, I., Shreve, S. (1997) *Methods of Mathematical Finance.* Springer, Berlin Heidelberg New York
[4] Baxter, M.W., Rennie, A. (1996) *Financial Calculus. An Introduction to Derivate Pricing.* Cambridge University Press, Cambridge

Wien W. Schachermayer

Yagdjian, K., The Cauchy Problem for Hyperbolic Operators. Multiple Charateristics. Micro-local Approach (Mathematical Topics, vol 12), Berlin: Akademie Verlag 1997, 398 Seiten, DM 130,–

Ziel der vorliegenden Monographie ist eine systematische Einführung in die Theorie der (hyperbolischen) partiellen Differentialoperatoren mit Charakteristiken variabler Multiplizität oder Ordnung. Zentral bei der Behandlung derartiger Operatoren ist die Levi-Bedingung, sie gibt eine gewisse Kontrolle über Terme niedriger Ordnung und gestattet es Fundamentallösungen für das Cauchy-Problem zu konstruieren. Eine wichtige Methode, besser ein wichtiges Hilfsmittel, bildet die „turning point theory" für gewöhnliche Differentialgleichungen. Diese wird ausführlich dargestellt und auch auf weitere Probleme, etwa (lokale) Lösbarkeitsfragen oder Hypoelliptizitätsprobleme, angewandt. Im Mittelpunkt der benutzten Techniken stehen naturgemäß Fourier-Integraloperatoren und mikrolokale Analysis. Im einzelnen gibt es die Kapitel:

1. Fourier integral operators
2. Ordinary differential equations with turning point
3. Fundamental solution of the Cauchy problem for operators with multiple characteristics. Degeneration with respect to time
4. Fundamental solution of the Cauchy problem for hyperbolic operators with multiple characteristics. Degeneration with respect to the spatial variable

5. Necessary correctness conditions for the Cauchy problem for operators with multiple characteristics

Der Gegenstand ist technisch sehr aufwendig, dies macht sich natürlich auch bei der Darstellung bemerkbar. Es liegt sicher kein Buch für Einsteiger vor, aber eine sorgfältig geschriebene Monographie für interessierte Forscher, Spezialisten für hyperbolische partielle Differentialgleichungen werden auf dieses Buch kaum verzichten können.

Neubiberg und Erlangen N. Jacob

Mascarello, M., Rodino, L., Partial Differential Equations with Multiple Characteristics (Mathem. Topics, Vol 13), Weinheim: Wiley-VCH 1997, 352 S., DM 148,–

Thema der vorliegenden Monographie ist das Studium von Singularitäten, lokaler Lösbarkeit und Cauchyproblem für partielle Differentialoperatoren mit charakteristischen Varietäten höherer Vielfachheit.

Das Buch beginnt mit einer lesenswerten motivierenden Einleitung: Hier werden die für das Folgende wesentlichen Modelloperatoren (Schrödinger-, Wärmeleitungs-, Grushin- und Mizohata-Operator und deren Potenzen) und Problemstellungen (Hypoelliptizität und Cauchyproblem) vorgestellt. Klassische Ergebnisse zeigen die Relevanz von Termen niederer Ordnung für die betrachteten Probleme auf.

Der einführende erste Teil des Buches umfaßt die Kapitel 1 bis 4. Kapitel 1 enthält die grundlegenden Räume und Begriffe, insbesondere Distributionen, Gevrey-Ultradistributionen und Kerne, C^∞-, Gevrey- und analytische Wellenfronten. Kapitel 2 stellt dem Leser die Kernfragen des Buches vor: Hypoelliptizität in klassischer und mikroanalytischer Formulierung, lokale Lösbarkeit und das Cauchyproblem. Die beiden ersten Kapitel sind weitgehend wörtlich dem Buch Rodino [1] entnommen, wobei Beweise und Literaturhinweise gestrichen wurden.

Hörmanders Pseudodifferentialoperatoren (ΨDO) der Klasse $S^m_{\rho,\delta}$, der zugehörige Kalkül und ihre Operation auf Mikrofunktionen und Mikrosupport werden in Kapitel 3 behandelt, wobei nun die wesentlichen Beweise vorgeführt werden. Das Kapitel schließt mit den entsprechenden Operatorklassen im analytischen bzw. Gevrey-Rahmen (zu den Beweisen wird hier auf [1] verwiesen). Der Aufbau des technischen Apparates endet mit der Einführung von Fourierintegraloperatoren (FIO) in Kapitel 4. Wesentliche Themen sind: Aktion von FIO auf ΨDO und Wellenfronten, Anwendung auf das Cauchyproblem für strikt hyperbolische Operatoren, kanonische Abbildung und Konjugation durch FIO, Invarianz des Hauptsymbols und Invarianten niederer Ordnung (im zentralen Abschnitt 4.3), Resultate für principle type Operatoren.

Der Hauptteil des Buches umfaßt die Kapitel 5 bis 8. Ziel ist die Untersuchung von Operatoren mit charakteristischen Varietäten konstanter Vielfachheit (und Kodimension 1) d.h. als mikrolokales Modell des Hauptsymbols dient das Produkt eines elliptischen Symbols $e_1(x,\xi)$ und einer Potenz eines principle type Symbols erster Ordnung $a_1(x,\xi)$. Den Kern des Buches bildet Kapitel 5. Es beginnt mit der Einführung einer mikrolokalen Version der Levi-Bedingung für die Terme niederer Ordnung und den Konsequenzen für Hypoelliptizität, Ausbreitung von Singularitäten und lokale Lösbarkeit. In den Abschnitten 5.2 bis 5.6 werden diese Fragen für Operatoren studiert, deren Subhauptsymbol nicht verschwindet, für die also die Levi-Bedingung nicht gilt. Das Kapitel schließt mit einem Abschnitt zum Cauchyproblem.

In Kapitel 6 werden Störungen von Potenzen des Mizohata-Operators betrachtet. Diese sind immer analytisch mikrohypoelliptisch und G^s-mikrohypoelliptisch für s nahe 1, während die C^∞-Hypoelliptizität von den Termen niederer Ordnung abhängt. Insbe-

sondere läßt sich so ein analytisch-hypoelliptischer, aber nicht C^∞-hypoelliptischer Operator finden. In Abschnitt 6.3 wird mit Abschätzungen vom Gevrey-Typ gezeigt, daß Operatoren mit dem obigen Modell-Hauptsymbol nicht lokal lösbar in den Distributionen sind, falls dies für $a_1(x, \xi)$ gilt. Kapitel 8 enthält Resultate zur Mikrohypoelliptizität von Operatoren mit nicht involutiver charakteristischer Varietät der Kodimension $k \geq 2$.

Das Buch endet mit einem kurzen Kapitel zu verwandten Fragen und offenen Problemen und einer ausführlichen Literaturliste.

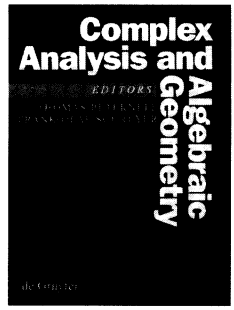
Das vorliegende Buch ist sorgfältig geschrieben und gut aufgebaut. Die (notwendigerweise) technischen Beweise sind klar gegliedert und gut lesbar. Rückgriffe auf klassische Beispiele und Ergebnisse sowie die Betonung von Modelloperatoren erleichtern den Einstieg in dieses faszinierende Gebiet und zeigen eindrucksvoll die Stärke der mikrolokalen Methoden. Das Buch ist uneingeschränkt zu empfehlen, sofern der Leser über solide Grundkenntnisse der Theorie der Distributionen und Gevrey-Ultradistributionen verfügt.

[1] Rodino, L.: Linear partial differential operators in Gevrey spaces. World Scientific Publishers, Singapur 1993.

Oldenburg M. Langenbruch

Complex Analysis and Algebraic Geometry

A Volume in Memory of Michael Schneider



EDITED BY THOMAS PETERNELL AND FRANK-OLAF SCHREYER

2000. 24 x 17 cm. X, 406 pages. Hardcover.
DM 298,– /EUR 152,36 /öS 2175,– /sFr 265,–
USA, Canada, Mexico. US$ 148.95
• ISBN 3-11-016204-0

The volume consists of invited refereed papers dedicated to the memory of Michael Schneider. The contributions cover a wide spectrum in complex analysis and algebraic geometry; the main focus is on:

- Higher dimensional varieties and Kähler geometry
- Moduli spaces and deformation theory
- Surfaces and 4-manifolds
- Real algebraic geometry

A part of the articles grew out of a symposium in honour of Michael Schneider, held in Bayreuth in June 1998 with about 80 participants.

Contents

Price is subject to change.

WALTER DE GRUYTER GMBH & CO. KG
Genthiner Straße 13 · D–10785 Berlin
Tel. +49-(0)30-2 60 05–0
Fax +49-(0)30-2 60 05–251
Internet: www.deGruyter.de

W DE G de Gruyter
Berlin · New York

Subscription Information

Journal of Group Theory ISSN 1433-5883

2000. Volume 3 (4 issues). 24 x 17 cm. Approx. 450 pages.
Annual subscription rate: *DM 338,- /EUR 172,82 /öS 2467,-/ sFr 301,-/US$ 179.00 plus postage and handling.
Single issue: DM 85,-/EUR 43,46/öS 621,-/sFr 77,-/US$ 45.00 plus postage and handling.

**Prices include online edition at no additional charge. For information on obtaining online access please see www.deGruyter.de/journals/ejform.html* Prices subject to change