107. Band Heft 3, September 2005 D 20577

# Jahresbericht

## der Deutschen Mathematiker-Vereinigung

3 – 2005

Herausgegeben von K. Hulek
unter Mitwirkung von
U. Gather, H.-Ch. Grunau, H. Lange,
J. Rambau, A. Schied, Th. Sonar

Teubner

# 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, Berichte aus der Forschung und Buchbesprechungen veröffentlicht werden.

**Manuskripte:**

Alle für die Schriftleitung des Jahresberichts bestimmten Briefe und Manuskripte sind an *Prof. Dr. K. Hulek* zu richten. Für Buchbesprechungen ist *Prof. Dr. H. Lange* zuständig. Bücher, von denen eine Besprechung erfolgen soll, werden bei den Verlagen angefordert.
Die Autoren werden gebeten, für Manuskripte und Buchbesprechungen die **Standard-LATEX-Klasse article mit 10pt (default), \textwidth139mm, \textheight205mm** zu benutzen. Sollen 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. Ein Foto des Autors sollte als Bilddatei in einem der gängigen Grafikformate (am unproblematischsten: TIF-Format; Graustufenbild mit einer Auflösung von mindestens 300 dpi) oder als normaler Papier-Fotoabzug zum Einscannen mitgeschickt werden. Als Datenträger sind ZIP-Disketten, CD-ROM bzw. Syquest (88 oder 200 MB) möglich.
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.

Weitere Informationen zum „Jahresbericht" finden Sie unter
http://www.mathematik.uni-bielefeld.de/DMV/jb/index.html

**Verlag:**

B. G. Teubner Verlag/GWV Fachverlage GmbH
Abraham-Lincoln-Straße 46
65189 Wiesbaden
http://www.teubner.de
http://www.gwv-fachverlage.de

*Geschäftsführer:* Andreas Kösters, Albrecht F. Schirmacher
*Verlagsleitung:* Dr. Heinz Weinheimer
*Gesamtleitung Anzeigen:* Thomas Werner
*Gesamtleitung Produktion:* Reinhard van den Hövel
*Gesamtleitung Vertrieb:* Gabriel Göttlinger

**Marketing/Sonderdrucke:**

Eva Brechtel-Wahl
Telefon: (06 11) 78 78-3 79
Fax: (06 11) 78 78-4 39
E-Mail: eva.brechtel-wahl@gwv-fachverlage.de

**Abonnentenverwaltung:**

(Änderungen von Adressen und Bankverbindung, Rückfragen zu Rechnungen oder Mahnung)
VVA-Zeitschriftenservice, Abt. D6F6 / Jahresbericht der Deutschen Mathematiker-Vereinigung, Postfach 7777, 33310 Gütersloh
Ursula Müller
Telefon: (0 52 41) 80-19 65
Fax: (0 52 41) 80-96 20
E-Mail: ursula.mueller@bertelsmann.de

**Bezugsbedingungen:**

Die Zeitschrift erscheint 4mal jährlich zum Jahresabonnementpreis von € 107,– (172,90 sF o. MwSt.) 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: Wilhelm & Adam, Heusenstamm

ISSN 0012-0456

## Inhalt

Jahresbericht der Deutschen Mathematiker-Vereinigung, 107. Bd. 2005, Nr. 3

Jahresbericht der Deutschen Mathematiker-Vereinigung, 107. Bd. 2005, Nr. 3

**In den nächsten Heften erscheinende Arbeiten**

**M. Grötschel:** MATHEON: Introducing the DFG Research Center „Mathematics for key technologies"
**L. A. Imhof:** Evolutionary Game Dynamics under Stochastic Influences
**J. Pach:** Directions in Combinatorial Geometry

---

**Anschriften der Herausgeber**

Prof. Dr. K. Hulek, Institut für Mathematik, Universität Hannover, Welfengarten 1, 30167 Hannover
E-Mail: hulek@math.uni-hannover.de

Prof. Dr. Ursula Gather, Lehrstuhl für Mathematische Statistik und industrielle Anwendungen, Universität Dortmund, 44221 Dortmund
E-Mail: gather@statistik.uni-dortmund.de

Prof. Dr. H.-Ch. Grunau, Institut für Analysis und Numerik, Otto-von-Guericke-Universität Magdeburg, Postfach 4120, 39016 Magdeburg
E-Mail: hans-christoph.grunau@mathematik.uni-magdeburg.de

Prof. Dr. Herbert Lange, Mathematisches Institut, Friedrich-Alexander-Universität Erlangen-Nürnberg, Bismarckstraße 1a, 91054 Erlangen
E-Mail: lange@mi.uni-erlangen.de

Prof. Dr. J. Rambau, Fakultät für Mathematik, Physik und Informatik, Universität Bayreuth, 95440 Bayreuth
E-Mail: rambau@zib.de

Prof. Dr. A. Schied, Institut für Mathematik, Technische Universität Berlin, Straße des 17. Juni 136, 10623 Berlin
E-Mail: schied@math.tu-berlin.de

Prof. Dr. Th. Sonar, Institut für Analysis, Technische Universität Braunschweig, Pockelsstraße 14, 38106 Braunschweig
E-Mail: t.sonar@tu-bs.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 347 b, POB 810, NL-2160 SZ Lisse/Holland

---

Jahresbericht der Deutschen Mathematiker-Vereinigung, 107. Bd. 2005, Nr. 3

# Vorwort

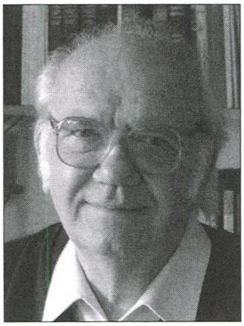
Das Thema dieses Hefts ist die Gruppentheorie.

In einem historischen Aufsatz berichtet P. Roquette über die „erstaunliche Karriere von Otto Grün“, der nie ein Universitätsstudium absolviert, aber dennoch bleibende Beiträge zur Gruppentheorie geliefert hat. Grün kam über das Fermatsche Problem zur Mathematik und hatte das große Glück, mit H. Hasse einen interessierten und hilfreichen Korrespondenten und späteren Gesprächspartner zu finden. Vom Fermatschen Problem verlagerte sich dann das Interesse von Grün zur Gruppentheorie. Mitte der 30er Jahre veröffentlichte er die Sätze, die später als der „erste“ und „zweite“ Grünsche Satz bekannt wurden und umgehend Eingang in die Lehrbuchliteratur fanden. Insgesamt veröffentliche O. Grün 26 Arbeiten, von denen die meisten der Gruppentheorie gewidmet sind. P. Roquette hat den Nachlass von Hasse in der Universitätsbibliothek in Göttingen gesichtet und stieß dabei auch auf die Korrespondenz zwischen Hasse und Grün. Dies ist der Ausgangspunkt dieses Aufsatzes.

Einen ganz anderen Aspekt der Gruppentheorie behandelt der Aufsatz von B. Eick. Sie gibt einen Überblick über „Computational Group Theory“. Gerade im Bereich der endlichen Gruppen haben computergestützte Untersuchungen wesentlich zur Weiterentwicklung des Gebiets beigetragen. Dies betrifft auch die Konstruktion und Klassifikation der endlichen einfachen Gruppen. So beruhte beispielsweise der erste Existenzbeweis für das Baby Monster u. a. auf Computerberechnungen. Neben innermathematischen Themen diskutiert Frau Eick auch Anwendungen in der Kristallographie und der Kryptograpie.

Wie immer enthält auch dieses Heft eine Reihe von aktuellen Buchbesprechungen.

K. Hulek



# From FLT to Finite Groups

## The remarkable career of Otto Grün

**Peter Roquette**

## Abstract


- Mathematics Subject Classification: 01 A 70, 11-03, 20-30
- Keywords and Phrases: Biographies, number theory-historical, group theory-historical


Every student who starts to learn group theory will soon be confronted with the theorems of Grün. Immediately after their publication in the mid 1930s these theorems found their way into group theory textbooks, with the comment that those theorems are of fundamental importance in connection with the classical Sylow theorems. But little is known about the mathematician whose name is connected with those theorems. In the following we shall report about the remarkable mathematical career of Otto Grün who, as an amateur mathematician without having had the opportunity to attend university, published his first paper (out of 26) when he was 46. The results of that first paper belong to the realm of Fermat's Last Theorem (abbreviated: FLT). Later Grün switched to group theory.

Eingegangen: 9. 3. 2005

Peter Roquette, Mathematisches Institut der Universität, Im Neuenheimer Feld 288, D-69120 Heidelberg, Germany, roquette@uni-hd.de

DMV
JAHRESBERICHT DER DMV

## Contents

# 1 Introduction

Students who start to learn the theory of finite groups will soon be confronted with the theorems of Grün, at least with Grün's "first" and "second" theorem. These theorems found their way into group theory textbooks immediately after their publication in the mid 1930s, with the comment that they are of fundamental importance in connection with the classical Sylow theorems. But little if anything is known about the mathematician whose name is connected with those theorems.

Recently, scanning through the legacy of Helmut Hasse which is kept at the University Library in Göttingen, I found 50 letters which were exchanged between Hasse and Grün, from 1932 to 1972. Hasse is known to have had an extended correspondence, freely exchanging mathematical information with his colleagues. Thus at first sight, I was not really surprised to find the name of Otto Grün among Hasse's many correspondence partners.

But while reading these letters there unfolded to me much more than just mathematical information, namely the remarkable and fascinating story of a mathematician, quite rare in our time, who was completely self-educated, without having attended university, and nevertheless succeeded, starting at age 44, to give important contributions to mathematics, in particular to group theory.

I am writing this article in order to share this discovery with other interested mathematicians. But I would like to make it clear that it is not meant to be a complete biography of Otto Grün. This article comprises mainly what we can conclude from the correspondence files of Hasse and some secondary sources, with emphasis on the genesis of Grün's main theorems. Perhaps a more detailed search of other sources could bring to light more facets of Grün's personality and work.

Acknowledgement: I had sent a former version of this article to a number of people who had met Grün and still remember him. I would like to thank all colleagues for their interest and for their various comments on the work and the personality of Grün. In particular I would like to thank B. Huppert and W. Gaschütz for their help concerning the group theoretic part of Grün's work. It seems to me that a more detailed survey of Grün's role in the development of group theory would be interesting and worthwhile. Last but not least I would like to thank the referee for several well founded comments.

# 2 The first letters: FLT (1932)

## 2.1 Grün and Hasse in 1932

Little is known about the early life of Grün. In his vita which he wrote in 1955 we read:

> Ich bin am 26. Juni 1888 zu Berlin geboren, besuchte das Friedrich-Werdersche Gymnasium zu Berlin, das ich 1908 mit dem Reifezeugnis verließ. Zunächst widmete ich mich dem Bankfach, nahm am ersten Weltkriege teil, ohne Schäden davonzutragen, und war weiterhin kaufmännisch tätig.

> *I was born on June 26, 1888 in Berlin. I attended the Friedrichs-Werder Gymnasium in Berlin until 1908. Then I worked in the banking business, participated in the first world war without being injured, and afterwards continued to work in a commercial job.*[1]

It is not known what kind of job this had been. There is some rumor that it had to do with butcher's business but we could not find any evidence for this. Grün continued:

> Da ich stets lebhaftes Interesse für mathematische Fragen hatte, beschäftigte ich mich nebenbei wissenschaftlich und kam auf diese Art zu einem Briefwechsel mit dem berühmten Algebraiker Helmut Hasse ...

> *All the time I had strong interest in mathematical problems, and in my spare time I occupied myself with scientific problems. In the course of this activity there started an exchange of letters with the famous algebraist Helmut Hasse...*[2]

The first letter of Otto Grün to Hasse is dated March 29, 1932, from Berlin. At that time Grün was (almost) 44 years old.

Helmut Hasse, 10 years younger than Grün, at that time was professor of Mathematics at the University of Marburg (since 1930) as the successor of Kurt Hensel. The years in the late twenties and early thirties are to be regarded as the most fruitful period in Hasse's mathematical life. Hasse had completed the last part of his class field theory report [Has30a], he had proved (with Richard Brauer and Emmy Noether) the Local-Global Principle for simple algebras [BHN32], he had determined the structure of cyclic algebras over a number field [Has32], he had discovered local class field theory [Has30b], given a new foundation of the theory of complex multiplication [Has26b], [Has31], and more. In Hasse's bibliography we have counted more than 50 papers in the period from 1926 to 1934. In March 1932, when he received Grün's first letter, he had just completed his seminal paper dedicated to Emmy Noether on her 50th birthday [Has33a], where he presented a proof of Artin's Reciprocity Law in the framework of simple algebras and at the same time determined the structure of the Brauer group over a number field. Now he was preparing his lecture course on class field theory which he was to deliver in the summer semester of 1932, the notes of which [Has33b] would be distributed widely and would influence the further development of class field theory. One year later, in March 1933, Hasse would prove the Riemann hypothesis for elliptic function fields.

It seems remarkable that in the midst of all this activity, Hasse found the time to deal carefully with the letters of Otto Grün, whom he had never heard of before. Hasse had the strong viewpoint that every letter from an amateur mathematician represents an unusual interest in mathematics by the sender and, hence, has to be taken seriously. And so he did with Grün's letter, thereby discovering that the sender was not one of the

[1] Here and in the following we use our own free translation of German text into English.

[2] I have found the vita which starts with the cited sentences, in the archives of the University of Würzburg where Grün had a teaching assignment (*Lehrauftrag*) during the years from 1954 to 1963 (see section 7.3 below). It is dated August 2, 1955. I do not know the occasion for which Grün had presented this to the university. Probably it was connected with his teaching assignment. – I am indebted in particular to Hans-Joachim Vollrath for his help to obtain access to the Würzburg archives.

usual *Fermatists* but, despite his lack of formal mathematical education, was unusually gifted and had a solid mathematical background.

## 2.2 Vandiver's conjecture and more

Grün's first letter begins as follows:

> Sehr geehrter Herr Professor! Ich habe aus Ihren Arbeiten die Takagische Klassenkörpertheorie kennengelernt. Ich glaube nun, auf dieser Grundlage zeigen zu können, daß auch im irregulären Körper $k(\zeta)$ der $\ell$-ten Einheitswurzeln der 2-te Faktor der Klassenzahl nie durch $\ell$ teilbar sein kann. Darf ich Ihnen vielleicht hier ganz kurz den Beweis skizzieren, zumal da ich als reiner Amateurmathematiker denselben doch nicht veröffentlichen würde.
>
> *Dear Herr Professor! From your papers I have learned Takagi's class field theory. I believe that on this basis I can show that also in the irregular field $\mathbb{Q}(\zeta)$* [3] *of the $\ell$-th roots of unity the 2nd factor of the class number can never be divisible by $\ell$. May I sketch briefly the proof since anyhow, as an amateur mathematician, I am not prepared to publish it ...*

By "class number" Grün means the number of ideal classes of the $\ell$-th cyclotomic field $\mathbb{Q}(\zeta)$ where $\zeta$ denotes a primitive $\ell$-th root of unity, $\ell$ being an odd prime. It is well known since Kummer [Kum50] that the class number $h$ of $\mathbb{Q}(\zeta)$ has a product decomposition

$$h = h_1 h_2$$

where the second factor $h_2$ equals the class number of the maximal real subfield $\mathbb{Q}(\zeta + \zeta^{-1})$. The first factor $h_1$ is a positive integer, called the "relative class number".[4] The prime $\ell$, or the field $\mathbb{Q}(\zeta)$, is called "regular" if the class number $h$ is not divisible by $\ell$. One of the monumental achievements of Kummer [Kum50] was the discovery that FLT holds for a regular prime number $\ell$, which is to say that the diophantine equation

$$x^\ell + y^\ell + z^\ell = 0$$

is not solvable in integers $x, y, z \neq 0$.

If $\ell$ is regular then, of course, both factors $h_1$ and $h_2$ are not divisible by $\ell$. If $\ell$ is irregular then it was known to Kummer already that $h_1$ is divisible by $\ell$, but nothing much was known about $h_2$. Now Grün claimed that $h_2$, even in the irregular case, is *not* divisible by $\ell$. This statement is today known as "Vandiver's conjecture", and it is considered quite important with respect to the structure of cyclotomic fields.[5]

[3] Grün writes $k(\zeta)$ (in conformity with the older notation) where we have written $Q(\zeta)$ (which is today's notation). In the interest of the reader we shall freely change notations from the original, whenever it seems appropriate for better understanding.

[4] The terminology "first" and "second" factor of the class number is generally used in the literature. But Hasse in his book [Has52] says that the inverse enumeration would be more natural: $h_2$ should be called the "first" and $h_1$ the "second" factor. In later letters (1957/58) Grün uses therefore this inverse terminology. Hasse himself in [Has52] writes $h*$ for $h_1$ and $h_0$ for $h_2$. Ribenboim [Rib79] writes $h^+$ for $h_2$.

[5] I am indebted to Franz Lemmermeyer for pointing out to me the paper [Van41] in which Vandiver expresses his "hope" that $h_2$ is always prime to $\ell$. Ribenboim [Rib79] remarks that Vandiver's conjecture is already stated in a letter of Kummer to Kronecker, dated December 28, 1849.

Thus in effect Grün claimed to have proved Vandiver's conjecture, although he did not mention Vandiver in his letter. Most probably he was not aware at that time of Vandiver's work.

Hasse replied on April 1, 1932 already, three days after Grün had dispatched his letter. We do not know the text of Hasse's letter[6] but from Grün's answer we can deduce that Hasse had pointed out the proof to be erroneous. Grün wrote on June 27, 1932:

> Gegen Ihre Bedenken kann ich natürlich nichts einwenden; der Beweis ist eben in der vorliegenden Form mißglückt.
>
> *Of course there cannot be any objection against your doubts. Thus my proof has not been successful in this form.*

In fact, Vandiver's conjecture has not been proved or disproved until today, despite strong efforts by many mathematicians.[7]

But Hasse had not been content just to point out the error in Grün's proof. He had added some comments for further work. Maybe he also recommended to Grün some of the relevant literature. For, Grün wrote in his second letter to Hasse (June 27, 1932) the following:

> ...glaube ich aus Ihrem Hinweis eine Folgerung für die Fermatsche Behauptung ziehen zu können, die ich Ihnen gern mitteilen möchte ... Wenn $x^\ell + y^\ell + z^\ell = 0$ in rationalen Zahlen $x, y, z$ und etwa $x$ durch $\ell$ teilbar, $yz$ prim zu $\ell$ ist, so muß der zweite Faktor der Klassenzahl durch $\ell$ teilbar sein ...
>
> *...in view of your comments I believe that I can derive the following result towards Fermat's Last Theorem which I would like to communicate to you ... If $x^\ell + y^\ell + z^\ell = 0$ is solvable in nonzero rational integers $x, y, z$ and $x$ is divisible by $\ell$ while $yz$ is not divisible by $\ell$ then the second factor of the class number is divisible by $\ell$.*

In dealing with the Fermat equation one usually distinguishes two cases: In the "first case" one assumes that none of $x, y, z$ is divisible by $\ell$. In the "second case" one of them, say $x$, is divisible by $\ell$ whereas $y, z$ are not. Thus Grün's claim says in effect:

> *If the second class number factor $h_2$ is not divisible by $\ell$ then the Fermat equation is not solvable in the so-called second case.*

And he sketched a proof of this result. But again, there was an error which Hasse pointed out to him in a letter two days later.

We should keep in mind that Grün had not received any formal mathematical education; mathematically he was completely self educated and this was the first occasion where he could discuss his ideas with a competent mathematician. The subject required a high level of sophistication, and after all he had no training in presenting mathematical ideas. Thus the failure of his first attempts to produce a consistent proof is under-

[6] Quite generally, the letters from Grün to Hasse are preserved in the Hasse legacy, whereas many of the letters from Hasse to Grün have to be considered as lost. Only in later years, in case the letters were written by typewriter, Hasse used to make a carbon copy for himself and so his letters are preserved too. But this was not the case for his early letters to Grün which were handwritten. In most cases however, by interpolating from Grün's replies we can deduce approximately what Hasse had written.

[7] By now the conjecture has been verified for all odd primes $\ell < 12 \cdot 10^6$ (communication by Franz Lemmermeyer).

standable. He was lucky to have found Hasse as his correspondence partner who, it seems, had recognized the mathematical capacity of the author of those letters.

After some more months, on September 28, 1932 Grün wrote again. He said that he had indeed observed the difficulty which Hasse had pointed out to him but had erroneously assumed that this could be handled by the methods of Kummer. Nevertheless, he now presented a correction of his result, namely with an additional hypothesis concerning certain divisibility properties of Bernoulli numbers.

The sequence of Bernoulli numbers $B_n$ can be defined as the coefficients appearing in the power series expansion:

$$\frac{x}{e^x - 1} = \sum_{n \geq 0} B_n \frac{x^n}{n!} .$$

These $B_n$ are certain rational numbers which are well known to be connected with the structure of the cyclotomic field $\mathbb{Q}(\zeta)$. Kummer had used the $B_n$ to formulate a necessary and sufficient criterion for $\ell$ to be regular. Namely, the numbers $B_2, B_4, \ldots B_{\ell-3}$ should not be divisible by $\ell$.[8] Kummer had also discussed the irregular case to some extent, and there too he had given sufficient criteria for the validity of FLT.

Now Grün's additional hypothesis reads as follows:

> Es mögen zwar beliebig viele Bernoullische Zahlen $B_i$ mit $i < \ell - 1$ durch $\ell$ in erster Potenz teilbar sein, jedoch gelte für keine von ihnen $B_{\ell i} \equiv 0 \bmod \ell^3$ bei geradem $i$.
>
> *Arbitrary many Bernoulli numbers $B_i$ with $i < \ell - 1$ may be divisible by $\ell$, but for none of them we have $B_{\ell \cdot i} \equiv 0 \bmod \ell^3$ with i even.*

It was well known, already to Kummer, that this hypothesis implies certain structural properties of the group of units of $\mathbb{Q}(\zeta)$. Grün showed that it is sufficient (in addition to the hypothesis that the second class number factor $h_2$ is not divisible by $\ell$) to deduce that the Fermat equation for exponent $\ell$ has no solution in the second case.[9]

This time Hasse did not find an error in Grün's proof. But he wanted to be sure that Grün's result was new. Perhaps Hasse remembered a paper by Vandiver [Van29] which in fact contained Grün's above cited result. But Grün's computations yielded at the same time a somewhat more general result than we have cited above, showing the impossibility not only for the Fermat equation in the second case, but also for certain other diophantine equations within the cyclotomic field $\mathbb{Q}(\zeta)$, going beyond Vandiver's results. Hence, even if Grün's result for the Fermat equation was known, perhaps his more general result was new?

Thus Hasse proposed that Grün should write to Vandiver at the University of Texas who was considered to be a specialist on those problems. Grün replied that he is afraid not to know the proper mathematical terminology in English language, and anyhow he does not know the address of Vandiver. Upon this Hasse himself wrote to Vandiver on behalf of Grün. Since several years Hasse had exchanged reprints with Vandiver and, as

[8] If the index $n > 1$ is odd then $B_n = 0$. Because of this, the enumeration of the Bernoulli numbers is sometimes changed, i.e., writing $B_n$ instead of $B_{2n}$ for $n > 1$. But we will keep the notation as given by the definition above.

[9] Ribenboim [Rib79] (p.188) says erroneously that Grün's result refers to the first case.

can be seen from the correspondence between the two, the latter had visited Hasse at least twice, once in Halle and another time in Marburg.[10]

Vandiver replied in a letter of November 14, 1932:

> *The two theorems you mention appear to be quite new. The first one seems to be a modification and extension of the Theorem I of my paper of the year 1929 in the Transactions A. M. S.*

Here Vandiver cites his paper [Van29].

This must have been sufficient for Hasse. Perhaps he was aware of the fact that one year earlier, in 1931, Vandiver had been awarded from the American Mathematical Society the highly prestigious Cole Prize in number theory for his work on FLT, in particular for his paper in the Transactions which Vandiver was citing in his letter. If Grün's result was an extension of Vandiver's then certainly, it should be published. Thus Hasse decided to accept Grün's manuscript for Crelle's Journal.

However, in the form as presented so far Grün's manuscript seemed not publishable. Hence Hasse would first do what he always used to do as an editor of Crelle's Journal: He would study the paper carefully and on that basis give advice to the author to produce a text which, in his opinion, meets the standards of scientific publication.[11] But he needed some time for this. Grün replied in a letter of December 19, 1932:

> Vielen Dank für Ihr freundliches Schreiben von 12. Ich bin Ihnen sehr verpflichtet, wenn Sie sich dem Beweis zum Fermatproblem weiter widmen wollen und es ist selbstverständlich, daß Sie jede Frist dazu haben.
>
> *Thank you very much for your kind letter of 12. I would be very obliged to you if you would continue to attend to my proof on Fermat's problem, and it is clear that there will be no time limit for this.*

We should note that just in this period, the last months 1932 and the first months of 1933, Hasse was busy with his attempts to prove the Riemann hypothesis for curves. We have reported in [Roq04] that in November 1932, when Hasse gave a colloquium lecture in Hamburg, he had a conversation with Artin who pointed out to him that his (Hasse's) research project on diophantine congruences was in fact equivalent to the proof of the Riemann hypothesis for the curves in question. This comment by Artin had decidedly changed the viewpoint of Hasse. He went to work intensively on this idea with the result that already in March, 1933 he arrived at his first proof for elliptic curves. In view of this we can understand that Hasse in this period tended to postpone, if possible at all, other obligations including the reading and correcting of Grün's manuscript. It was May 1933 until he turned to Grün's manuscript again.

[10] Vandiver too, like Grün, did not have a formal mathematics education. In the biography of Vandiver (1882–1973) in [Leh74] we read: *"This remarkable man ... was self-taught in his youth and must have had little patience with secondary education since he never graduated from high school."* However, already with 22 years Vandiver wrote his first mathematical paper whereas Grün was 47 when his first paper appeared.

[11] Rohrbach [Roh98] reports: *"With his* [Hasse's] *characteristic conscientiousness, he meticulously read and checked the manuscripts ... word by word and formula by formula. Thus he very often was able to give all kinds of suggestions for improvements to the authors, concerning contents as well as form."* The correspondence Hasse-Grün gives ample witness of this.

Grün's paper [Grü34b] appeared in 1934. The date of submission is recorded as May 17, 1933. His result in the final form reads as follows. As above, $\ell$ denotes an irregular prime number and $\zeta$ a primitive $\ell$-th root of unity. Let $k_0 = \mathbb{Q}(\zeta + \zeta^{-1})$.

> *If the second class number factor $h_2$ is prime to $\ell$ and if none of the Bernoulli numbers $B_{\ell n} \equiv 0 \bmod \ell^3$ (for $n = 2, 4, \ldots, \ell - 3$) then the equation*
>
> $$\varepsilon(\zeta - \zeta^{-1})^m \alpha_1^\ell + \alpha_2^\ell + \alpha_3^\ell = 0$$
>
> *is not solvable in algebraic integers $\alpha_1, \alpha_2, \alpha_3 \in k_0$ which are prime to $\ell$, provided $m \geq 3\ell - 1$ and $\varepsilon$ is a unit in $k_0$.*

This was Grün's first publication. Compared with the other existing literature on FLT it cannot be rated as exceptional. Grün followed the known footsteps in the direction which had been pointed out by Kummer in the mid 19th century and his result was close to that of Vandiver [Van29]. But we should keep in mind that FLT had not yet been proved generally at that time. Hence any partial result which points towards the validity of FLT was welcomed, even if the progress compared with former results seemed to be small.

However, if we consider that Grün had originally not been aware of Vandiver's paper and that his result contained Vandiver's, then we have to rate Grün's achievement as extraordinary – in particular if we remember that he had no formal mathematical training and had reached his high status of expertise through self-education.

## 3 From FLT to finite groups (1933)

In a letter of December 6, 1932 Grün started to discuss other problems; these belong to general class field theory and are only indirectly connected with FLT. Here we will not go into all details but restrict our discussion to the following two topics.

### 3.1 Divisibility of class numbers: Part 1

Grün wrote:

> ... Ich möchte noch einen Satz beweisen, der vielleicht gelegentlich gebraucht werden kann: Wenn $K$ den Körper $k$ enthält und kein Zwischenkörper existiert, der über $k$ Abelsch mit der Relativdiskriminante 1 ist, so ist die absolute Klassenzahl von $K$ durch die absolute Klassenzahl von $k$ teilbar.
>
> *... I would like to prove yet another theorem which may be useful occasionally: If $K$ contains the field $k$ and there is no proper intermediate field which is abelian over $k$ and of relative discriminant 1 then the class number of $K$ is divisible by the class number of $k$.*

This is quite interesting. We know that five years earlier Artin had observed the same fact, and he had found it worthwhile to communicate it to Hasse. Let us cite from Artin's letter of July 26, 1927:

> Nun etwas anderes, das mir großen Spaß bereitet hat und das ich gestern im Heckeseminar erzählte. Das Resultat scheint, so trivial der Beweis ist, neu zu sein. Eine ganz kindische Vermu-

tung jedes Anfängers ist doch diese: Ist $k$ Unterkörper von $K$, so ist die Klassenzahl von $k$ ein Teiler der Klassenzahl von $K$. Ich möchte zeigen, daß dies "fast" immer richtig ist, mehr noch:
**Satz:** Enthält $K/k$ ... keinen in bezug auf $k$ Abelschen und gleichzeitig unverzweigten Zwischenkörper, so besitzt die Gruppe der absoluten Idealklassen von $K$ eine Faktorgruppe isomorph mit der Gruppe der absoluten Idealklassen in $k$.

*Now something else which I had talked about yesterday in Hecke's seminar with great fun. The result seems to be new in spite of the simplicity of proof. A very childish expectation of every beginner is the following: If k is a subfield of K then the class number of k divides the class number of K. Now I show that this is true "almost always", and even more:*
**Theorem:** *If $K|k$ ... does not contain any intermediate field which is abelian and at the same time unramified then the class group of K admits a factor group isomorphic to the class group of k.*

Artin proceeds in his letter to describe a proof which, as he had said, is quite simple. After checking we found that Grün's proof was the same as Artin's. The essential fact to be used in the proof is that, under the hypothesis of the theorem, the absolute class field of $k$ is linearly disjoint to $K$. It seems that Hasse in his reply to Grün had mentioned Artin, for Grün wrote in his next letter (December 19, 1932) that he did not wish to claim priority.[12]

Thus again, on his way teaching himself algebraic number theory, Grün had found for himself a theorem which was familiar to the specialists, this time Artin. Note that Artin had never published his proof.

But there had been a recent publication by Chevalley [Che31] containing the same theorem. Certainly Hasse, who at that time was in close contact with Chevalley, knew about Chevalley's paper, and perhaps he had pointed out that paper to Grün after receiving Grün's letter. At first sight Chevalley's proof looks somewhat different than that of Artin-Grün but at closer inspection we find that it is essentially the same[13]. Chevalley mentions that the same result would be contained in a forthcoming paper by Herbrand which we have found to be Théorème 2 in [Her32]; there Herbrand used it for a new foundation of Kummer's theory of ideal classes in cyclotomic fields. After checking we found that again, Herbrand's proof is the same as Artin's and Grün's.

From all we know about Grün we have no doubt that he had found his proof independently, i.e., independent not only of Artin but also of Chevalley and of Herbrand. Grün in his letter cites Hilbert who in his *Zahlbericht* [Hil97] § 117, page 378 [14] mentions that Kummer had stated the above theorem for the subfields $K$ of $\mathbb{Q}(\zeta)$ but that Kummer's proof was incorrect.[15] Of course, Kummer's theorem is an immediate consequence of the general theorem of Artin-Grün since $\mathbb{Q}(\zeta)$ is purely ramified.

[12] "Ich wollte den Satz nicht als mein geistiges Eigentum angesehen wissen."

[13] The difference between Chevalley's and Artin's arguments can be described as follows: Let $k'$ be the absolute class field of $k$. Artin uses only the fact that $k'$ is abelian and unramified over $k$, and that these properties are preserved after extending the base field from $k$ to $K$ – which directly implies the result. Chevalley uses the *Verschiebungssatz* (shift theorem) of class field theory in order to describe $Kk'$ explicitly as class field over $K$. Thus he uses more machinery from class field theory than Artin-Grün. However, if one comes to think of it, the proof of the *Verschiebungssatz* in this special case reduces to the argument of Artin-Grün and so, in this sense, we may regard both proofs as essentially the same.

[14] The page number refers to the original *Zahlbericht* whereas its copy in the "Collected Papers" of Hilbert has different pagination.

But in Kummer's case, i.e., for subfields of $\mathbb{Q}(\zeta)$ where $\zeta$ is a prime power root of unity, the theorem had been proved much earlier by Furtwängler [Fur08]. Although in 1908 class field theory was not yet completed by the theorems of Takagi and Artin, enough was known to prove the divisibility of class numbers which Kummer had conjectured. It seems that neither Artin nor Grün had been aware of Furtwängler's proof. But Hasse did know it, for in Hasse's diary we have found an entry dated October 10, 1925 with the title: *The ideal class groups of relatively abelian fields. (Generalization of a theorem of Furtwängler.)*[16] There, Hasse proved the Artin-Grün theorem in the special case when $K|k$ is abelian. Thereby he regards $K$ as class field over $k$, thus he used still more machinery from class field theory. As it turned out in the proof of Artin-Grün, this is not necessary. Here again, as it is the case so often in Mathematics, the generalization (omitting the assumption that $K|k$ is abelian) leads to a simplified proof.[17]

### 3.2 Divisibility of class numbers: Part 2

In his next letter of December 19, 1932 Grün mentions another problem concerning class numbers. While his above mentioned result yields a lower bound of the class number $h$ of $K$ (it is divisible by the class number of a subfield under certain conditions), he now claimed to have an upper bound for $h$ (under certain conditions it divides the class number of a subfield times a certain factor dependent on the structure of the Galois group). This time, however, he is not sure that his arguments are correct, and so he writes:

> Aber ich gestehe Ihnen, verehrter Herr Professor: Ich traue meinen eigenen Ergebnissen nicht; die Sätze sind mir zu überraschend. Ich kann aber, soviel ich mich auch bemühe, den Fehler nicht finden. Und deshalb bitte ich Sie, mir zu sagen, ob und wo in meiner Rechnung ein Fehler steckt.

> *But I admit, dear Herr Professor, that I do not trust my own results: the theorems are very surprising to me. However I cannot find the error although I have tried to. Therefore I am asking you to tell me whether and where there is an error in my computations.*

The situation is the following: $K|k$ is a Galois extension of number fields[18]. Let $K'$ be the maximal subextension which is abelian over $k$. Grün proved:

> *Suppose that the class group of $K$ is cyclic. Then the class number $h$ of $K$ divides the product of the class number $h'$ of $K'$ with the relative degree $[K : K']$.*

Actually Grün wrote that he assumed the cyclicity of the class group of $K$ "for simplicity only", and claimed that his proof could be extended to cover the case of an arbi-

[15] The same reference to Hilbert's *Zahlbericht* we have found in Artin's letter to Hasse, cited above.
[16] At the end of this entry Hasse later had added a reference to Artin's letter of July 26, 1927 which we have cited above.
[17] By the way, the Artin-Grün theorem with the same proof appears in [ACH65]. There, Hasse cites the letter of Artin and also his own diary entry of October 10, 1925.
[18] Grün considered only the case $k = \mathbb{Q}$.

trary class group. However that is not the case. Hasse pointed out this fact to Grün, and we shall see below that this led to remarkable consequences.

In the case of a cyclic class group of $K$, Grün's proof turned out to be correct. But it seems that Hasse was not sure whether this result was known already, since he proposed to put this theorem as a problem in the *Jahresbericht* of the DMV. [19] At that time, the *Jahresbericht* provided a section where any member could state a problem, and the incoming solutions were published in the next issue. Quite often such problems were posed even if the author had already obtained a solution, but he wished to find out whether a solution, possibly simpler, was known already.

Grün consented and Hasse submitted the theorem (for cyclic class group of $K$) under the name of Grün as a problem, which appeared as no. 153 in vol. 43 (1934) of the *Jahresbericht.* Promptly there were two solutions received, published in volume 44, one of L. Holzer and the other of A. Scholz, both being renowned number theorists. It turned out that both solutions were essentially the same as Grün's original proof in the letter to Hasse, and were independent of class field theory.

The proof is short and straightforward: One has to use the fact that the automorphism group of a cyclic group is abelian and, hence, the commutator group $G'$ of the Galois group $G$ of $K|k$ acts trivially on the ideal class group of $K$. Consequently, if $c$ is any divisor class of $K$ then the norm $N_{K|K'}(c)$ equals $c^{[K:K']}$ and therefore, since $N_{K|K'}(c)$ is a divisor class of $K'$, we have that $c^{[K:K']h'}$ is the principal class. Hence the exponent of the class group of $K$ divides $[K:K']h'$. Since the class group of $K$ is assumed to be cyclic the contention follows.[20]

But the result seems to be quite special because of the assumption that the class group of $K$ is cyclic. Therefore Hasse proposed to Grün to investigate the general case, with class group of arbitrary structure. Clearly, whenever a subgroup $G_1$ of $G$ can be found which acts trivially on the class group of $K$ then a similar argument can be applied to obtain an upper bound for the exponent of the class group of $K$ (not necessarily for the class number $h$ itself), with $K'$ being replaced by the fixed field $K_1$ of $G_1$.

### 3.3 Representations over finite fields

On April 19, 1933 Grün answered that his attempts to deal with non-cyclic class groups had not been successful. However after some time, on December 5, 1933 he wrote:

> Nach langer Zeit kann ich Ihnen heute wieder etwas berichten. Ich habe mich mit gruppentheoretischen Untersuchungen beschäftigt ... Ich knüpfe an an meine Aufgabe No.153 im Jahresbericht. Als ich Ihnen damals das Resultat mitteilte, stellten Sie die Frage: "Wie lautet das genaue Analogon für allgemeine Abelsche Klassengruppen?" Um dieses Problem handelt es sich hauptsächlich.
>
> *After a long time I am able again to report something to you. I have been busy with group theoretical questions ... I refer to my problem no. 153 in the Jahresbericht. When I had reported to you*

[19] DMV = *Deutsche Mathematiker Vereinigung* = German Mathematical Society.
[20] I am indebted to Franz Lemmermeyer for the information that Yamamura had rediscovered and used this theorem of Grün. See [Yam97], p.421. Lemmermeyer himself has used (and proved) this theorem in [Lem97], Prop.6, citing Grün.

*on that result, you asked: "What is the exact analogue for arbitrary abelian class groups?" The following is mainly concerned with this question.*

And Grün continues with a description of his results. Let $G$ be a finite group which acts on an abelian group $A$ of exponent $p$, a prime number. (We observe that Grün discussed, as a first step, not arbitrary abelian class groups but only $p$-groups of exponent $p$, i.e., vector spaces over $\mathbb{F}_p$.) Let $m$ be the rank of $A$. For any prime $\ell \neq p$ let $m_\ell$ denote the order of $p$ mod $\ell$. Grün wrote that indeed he has found general statements about subgroups of $G$ which act trivially on $A$. He proved:

*If $\ell > \frac{m}{m_\ell}$ then the commutator group of an $\ell$-Sylow group of $G$ acts trivially on $A$. In other words:*

If $\ell > \frac{m}{m_\ell}$ then the $\ell$-Sylow groups of the automorphism group of $A$ are abelian.

Hasse had Grün's manuscript refereed by Magnus who at that time was already considered to belong to the leading German mathematicians in the field of group theory.[21] Hasse asked him whether Grün's result has appeared already in the literature. Magnus replied that he knew only one source, an American paper by Brahana [Bra34], which dealt with similar problems. Brahana's result appears as a special case of Grün's. And he added (letter of December 16, 1933):

> ... Ich finde die Sache wirklich sehr hübsch, auch der von ihm angegebene Beweis des schon von Brahana gefundenen Spezialfalls ... scheint mir etwas durchsichtiger zu sein als bei B., und wenn sich die Ergebnisse auf Klassenkörperprobleme anwenden lassen, wäre das ja besonders erfreulich.

> *... I regard the matter as quite nice. Also, Grün's proof in the special case which had already been found by Brahana ... seems to me to be somewhat more transparent than B.s proof. And if Grün's results can be used in class field theory then this would be particularly nice.*

Obviously Hasse had written to him that he expects Grün's results to be applicable in class field theory. In fact, as we have seen, Grün's group theoretical problem arose from a question about class numbers.

Grün in his letter also mentions that in addition to the above result, he has determined the structure of *all* Sylow groups, not only those for large $\ell$, of the automorphism group of an abelian $p$-group $A$ of exponent $p$. Moreover, all those results are valid for the automorphism group of any vector space of finite dimension over an arbitrary finite field of characteristic $p$.

In fact, this is the content of the paper which Hasse finally accepted for Crelle's Journal, already in the same year [Grü34a].

We see that Grün's main interest had by now shifted to group theory – in consequence of Hasse's question. The application to class field theory, he writes, will be given later. But he never did so. It seems that from now on group theory absorbed all his interest.

[21] Wilhelm Magnus in Frankfurt had received his doctorate 1931 with Max Dehn as his supervisor. The correspondence between Hasse and Magnus is preserved; it had started in 1930 when Magnus submitted his dissertation [Mag30] for publication to Hasse as an editor of Crelle's Journal.

## 4 The two classic theorems of Grün (1935)

More than one year later, on March 30, 1935, Grün submitted to Crelle's Journal another manuscript on group theory. This has turned out to become a classic and made his name widely known [Grü35].

There are two main parts of the paper. In the first part he gives a direct generalization of what we have discussed in the foregoing section (and what had already appeared in Crelle's Journal). Namely, he dropped the condition on the $G$-module $A$:

Let $G$ be a finite group which acts on an abelian $p$-group $A$ of arbitrary structure, not necessarily of exponent $p$. Let $m$ denote the rank of $A$. Let $\ell$ be a prime $\neq p$. Then:

*If $k$ is the smallest exponent with $\ell^k > \frac{m}{m_\ell}$ then the $k$-th commutator group of an $\ell$-Sylow group of $G$ acts trivially on $A$.*

The paper contains an even further generalization, namely for an arbitrary $p$-group $A$, not necessarily abelian, on which $G$ acts. Then one has to consider the ascending central series of $A$, and in the condition for $\ell^k$ the number $m$ has to be defined as the maximal rank of the factor groups of that series.

### 4.1 The second theorem of Grün

But the main results of this paper are to be found in the second part where we find the two famous "Theorems of Grün".

Given a finite group $G$ and a prime number $p$, the problem is to describe the structure of its maximal abelian $p$-factor group $G/G^{(p)}$. Here, $G^{(p)}$ denotes the $p$-commutator group of $G$. This description turns out to be particularly simple for groups which have a property which is called "$p$-normal".[22] This property is defined as follows: *the center $C$ of a $p$-Sylow group $P$ of $G$ coincides with the center of any other $p$-Sylow group in which $C$ is contained.* Grün proves:

*If $G$ is $p$-normal then the maximal abelian $p$-factor group $G/G^{(p)}$ is isomorphic to the maximal abelian $p$-factor group $N_C/N_C^{(p)}$, where $N_C$ denotes the normalizer of the center $C$ of a $p$-Sylow group $P$ of $G$.*

The idea behind this is that a $p$-Sylow group $P$, its center $C$ and the normalizer $N_C$ are in general much smaller and easier to handle than the whole group $G$. Hence this theorem yields a criterion for a group $G$ to have a non-trivial $p$-factor group, namely: this is the case if and only if $N_C$ has this property. Note that $N_C$ contains $C$ as an abelian normal subgroup, thus we have the situation which Grün considered in the first section of this paper, and that result is applicable to $N_C$ acting on $C$.

If in particular the $p$-Sylow group $P$ of $G$ is abelian and is contained in the center of its normalizer then $G$ is $p$-normal and it follows the isomorphism $G/G^{(p)} \approx P$ which is a classical theorem of Burnside, and was well known also to Grün. In this sense Grün's

[22] This terminology had been proposed by Hasse (letter to Grün of May 28, 1935).

theorem can be regarded as a generalization of Burnside's theorem – and a far reaching generalization at that.

The above theorem is usually called the "second theorem of Grün" although in Grün's paper it is proved first, whereas the "first theorem of Grün" is what Grün proves afterwards. The switch in the enumeration is probably due to Zassenhaus[23] who in his group theory text book [Zas37] included the two theorems of Grün and introduced the enumeration used today. This makes sense since Grün's second theorem (in Zassenhaus' enumeration) can be regarded as a corollary of his first theorem.

## 4.2 The first theorem of Grün

The "first theorem" of Grün gives a description of $G/G^{(p)}$ for an arbitrary finite group $G$, not necessarily $p$-normal. This is somewhat more complicated than in the case of a $p$-normal group. Namely:

*For an arbitrary finite group $G$, its maximal abelian p-factor group $G/G^{(p)}$ is isomorphic to the following abelian factor group of its p-Sylow group $P$:*

$$G/G^{(p)} \approx P/P^{\star} ,$$

*where the normal subgroup $P^{\star} \subset P$ can be described as*

$$P^{\star} = (P \cap N'_P) \prod_{\sigma \in G} (P \cap \sigma^{-1} P' \sigma) .$$

Note that here appears the normalizer $N_P$ of the whole $p$-Sylow group $P$ in $G$ (not only $N_C$). As usual, $P'$ denotes the commutator group of $P$, and similarly $N'_P$ is the commutator group of $N_P$.

Admittedly, this result looks somewhat complicated because of the definition of $P^{\star}$. Nonetheless it has turned out to be quite important in group theory, in as much as it shows that the maximal abelian $p$-factor group of any group $G$ can be found as an explicitly given factor group of the (usually much smaller) $p$-Sylow group $P$. Its kernel $P^{\star}$ depends very much on how the $p$-Sylow group $P$ is embedded into the group $G$.

We have already said that Zassenhaus, who at that time was writing a textbook on group theory, immediately recognized the importance of Grün's theorems and decided to include them into his book [Zas37].[24]

While reading this paper of Grün one can observe that its style is quite different from that of his other papers. The paper is well written, careful in the use of notations, and it contains several diagrams which nowadays are known as "Hasse diagrams". The explanation of this is, that the manuscript, in the form as published, had been entirely written by Hasse himself.

[23] Hans Zassenhaus got his doctorate 1934 under the supervision of Artin. From 1934 to 1936 he worked at the University of Rostock, and there he wrote his famous text book on group theory.
[24] Zassenhaus, in his paper [Zas35b] on finite near-fields, had already discussed certain results centered around the classical Burnside theorem as mentioned above. This may explain Zassenhaus' great interest in results of the kind of Grün's theorems.

### 4.3 Hasse and the transfer

We have already said that Hasse, being an editor of Crelle's Journal, used to check every manuscript carefully before sending it to print. So he did also with Grün's manuscripts, and in particular with the manuscript under discussion. After all, Grün as an amateur had no experience with writing a paper. The letters of the Hasse-Grün correspondence show that Hasse worked quite hard to put this paper into shape. After an extended exchange of letters there were so many corrections, additions and deletions that the original manuscript was hardly readable any more. Finally Hasse, seemingly somewhat exasperated, proposed that he himself will now compose a new manuscript. To which Grün replied (letter of May 18, 1935):

> Ihre Mitteilung, daß Sie ein neues Ms. herstellen wollen, hat mich zwar einerseits hoch erfreut, aber – darf ich denn das annehmen? . . . Ich weiß wirklich nicht, ob ich das zugeben darf. Wir müßten natürlich auch Ihre tätige Mitarbeit ausdrücklich vermerken. In jedem Falle . . .: Wenn Sie von Ihrer eigenen Zeit etwas opfern wollen, müssen Sie die betr. Sache schon für sehr wichtig halten. Das ist das beste Lob, das ich mir denken kann.
>
> *On the one hand, I am very glad about your proposition that you will compose a new manuscript but – could I accept this? . . . Really, I do not know whether I am allowed to give my consent. Of course, we would have to state explicitly your extensive cooperation. In any case . . .: If you will spend your own time on this then you must consider it very important. This is the best praise from you which I can imagine.*

Hasse replied on May 21, 1935:

> Ich halte es wirklich für das Beste, wenn ich hier ein neues Manuskript herstelle. Die Arbeit daran würde mir Freude machen und Sie brauchen sich darüber keine Gedanken zu machen. Dies in der Arbeit selbst zu erwähnen, würde mir nicht zusagen. Sie mögen das so auffassen, daß es zu meinen Aufgaben als Herausgeber gehört, wenn man diese im weiteren Sinne auslegt.
>
> *Indeed, I believe it is the best solution if I will write a new manuscript here. It will be a pleasure to me and you do not have to worry about it. But I would not like that this be mentioned in the paper. You might regard it as belonging to my tasks as an editor, if one interprets them in a wider sense.*

Certainly, Hasse regarded Grün's results as important and this was one of his motivations to help Grün to put it into a form which would be appreciated by the mathematical public. But another reason which required a complete rewriting of the manuscript, was Hasse's proposition that the *transfer map* (*Verlagerung*) should be used as an adequate tool which provides the isomorphisms of Grün's theorems. For, in his original version Grün had not used the transfer and not obtained those isomorphisms, but he was content with saying that if one of the two factor groups (which we now know to be isomorphic) is non-trivial then the other is non-trivial too.

The transfer $V_{G \to H}$ from $G$ to a subgroup $H$ is a group homomorphism from $G$ into the factor commutator group $H/H'$. It can be defined as the determinant of the canonical monomial representation of $G$ modulo $H$ with coefficients in $H/H'$. It had first been constructed and used by Schur in 1902, as a variant of Burnside's method who used the monomial representation with coefficients being roots of unity (i.e., a one-dimensional representation of $H$). Later in 1927 the transfer was re-discovered by Artin and Schreier during their attempts to prove the conjectured principal ideal theorem of class field theory. We know this from Artin's letter to Hasse of August 2, 1927. See also Artin's paper [Art29]. It seems that neither Artin nor Hasse were aware of the old paper by Schur because they never mentioned it in their letters nor in their publications. Artin was able, by means of his general reciprocity law, to reformulate the principal ideal theorem as a purely group theoretical statement concerning the transfer.[25] Hasse in his class field report II [Has30a], p. 170 introduced the name "*Verlagerung*" for this group theoretical map, which then was translated into English as "transfer".

By 1935 the transfer map was a well established tool but apparently it was used mainly in number theory in connection with the principal ideal theorem and related questions. It seems that in abstract group theory it had not yet found many applications (except in Schur's paper mentioned above). But this changed after Grün's paper.

In Grün's letter of May 18, 1935 we read:

> Haben Sie vielen Dank für Ihre Briefe und die darin enthaltenen wertvollen Anregungen. Der Gedanke, die Theorie der Verlagerung heranzuziehen, ist außerordentlich glücklich. Ich hatte ja auch bei meinem Beweis von Satz 5 ähnliche Wege eingeschlagen, ohne aber diese Theorie wirklich zu benutzen. Die Verlagerungstheorie gestattet, in einfacher Weise die Sätze 4 und 5 voll zu beweisen. Für Satz 4 haben Sie dies ja schon liebenswürdiger Weise so weit durchgeführt, ...
>
> *Many thanks for your letters and the valuable suggestions therein. The idea to use the transfer theory is extraordinarily fortunate. In my proof of theorem 5 I had used similar methods but without really using that theory. Transfer theory leads to simple complete proofs of theorems 4 and 5. In case of theorem 4 you have already kindly done it so far, ...*

Grün proceeds to expound in detail the proofs which Hasse had indicated using transfer theory. And later in this letter he writes:

> Natürlich muß aber [in der Arbeit] in jedem Falle darauf hingewiesen werden, daß die Anwendung der Theorie der Verlagerung auf Ihre Anregung hin erfolgt ist und ich somit diese eleganten Beweise Ihnen verdanke.
>
> *Of course, it should be mentioned [in the paper] that the application of transfer theory is due to your suggestion and that, hence, I owe these elegant proofs to you.*

But Hasse replied:

> ... scheint es mir aus sachlichen Gründen notwendig, in einer Fußnote zu erwähnen, daß der Gedanke, die Verlagerung bei den Beweisen von Sätzen Burnside'scher Art zu benutzen, von Herrn Ernst Witt, Göttingen, stammt.
>
> *... I find it necessary to mention in a footnote that the idea to use the transfer in the proofs of theorems like Burnside's is due to Mr. Ernst Witt, Göttingen.*

Whereupon Grün, in a footnote to his paper [Grü35], inserted the following text:

> Den Gedanken, bei diesem Beweis die ursprünglich von mir verwendeten monomialen Darstellungen durch die Verlagerung zu ersetzen, verdanke ich einer Mitteilung von H. Hasse. Dieser wurde seinerseits geleitet durch eine mündliche Mitteilung von E. Witt, wonach sich der

[25] One year later, in 1928, Furtwängler [Fur29] succeeded to prove this group theoretical statement. Later there were simplifications of Furtwängler's proof, one also by Magnus [Mag34], but the most significant one by Iyanaga [Iya34]. (By the way, Iyanaga says in the introduction that the greater part of his paper is due to Artin.)

klassische Beweis des Burnsideschen Satzes in ganz entsprechender Weise einfacher und durchsichtiger gestalten läßt.

*The idea to replace the monomial representations (which I originally used) by the transfer map, arose from a suggestion of H. Hasse. He had been led by an oral communication of E. Witt who pointed out that the classical proof of Burnside's theorem can similarly be simplified.*[26]

There is another footnote, after the statement of the "first theorem of Grün", reading as follows:

Diesem Satz und seinem Beweis hat Herr Hasse die vorliegende Form gegeben. Ich habe mich ursprünglich darauf beschränkt, bei den gemachten Voraussetzungen eine zyklische $p$-Faktorgruppe nachzuweisen.

*This theorem and its proof has been put into the present form by Mr. Hasse. Originally I had been content with showing, under the assumptions as stated, the existence of a cyclic p-factor group.*

By this Grün means a non-trivial cyclic factor group of $P/P^*$ as a necessary and sufficient condition that $G/G^{(p)}$ is non-trivial. Certainly, the idea to establish group isomorphisms (when possible) instead of only considering the group orders, is part of the "Modern Algebra" which had been propagated by Emmy Noether and had found its expression in van der Waerden's text book [vdW31]. Hasse explained this to Grün in his letter May 28, 1935 as follows:

Entgegen Ihren brieflichen Andeutungen sehe ich allerdings doch das Hauptgewicht Ihrer Sätze in der Herleitung von notwendigen und hinreichenden Bedingungen für die *isomorphe Übertragung* von Untergruppen oder Faktorgruppen innerhalb $P$ auf Faktorgruppen von $G$, und nicht so sehr in der bloßen Folgerung auf die *Ordnungen* dabei. Daher habe ich in den Formulierungen immer nur die Isomorphiebehauptungen angeführt und meine, man kann es ruhig dem Leser überlassen, die daraus ohne weiteres ablesbaren Folgerungen für die Ordnungen zu ziehen.

*Contrary to your hints in your letters I regard the main point of your theorems to be the isomorphic transport of subgroups and factor groups within P to factor groups of G, and not so much in the mere consequence for the group orders. Therefore, I have formulated all the theorems as referring to isomorphisms. In my opinion it can be left to the reader to draw from this the consequences concerning the group orders ...*

Finally on June 7, 1935, when the manuscript seemed to have acquired a form satisfactory to both, Grün wrote:

Lieber Herr Professor Hasse! Vielen Dank für die Übersendung des Manuskriptes und Durchschlages. Jetzt ist doch wirklich etwas aus meiner ursprünglichen Arbeit geworden. Ich gestehe Ihnen, daß ich erst nun wirkliche Freude an 'meinem' Manuskript habe.

[26] Burnside's theorem (as explained in section 4.1) can be found in his book [Bur11], §243. The computations performed there are indeed the same as computing the kernel and the image of the transfer map in the special situation at hand. However, Burnside does not mention (nor does he care) that this is a general procedure, referring to a generally defined map. Therefore, if it is said that the definition of the transfer map goes back to Burnside, such statement has to be interpreted with appropriate caution. It takes some insight to realize that Burnside's arguments indeed can be looked at as evaluating a homomorphic map. We do not know whether Witt had known Schur's paper [Sch02] or whether he had observed this himself.

*Dear Professor Hasse! Many thanks for the manuscript and carbon copy. Really, now there has developed something out of my original paper. I have to admit that only now I have real pleasure with 'my' manuscript ...*

But the correspondence about this continued and several points had still to be cleared. It took until August 13, 1935, after more than 18 letters [27] had been exchanged between Hasse and Grün concerning this manuscript, that finally Grün could send the corrected proof sheets to Hasse. The paper appeared in the same year 1935 in Crelles Journal [Grü35].

We have reported about this part of the Hasse-Grün correspondence in a somewhat greater detail, since it does not seem to be widely known to what extent Hasse had a share in Grün's classic paper. The title of the paper is:

"*Contributions to group theory I.*" (Beiträge zur Gruppentheorie I.)

In one of his letters Grün had announced that there will be a second and perhaps more parts of such "contributions". But the next he submitted in 1943 only (due to the problems in war time it appeared in 1945; see [Grü45]). Later in the course of time Grün produced 10 such "contributions", the last appearing 1964 again in Crelle's Journal, when Grün was 74.[28]

### 4.4 Grün, Wielandt, Thompson

Let us jump 4 years ahead to the Göttingen group theory conference in 1939.[29] There on June 27, 1939, Wielandt[30] delivered a talk with the title: "$p$-Sylow groups and $p$-factor groups". This is precisely the topic of Grün's classic paper [Grü35] which we just have discussed. In fact, Wielandt presented (among other results) a far reaching generalization of Grün's result. The main theorem of Wielandt ist somewhat involved and we do not reproduce it here. One of its many consequences concerns the case when a $p$-Sylow group $P$ of $G$ is *$p$-regular* in the sense of Ph. Hall. This means that

$$x^p y^p \equiv (xy)^p \bmod \langle x, y\rangle'^{\,p}$$

holds for every $x, y \in P$. (In other words: The operation "$p$-th power" can be performed termwise, modulo a product of $p$-th powers of commutators from the group generated by $x$ and $y$.) Under this assumption it follows from Wielandt's main results that *the maximal $p$-factor group of $G$ is isomorphic to the maximal $p$-factor group of the normalizer $N_P$.* Note that here the $p$-factor groups in question may be non-abelian whereas

[27] This means that 18 letters have been preserved, 6 of them by Hasse and 12 by Grün. Those letters of Hasse which are preserved are written with typewriter, and Hasse had made carbon copies. Probably another six letters by Hasse were handwritten and, hence, not preserved.

[28] In Grün's enumeration there were "Contributions" no. I–IX and XI published, but not no. X. We do not know his plans for no. X.

[29] For more on this conference see section 6.2.

[30] Helmut Wielandt had studied in Berlin with I. Schur and was awarded his doctorate in 1935. In 1939, the year of the Göttingen group conference, he held a position of assistant at the University of Tübingen.

Grün's results refer to abelian $p$-factor groups only. Wielandt achieves this by manipulating the monomial representation directly in a suitable way, not only the transfer map which is the deterninant of the monomial representation.

Wielandt's talk was published 1940 in [Wie40] . It is evident that Wielandt's paper is directly influenced by Grün's [Grü35].

The following text is contained in a letter of B. Huppert to the author:

> Eines der Ziele von Wielandt wird in dieser Arbeit mit keinem Wort erwähnt, nämlich die Nilpotenz des Frobenius-Kerns einer Frobenius-Gruppe. Diese wurde zuerst von J. Thompson bewiesen. Im Sommer 1958 gab es in Tübingen eine lange Unterhaltung zwischen Wielandt und Thompson. Unmittelbar danach sagte Wielandt zu mir: "Das ist ein sehr scharfsinniger Bursche, von dem kann man etwas lernen." Einige Monate später reichte Thompson seine Arbeit bei der Mathematischen Zeitschrift zur Publikation ein. Demnach gibt es eine ganz deutliche mathematische Verbindungslinie von Grün über Wielandt bis zu Thompson.

> *One of Wielandt's motivations is not mentioned at all in this paper [Wie40], namely to prove the nilpotency of the Frobenius kernel of a Frobenius group. This was proved later only by J. Thompson [Tho59]. In the summer of 1958 there was a long discussion in Tübingen between Wielandt and Thompson. Immediately thereafter Wielandt said to me: "This is a very sharp-witted guy, from him one could learn a lot." Several months later Thompson submitted his paper [Tho59] to Wielandt for publication in the Mathematische Zeitschrift. Thus we can observe very clearly a line of mathematical influence from Grün over Wielandt to Thompson*[31].

## 5 Grün meets Hasse (1935)

### 5.1 Hasse's questions

Grün, in his first letter to Hasse, had introduced himself as an amateur mathematician. But it seems that Hasse, impressed by Grün's achievements, had some doubts by now. Although there had been an exchange of letters since three years, he did not know anything definite about Grün's mathematical background. So Hasse at last asked in his letter of May 8, 1935:

> ... Sind Sie eigentlich Mathematiker von Hauptberuf, oder treiben Sie die Mathematik nur nebenbei als Liebhaberei?

> ... *By the way, are you a mathematician by profession, or are you doing Mathematics as a hobby?*

To which Grün replied (letter of May 9):

> Ich wollte, verehrter Herr Professor, ich wäre Mathematiker von Hauptberuf. Leider ist das nicht der Fall, ich muß mich ohne besondere Begeisterung kaufmännisch betätigen, um zu leben.

[31] *Added in Proof:* R. W. van der Waall has pointed out to me that the line of mathematical development which started with Grün's paper can be traced much further. There are quite a number of subsequent papers continuing the ideas of Grün and supplementing his results. Of particular interest is the following result contained in a paper by T. Yoshida published in the Journal of Algebra 52 (1978), pp.1–38. It says that the transfer isomorphism $G/G^{(p)} \approx N_P/N_P^{(p)}$ holds quite generally, with exceptions possible only if $P$ admits a factor group isomorphic to the wreath product of the cyclic group of order $p$ with itself. Indeed this is a very strong generalization of the first theorem of Grün. The transfer map and its dual have become standard tools in the theory of finite groups.

*... I would wish, dear Herr Professor, that I could be a professional mathematician. Unfortunately this is not the case; I have to work for a living in a commercial job, though without particular enthusiasm.*

But Hasse continued to inquire (letter of May 13):

Wo haben Sie sich denn Ihre mathematischen Kenntnisse erworben? Haben Sie einen bestimmten Mathematiker zum "Lehrer" gehabt?

*... But where did you pick up your mathematical knowledge? Have you had a "teacher" who was a mathematician?*

Grün's reply (letter of May 15):

Ob ich einen bestimmten "Lehrer" gehabt habe? Ich habe meine Kenntnisse nur aus Büchern geschöpft und da sind Sie selbst zu einem großen Teil mein Lehrer gewesen. Ich bekam zufällig Ihre beiden Berichte in die Hand und damit begann mein intensives Interesse für Klassenkörpertheorie. Natürlich war ich mathematisch so weit vorgebildet, daß ich fähig war, die Berichte durchzuarbeiten. Die außerordentliche Klarheit und Durchsichtigkeit Ihrer Darstellung nimmt ja dem Leser jede Arbeit ab. Bis dahin hatte ich mich eigentlich mehr für Funktionentheorie interessiert, allerdings hatte ich wenigstens Hilberts "Zahlbericht", Dirichlet, Dedekind und die einzelnen Kummerschen Arbeiten gelesen. Nun wurden Ihre Berichte für mich Veranlassung, mich intensiv mit Gruppentheorie zu befassen.

*... Whether I have been taught by a particular teacher? I have acquired my knowledge from books only, and there to a large degree my teacher has been you. Your two reports*[32] *came by chance into my hands, and this started my intensive interest in class field theory. Of course I had already acquired enough of the mathematical prerequisites which enabled me to read your reports. After all, the wonderful clarity and transparency of your presentation spares the reader much of the work. Until then I tended to have more interest in the theory of complex functions, but I had already read Hilbert's "Zahlbericht", Dirichlet, Dedekind and various papers by Kummer.*[33] *Now your reports had induced me to look intensively into group theory.*

When Grün states that his interest in group theory had been induced by Hasse's class field report, then we see that by now he had well grasped the main trend in the then "modern" class field theory, as expressed in the foreword to Part II of that report:[34]

*Artin's Reciprocity Law constitutes an advance of the utmost importance. Its importance lies not so much in the direction which might be suggested by the name "reciprocity law" and its classical formulation, but in the general class field theory. The ultimate aim of it is the coding of all arithmetical properties of a relative abelian number field in its Galois group, similarly as the aim of Galois theory is the coding of field theoretic properties in the Galois group.*

However, Grün's mathematical interests had now shifted from FLT and class field theory almost entirely to group theory. The application to class field theory does not appear in his further publications. In group theory Grün had found his main subject where he would be active in the future. A majority of 21 of his total of 26 papers from 1934 to 1964 belong to group theory.

[32] Grün refers to Hasse's class field reports, the first on Takagi's class field theory [Has26a], and the second on Artin's reciprocity law [Has30a].

[33] At that time, the "Collected Papers" of Dirichlet and Dedekind were available, but not yet Kummer's. The latter would be published in 1975 only, edited by André Weil.

[34] The following is a free translation of essential features of Hasse's foreword of [Has30a]. – The reader may compare this with Hasse's foreword in his book on abelian fields [Has52] .

## 5.2 Grün's visit

In view of this correspondence, Hasse now wished to meet Grün personally, in particular since Grün had announced to have many more results in his files. For, in his letter of May 9, 1935 Grün had written:

> Nach der Veröffentlichung meiner beiden Noten über den Fermat und Gruppen im Galoisfeld hat mir das Kultusministerium eine gewisse Unterstützung zuteil werden lassen, die mich in Stand setzte, mich einige Zeit fast ausschließlich mathematischen Untersuchungen zu widmen. Die Folge ist, daß ich geradezu eine Unmenge von Notizen habe, in denen die wesentliche Vorarbeit für eine Veröffentlichung schon geleistet ist; alle diese Arbeiten sind gruppentheoretischer Natur, natürlich mit körpertheoretischen Anwendungen.
>
> *After publication of my two notes on Fermat and on groups in a Galois field the ministry of education had granted me a certain stipend which enabled me to devote almost all my time to mathematical work. As a consequence I have a huge pile of notes which already contain the essential ingredients of future publications. All of this work is of group theoretical nature, of course with applications to field theory.*[35]

So Hasse wrote on May 13, 1935:

> Wir haben hier in diesem Semester gerade eine kleine Arbeitsgemeinschaft über Gruppentheorie, in der wir mit Ihren Untersuchungen sehr verwandte Dinge betreiben, insbesondere die beiden neuen gruppentheoretischen Arbeiten von Zassenhaus studieren, die im letzten Heft der Abhandlungen des Hamburger Mathematischen Seminars erschienen sind.
>
> *In this semester we have here a small workshop on group theory, on topics which are closely related to your investigations. In particular we are studying the two new group theoretic papers of Zassenhaus which have appeared in the last issue of the Hamburger Abhandlungen*[36]...

And Hasse continued:

> Sehr gerne würde ich Sie auffordern, doch im Monat Juni einmal hierher zu kommen und bei uns in der Arbeitsgemeinschaft über Ihre gruppentheoretischen Studien vorzutragen, ganz zwanglos, d. h. so daß man dazwischenfragen darf, wenn man etwas nicht versteht, und das ganze mehr den Charakter einer gemeinsamen Erarbeitung hat.
>
> *I would like very much to invite you to visit us some time in June, and to inform us about your group theoretic work. This should be completely informal, so that it will be possible to put questions; the whole thing should have the character of a common discussion.*

On June 13, 1935 Grün arrived in Göttingen[37]; his talk in the workshop was scheduled for the next day, a Friday. Hasse had offered him to lodge in the Mathematical Institute where there was a visitor's room available, and to stay over the weekend in order

[35] To this Grün added: *"I have to acknowledge with thanks the support which I have found with the minister of education, for neither was I a member of the party nor have I become such."* Of course, the "party" which he alludes to, was the NSDAP, the Nazi party which had come to power in Germany in January 1933. Indeed it seems remarkable that Grün was supported in his work by the government of that time although he did not conform to the official party line. Later in 1946 he wrote that he had to suffer severe personal repression because he repeatedly had been urged to join the party but always refused.

[36] These were the papers [Zas35a] and [Zas35b], the first one on the characterization of linear groups as permutation groups, and the second on finite near-fields.

[37] Note that in the summer of 1934 Hasse had left Marburg and accepted a position at the University of Göttingen. Thus Hasse's invitation to Grün was meant for Göttingen, not Marburg. For

to have opportunity for discussions with the people of, in Hasse's words, "*the small but lively group of algebraists*" in Göttingen. We know from other sources the names of the members of that group, the most outstanding members besides Hasse being Witt, Teichmüller and also H. L. Schmid.[38] The latter was to play, ten years later, an important role in Grün's life.

In a former letter Grün had asked whether his talk in the workshop could be about $p$-groups, and Hasse had replied that the choice was entirely up to the speaker. And, knowing from his correspondence that Grün may have some problems to explain mathematical arguments in a correct form, Hasse had added the advice that Grün in his talk should be very explicit in all details.

Perhaps it is not without interest to cite Hasse's words where he tried to inform Grün about what had been discussed in the workshop so far, i.e., what he could assume to be known:

> Über $p$–Gruppen haben wir auch schon gesprochen. Wir haben die klassische Theorie (Speiser) durchgenommen, ferner noch einige weitere Sätze über die Anzahlen der Untergruppen oder Normalteiler gegebener Ordnung in einer $p$-Gruppe. Weiter die Theorie der Hamiltonschen Gruppen (alle Untergruppen Normalteiler) und der $p$–Gruppen, in denen es nur eine Untergruppe der Ordnung $p$ gibt (nur für $p = 2$ gibt es nicht zyklische solche Gruppen). Ich werde morgen über Satz 5 und Satz 9 Ihrer Arbeit vortragen.
>
> *We have already discussed p-groups. We worked through the classical theory (Speiser)*[39] *and in addition some theorems about the number of subgroups and normal subgroups of given order in a p-group. Furthermore the theory of Hamiltonian groups (all subgroups are normal), and the p-groups with only one subgroup of order p (only for p=2 there are non-cyclic groups with this property). Tomorrow I shall talk about theorems 5 and 9 of your paper.*

Theorems 5 and 9 were the second and the first theorem of Grün as discussed above.

The above lines show that in the circle around Hasse there was lively interest to learn more about the newest results of finite groups, in particular $p$-groups. This may have its explanation by the fact that during those years the theory of $p$-groups had been used heavily in algebraic number theory. We only mention the work of Arnold Scholz (who has had an extensive exchange of letters with Hasse) and who just recently had proved the existence of number fields with a given $p$-group of class two as Galois group [Sch35]. (And one year later Scholz would prove the same for an arbitrary finite $p$-group [Sch37].) This gives us perhaps another clue why Hasse was so much interested in Grün's results on $p$-groups.

Unfortunately we have not found any record about what Grün had actually talked about, nor how his talk was received by his young audience. Did Grün indeed talk about $p$-groups and what were his results which he presented? We can imagine that Grün, not being used to lectures and colloquium talks, had some difficulties to address

details of Hasse's change to Göttingen in the midst of the political upheavals of the time, we refer to [Fre85] and [Sch87].

[38] This was the same *Arbeitsgemeinschaft* in which one year later the Witt vectors were discovered, together with their application to cyclic extensions in characterististic $p$ and class field theory, as well as to the structure theory of p-adic fields. Those results are all published in one volume of Crelle's Journal (vol. 176), together with the seminal paper of Hasse who used Witt vectors for the explicit p-power reciprocity law of class field theory.

[39] Hasse means Speiser's monograph on group theory [Spe27].

such a group of brilliant young mathematicians who were used to high standards not only with respect to the mathematical topics under discussion but also as to the way of presenting new material. Doubtless Grün met high respect among these people, in view of his outstanding results so far. But did they appreciate his talk? From other sources (in later years) we infer that Grün's talks used to be somewhat clumsy and difficult to follow.

One week after Grün's talk, Zassenhaus visited the workshop in Göttingen, on June 21, 1935. Hasse had offered Grün to stay longer in order to meet Zassenhaus, and Grün did so. Note that Grün's paper [Grü35] had not yet appeared, and that Zassenhaus was just working on the text of his group theory book [Zas37]. It seems probable that Zassenhaus, when he met Grün in Göttingen, learned about Grün's theorems and realized their importance. In the foreword to his book (which appeared in 1937) Zassenhaus says that he wished to include the new and far-reaching results in group theory of the last 15 years; certainly Grün's theorems were among those and thus found their way into Zassenhaus' book.[40]

Two months after Grün's visit to Göttingen he wrote to Hasse (letter of August 13, 1935):

> Lassen Sie mich Ihnen nochmals danken für die Gastfreundschaft, die ich in Göttingen gefunden habe. Es war geradezu eine Wohltat für mich, einmal nur mit wissenschaftlichen Problemen beschäftigt zu sein. Wenn nicht meine wirtschaftliche Lage etwas anderes forderte, würde ich mich in Göttingen niederlassen und mich völlig meinen mathematischen Untersuchungen widmen.
>
> *Thank you again for the hospitality which I have found in Göttingen. It was really a great pleasure to me to be occupied exclusively by scientific problems. If my economic situation would have been different then I would settle in Göttingen and would occupy myself completely with mathematical research.*

This sounds as if Grün had hoped to be offered a position at the University of Göttingen which would enable him to exclusively follow his research work. But this was not the case.

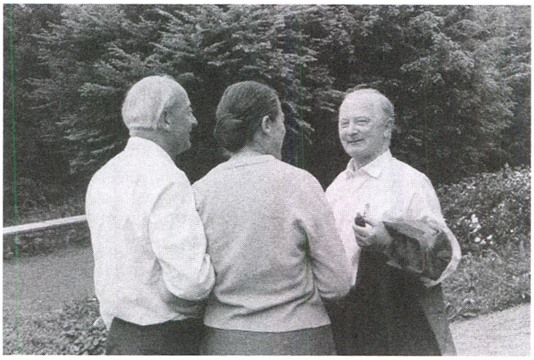
With the same letter Grün returned the proof sheets of his paper [Grü35]. Recall that the title of that paper carried the label "Part I" which implied that there would be more parts, at least a second part. Accordingly, Grün mentioned in his letter his plans for "Part II", and that this would include investigations on $p$-groups. From this we may perhaps conclude that indeed, his talk in Göttingen was about $p$-groups, and that he had been asked to send a manuscript about his talk to Crelle's Journal, to be published as Part II of his "investigations".

But this Part II did not materialize in the form as planned. Several months later, in a letter of February 7, 1936, Grün apologized to Hasse that the envisaged paper on $p$-groups is not yet finished. He announced the manuscript to be finished in about two

[40] Zassenhaus' book on group theory has been said to have been *"for decades the bible of the group theorists"* (Reinhold Baer). – Nowadays both Grün's theorems do appear in many textbooks on group theory, for instance in Huppert [Hup67]. Perhaps it is not without interest to note that Grün's theorems have been included and generalized in the setting of homological algebra. See, e.g., the book of Cartan-Eilenberg [CE56] chap.XII theorem 10.1.

Grün (lower right) at the group theory meeting Oberwolfach 1955

Grün with B. Huppert and H. Wielandt



Grün with R. Baer and Mrs. Baer

Fotos: W. Gaschütz.
Mit freundlicher Genehmigung des Mathematischen Forschungsinstituts Oberwolfach.

weeks, but finally it took several years for this. And the real Part II, which we have said appeared in 1945 only, did not deal particularly with $p$-groups [Grü45].

# 6 The Burnside problem (1939)

## 6.1 Dimension groups

After the appearance of Grün's paper [Grü35], his exchange of letters with Hasse slowed down in frequency and intensity. Grün had found his main interest to be group theory. He knew that Hasse's main interest was number theory, and so he may have felt that now he could pursue his work without having to rely every time on Hasse's advice.[41]

In the year 1936 there appeared the paper [Grü36] on the descending central series of free groups. This paper is never mentioned in the Hasse-Grün correspondence. Grün proves, with an unusual and somewhat peculiar argument using group representations, that the "dimension groups" as defined by Magnus [Mag35] do coincide with the members of the descending central series of the given free group. This was considered an important result.

Since Grün's paper directly refers to a paper by Magnus it is not unreasonable to assume that Grün had discussed it with Magnus before publication. Maybe it was Magnus himself who had posed the problem to Grün. We know from several sources that there was mathematical contact between Grün and Magnus in those years since 1935. But the correspondence Grün-Magnus seems to be lost and so we do not know the details of how strong Magnus' influence had been for this paper.

In any case, one year later Magnus himself provided a simplified proof, published in Crelle's Journal [Mag37]. But Grün's proof was duly registered as the first, and was appreciated by the specialists.

## 6.2 The group theory conference in Göttingen

In June 1939 Hasse had organized a 5-day group theory conference in Göttingen.

About the preparations for this conference we read in a letter which Hasse had sent jointly to Magnus and Zassenhaus, dated February 18, 1939:

> Die Göttinger Mathematische Gesellschaft plant in der letzten Woche des Sommersemesters 1939 eine größere Vortragsveranstaltung über das Thema Gruppentheorie. Wir haben dazu Herrn P. Hall von King's College, Cambridge eingeladen, uns drei größere Vorträge aus seinem Arbeitsgebiet zu halten. Zu meiner großen Freude hat Herr Hall sich dazu bereit erklärt . . .
>
> *The Mathematical Society of Göttingen is planning a conference on "Group Theory". We have invited Mr. Ph. Hall from King's college, Cambridge, for three lectures from his field of research. I am very glad that he has consented . . .*[42]

[41] In [JL98] it is said that, according to Grün himself, it was Hasse who had advised him to switch from number theory to group theory.

Hasse then explained that the lectures of Philip Hall should form the core of the conference, but in addition he wished that a number of German mathematicians who were working in group theory, should be given the opportunity to participate as invited speakers. And Hasse asked Magnus and Zassenhaus to help him with their expertise and advice to prepare this conference.

In the ensuing correspondence between Hasse, Magnus and Zassenhaus it was decided that not too many talks should be scheduled, which meant that only those German mathematicians should be invited as speakers whose field of research had some connection to Hall's, which is to say mainly $p$-groups and solvable groups and related topics. This then would include Grün, as Hasse observed:

> Wenn Grün gewonnen werden könnte, so wäre das natürlich sehr schön. Er hat doch bei allem Ungeschick seiner Darstellung die Gruppentheorie um einige wichtige Erkenntnisse bereichert, die in engstem Zusammenhang mit den Hallschen Arbeiten stehen. Ich bitte Herrn Magnus, sich mit ihm in Verbindung zu setzen.
>
> *If Grün could be won over then this would be very nice indeed. Notwithstanding his awkwardness in the presentation of material, he has enriched group theory with some important discoveries which are very closely connected with Hall's papers. I am asking Mr. Magnus to get in touch with him.*

When Hasse mentioned the "awkwardness in the presentation" then he may have recalled his experiences four years ago with Grün's paper which he (Hasse) had to rewrite completely. Maybe Grün's talk in the Göttingen *Arbeitsgemeinschaft* had also added to this impression. Nevertheless, in view of Grün's achievements Hasse did not hesitate to name him as invited speaker of the conference.

And when Hasse asked Magnus to get in touch with Grün, then this reflects the fact that, as said above, by now the mathematical contact of Grün with Magnus had become closer than his contact with Hasse.

The Göttingen group theory conference took place from June 26 to June 30, 1939. The program is published in 1940 in volume 182 of Crelle's Journal, together with the papers presented at the conference.[43] Hence it will not be necessary to go into all details here. The paper of Grün [Grü40] has the title:

> Zusammenhang zwischen Potenzbildung und Kommutatorbildung.
>
> *The connection between forming powers and commutators.*

The paper is motivated by and closely connected to the old

> Burnside problem: *Is every finitely generated group of finite exponent necessarily finite?*

See [Bur02]. For $m = 2$ the problem has a positive answer, already given by Burnside. This is so because every group of exponent 2 is commutative, as a consequence of the formula

$$t^{-1}s^{-1}ts = t^{-2}(ts^{-1}t^{-1})^2(ts)^2$$

[42] In the end, Hall delivered four lectures. – Hall was criticised for going to Germany at this difficult time but he defended his actions saying: "... *the German mathematicians* ... [are] *as little responsible for the present situation (and probably enjoy it as little) as you or I do.*" (Cited from "The MacTutor History of Mathematics archive".)

[43] Among them the paper by Wielandt which we have mentioned in section 4.4.

which expresses commutators as products of squares. This led Grün in his paper to study similar formulas connecting commutators and powers.

Burnside's problem has also a

Restricted version: *Are there only finitely many finite groups with a given number r of generators and a given exponent m?*

Grün's paper [Grü40] was the first in which this "restricted" Burnside problem was specifically addressed, but not under that name. The term "restricted Burnside problem" was coined later by Magnus [Mag50].

Let $F_r$ denote the free group with $r$ generators, and $F_r^m$ the subgroup generated by the $m$-th powers. The Burnside problem asks whether the factor group $F_r/F_r^m$ is finite. In his paper Grün considers the case when $m$ is a prime power $p^k$; this implies that the group of $F_r/F_r^m$ and its factor groups are $p$-groups.

Grün observes that the restricted Burnside problem has an affirmative answer for the pair $r, m$ if and only if the descending central series of $F_r/F_r^m$ terminates after finitely many steps. Note that the descending central series is defined by commutators, and so the above condition requires certain relations between powers and commutators. In his proof Grün used his results of his former paper [Grü36], as well as results of Magnus [Mag35], of Witt [Wit37] and Zassenhaus [Zas39].

Grün's paper was refereed in *Zentralblatt* by Zassenhaus, in *Fortschritte der Mathematik* by Speiser, and in the newly founded *Mathematical Reviews* by Baer. In the review by Zassenhaus we find the statement that Grün solved the restricted Burnside problem in the positive sense for $r = 2$, $m = 5$. Baer in his review says "the author may prove that ... " without saying that he really had proved it. The computations are quite involved and it seems that nobody had checked it. Later Kostrikin [Kos55] claimed that he had proved the restricted Burnside problem for $r = 2, m = 5$ but again, this seemed to be doubtful until Higman [Hig56] independently had settled the question positively, for aritrary $r$ and $m = 5$.[44]

Although Grün's paper carries the date of receipt as of August 21, 1939, Hasse would accept it only after it had been checked carefully by Magnus. With Magnus' help the paper underwent a thorough clean up. On January 21, 1940 Magnus wrote from Berlin[45] that he had worked the last two weekends with Grün, and that the latter had promised to complete his manuscript until the next weekend. The final version ready for printing arrived at Hasse's office on January 31, 1940.

[44] For arbitrary parameters $r$, $m$ the restricted Burnside problem has been finally solved in the positive sense by E. Zelmanov who had been awarded the Fields Medal in 1998.

[45] Magnus had accepted a job in industry in Berlin in August 1939. From the correspondence Hasse-Magnus we know that one year earlier, at the annual DMV-meeting in Baden-Baden, he had approached Hasse and asked whether Hasse could help him to find a new job since his position of *Privatdozent* at the University of Frankfurt had become unsustainable for political reasons. Hasse was able, with the help of Wilhelm Süss who had acquired some influence in the ministry of education, to find for Magnus a position of Privatdozent at the University of Königsberg. Magnus went there for the summer semester 1939 but then decided to accept a job in industry with the electronic company *Telefunken* in Berlin.

The attentive reader will have observed that between the dates involved, June 1939 (date of the Göttingen conference) and January 1940 (receipt of Grün's paper in final version) there was September 1, 1939, the outbreak of world war II. The publication of the conference papers in Crelle's Journal was somewhat delayed because one of the authors, Philip Hall, was a citizen of a country which now was in state of war with Germany. Hence it was necessary for Hasse to obtain the permission of the proper German governmental offices to publish Hall's papers in Crelle's Journal. When that permission was finally granted it turned out that only two of the four anticipated papers by Philip Hall had arrived. Since postal service between Germany and Great Britain had ceased there was no hope that the two missing articles would arrive by ordinary mail, and Hasse had to find other ways to obtain those articles. This was finally possible with the good services of Carleman at Djursholm who resided in Sweden, a neutral country.

## 6.3 A letter of 1952

Although Grün's power-commutator formulae in [Grü40] turned out to be useful in several respects, they did not lead Grün to the general solution of Burnside's problem, restricted or not, as he had hoped.

But Grün did not give up. Twelve years later, on June 30, 1952, after Hasse had sent him gratulations for his 64-th birthday he thanked Hasse for it and then wrote:

> . . . ich habe ein Ergebnis erhalten, das ich sehr hoch einschätze: Die absteigende Zentralreihe hat gesiegt! Die Vermutung von Burnside "Setzt man in einer aus endlich vielen Elementen erzeugten freien Gruppe $F$ alle $m$–ten Potenzen gleich 1, $m$ eine beliebige natürliche Zahl, so entsteht eine endliche Gruppe" ist irrig. Es gilt im Gegenteil: . . . $F_r/F_r^m$, kann nur dann endlich sein, wenn entweder $F_r$ zyklisch $(r = 1)$ oder $m = 2^i3^k$ ist. In allen anderen Fällen ist $F_r/F_r^m$ gewiß unendlich.
>
> *I have obtained a result which I estimate quite highly: The descending central series has won! The conjecture of Burnside, "If in a finitely generated free group F all m-th powers are put to 1 then there appears a finite group", is not true. On the contrary: . . .* $F_r/F_r^m$ *can be finite only if either* $F_r$ *is cyclic* $(r = 1)$ *or* $m = 2^i3^k$. *In all other cases* $F_r/F_r^m$ *is infinite.*

Hasse replied on July 15, 1952:

> Was Ihr neues Resultat betrifft, so ist das ja in der Tat ganz aufregend. Herr Witt, dem ich sofort davon Mitteilung machte, meinte, Sie hätten wohl das Resultat nicht ganz präzis mitgeteilt, denn bei zwei Erzeugenden sei doch im Falle $m = 5$ bekannt, daß die Gruppe endlich sei . . .
>
> *Concerning your new result, this is indeed very exciting. I have immediately informed Mr. Witt*[46]*, and he thinks that you had not stated the result in sufficiently precise form, for with two generators and* $m = 5$ *it is known that the group is finite.*[47]

And Hasse asked Grün to send him the precise formulation of the result.

[46] In 1952 Hasse and Witt were colleagues at the university of Hamburg.
[47] I am somewhat puzzled by Witt's statement. As far as I know the Burnside problem in the unrestricted sense is still open in the case $r = 2$ and $m = 5$. Did Witt have a proof which he never published? Or did Witt refer to the restricted Burnside problem? But the text of Grün's letter indicates that he is concerned with the unrestricted problem.

We do not know Grün's proof but since he did not reply to Hasse and did not publish this result there was probably an error in it. Maybe Grün had shown his proof to Magnus who pointed out the error. Note that Magnus had published two years earlier another paper connected with Burnside's problem [Mag50], hence he was still interested and informed about the problem.

At the DMV-meeting 1953 in Mainz Grün had announced a talk mentioning the Burnside problem and the Baker-Hausdorff formula in the title. In the same year Grün published a paper [Grü53] on $p$-groups in the Osaka Mathematical Journal in which some connections to the Burnside problem were given. The paper was rated as an "interesting paper" by Suzuki in his *Zentralblatt* review. But apparently nothing decisive concerning the Burnside problem came out of these activities.

So this is another case where Grün had attempted to solve a famous great problem but failed in the end, although he was able to contribute interesting methods, formulas and lemmas.

## 7 Later years (after 1945)

Grün had expressed in one of his first letters to Hasse that he did not particularly like his commercial job, and that he wished to be free to do mathematical research exclusively. In the year 1938 he finally had the opportunity to leave his unbeloved commercial job (whatever it was). As he reports in his vita[48]:

> Auf Bemühungen einflußreicher Mathematiker wurde ich 1938 Chefmathematiker am Geophysikalischen Institut in Potsdam.
>
> *Due to the help of influential mathematicians I was appointed chief mathematician at the Geophysics Institute in Potsdam.*[49]

But we are somewhat doubtful whether this new job did leave him much more time for group theory research as did his former job. (Although, as we have seen in section 5.2, he could participate in the Göttingen group theory conference in 1939.) In any case, during the war years until 1945, Grün was drafted to work as an "expert" at the Navy Headquarters in Berlin[50]; from this work there resulted a paper on theoretical physics (which was published later in 1948 [Grü48b]). Again it does not seem likely that in this period Grün had much time to spare for group theory.

After the war Grün found himself in the devastated city of Berlin without a job, hence free to tend exclusively to his mathematical research, but also without any income. In this situation he was picked up by Hermann Ludwig Schmid.

[48] We are referring to the same vita from which we have cited in section 2.1.

[49] I do not know the identity of the "influential mathematicians" mentioned by Grün. It seems unlikely that it was Hasse; the topic of Grün's job in Potsdam was never mentioned in their correspondence.

[50] *"Sachverständiger beim Oberkommando der Marine",* according to his own words in his vita. – We do not know whether it was the same military department where Hasse and a group of other mathematicians (including Magnus) were working during the war years.

## 7.1 H. L. Schmid and Grün

The mathematical scene in Berlin of the immediate post-war years has been vividly pictured by Jehne and Lamprecht [JL98].[51] H. L. Schmid was the main figure who took the necessary initiative and started to rebuild Mathematics at Berlin University and at the Berlin Academy from level zero. He was successful to attract mathematicians of high standing to Berlin, like Hasse and Erhard Schmidt (and others). He built and managed the new editorial office of the *Zentralblatt der Mathematik* in Berlin. Against many obstacles he founded a new mathematical journal, the *Mathematische Nachrichten*, and served as its managing editor. Using his diplomatic skills he succeeded to create a quiet atmosphere where mathematical life could prosper, protected from an evironment full of all kinds of basic day-to-day problems. He *"led mathematics in Berlin to a first revival"*.[52] For a time it looked like Berlin could become a leading center in Germany for Mathematical Sciences.

H. L. Schmid took Grün under his wing and was able to get him some financial support, first in the University of Berlin[53] and since 1947 in the newly founded Mathematics Research Institute of the Berlin Academy of Science.[54]

H. L. Schmid had been assistant to Hasse in 1935, and he had met Grün when the latter visited Göttingen (see section 5.2). Since 1940 H. L. Schmid worked in Berlin as an assistant to Geppert in the editorial office of the refereeing journals *Zentralblatt für Mathematik and Fortschritte der Mathematik*. At the same time he was *Privatdozent* at Berlin University. From then on H. L. Schmid lived in the same city as Grün and it is quite probable that they had met there occasionally. In any case, H. L. Schmid knew about the mathematical background and the achievements of Grün, and he knew what Grün needed: namely a quiet place to pursue his research on group theory. This was what he could offer now, with remarkable consequences for Grün's output of mathematical papers in the years to follow (see section 7.2).

Grün's salary at the Berlin Academy was not high, in fact it was quite small and just enough to live on. But since Grün was single, this was acceptable to him.[55]

[51] Klaus Krickeberg has pointed out to me that the article [JL98] describes only part of the "mathematical scene" in Berlin of those years. Another part was dominated by Erhard Schmidt in the direction of analysis.

[52] Cited from [JL98].

[53] In a letter to Hasse dated July 1, 1946 Grün wrote: "I *am relatively well off considering the circumstances. I am working at the university but as a researcher only, which after all is what I wish to do."*. – After the war in 1945, the "Friedrichs-Wilhelm Universität" of Berlin was short named "Universität Berlin", and later in 1949 it was renamed "Humboldt Universität zu Berlin". It was situated in the Eastern (Soviet) sector of Berlin and is to be distinguished from the "Free University" which had been founded in the Western sector.

[54] The documents of Grün's employment at the Berlin Academy are preserved and available in the Academy's archive.

[55] H. L. Schmid was able to support also a number of other young (and not so young) math-ematicians who needed help. One of them was Kurt Heegner, the man who later would be the first to solve the class number 1 problem for imaginary quadratic fields [Hee52]. (Heegner's paper was formulated in too fragmentary style and hence it was not understood properly until Deuring [Deu68] cleared up the situation.)

In October 1946 Grün had received an offer for a teaching position from the University of Greifswald, as he narrates in his vita written August 2, 1955. However, they required there that he publicly committed himself to a political party in the Sowjet occupation zone, and this he refused. Grün was a non-conformist: in the 1930s he had refused to join the Nazi party, and now he did the same thing with the communist dominated parties.[56]

Perhaps we are not wrong to assume that there was another reason for Grün, conscious or unconscious, to reject this offer to Greifswald. For, he did not like to teach. In fact, by all indications we know he was not a good lecturer. And so he preferred to live on the small but sufficient income he got from the Berlin Academy, free to pursue his studies on group theory without worrying about teaching and administrative or political problems.

Already in 1942 Hasse had written to Grün explaining what possibilities there were for him to obtain his doctorate. But at that time nothing came out of this. Now in 1946 H. L. Schmid proposed to Grün to apply to the university for admission to promotion for doctorate . It is reported (by hearsay) that Grün was quite hesitating because he did not like formalities of any kind. For, there had to be an extra permission because Grün had not been a student of Berlin University, in fact he had never attended any university. But H. L. Schmid finally succeeded to persuade Grün.[57]

Thus on April 2, 1946 Grün submitted the necessary application form to the dean of the science faculty of Berlin University. The fields in which he asked to be examined were "Pure Mathematics, Applied Mathematics and Theoretical Physics". He submitted the thesis *Contributions to group theory III* which two years later was published in the first volume of the new journal *Mathematische Nachrichten* (See [Grü48a]). Officially H. L. Schmid signed as the first referee for the thesis but he mentioned in his report that Magnus, as an expert in this field, had checked it thoroughly.

The promotion documents for Otto Grün are preserved at the archives of the Humboldt University. The examination took place on June 20, 1947 and the final doctor's diploma is signed on September 20, 1948. At this date Grün was 60 years of age.

## 7.2 16 more papers

In section 5.2 we have cited a letter of Grün (dated May 9, 1935) in which he claimed to have "*a huge pile of notes which already contain the essential ingredients of future publications.*" Some of those publications, until 1945, we have already mentioned. But it seems there was more in Grün's pile of notes. For, from 1948 to 1964 Grün published 16 more papers, 13 of them on $p$-groups and related topics. (The first of those papers he used as his doctoral thesis as mentioned above already.) About every year he completed a new

[56] Quite generally, people who knew him tell me that Grün's opinions and beliefs were remarkably independent of the *Zeitgeist*.

[57] It is not unlikely that H. L. Schmid used the argument that if Grün had the title of "doctor" then this would imply some increase of his (small) salary.

paper. This activity seems quite remarkable, considering that Grün in 1948 was of age 60, and he was 76 at the time when his last paper appeared.

The first few of these papers were still checked by Magnus before publication, but later, Magnus had emigrated to USA, Grün was at last able to work on his own. He had learned to avoid erroneous conclusions in his publications and had become a respected colleague among group theorists. He wisely stayed away from great and famous problems, in view of his experiences he had gone through in earlier years with Vandiver's conjecture, Burnside's problem and the conjecture of Schur.[58] His papers constituted valuable and useful contributions for the specialists; they appeared in good journals in Germany and elsewhere. Grün became a known expert in $p$-groups and related structures, and he was consulted as a referee for doctorate theses etc.

Two of Grün's papers from this time were on number theory: perfect numbers, and Bernoulli numbers. But these were only small notes.

In 1958 there was an increase in exchange of letters between Hasse and Grün, and this concerned class groups of cyclotomic fields. Thus Grün had not completely forgotten this topic with which he had started in the 1930s. As a result of this correspondence Grün obtained a theorem which, however, turned out to be a special case of Leopoldt's *Spiegelungssatz* [Leo58]. Leopoldt's paper was in press but not yet published. Hasse offered to publish Grün's manuscript since, after all, it had been obtained independently, but Grün withdrew his manuscript. Nonetheless his letters show that Grün's number theoretical interest was still alive, and his standard was high.

### 7.3 Würzburg (1954 – 63)

The hope that Berlin would be able to establish itself as a center of Mathematics in Germany dwindled soon. Around 1950 the "*Gleichschaltung*", in the communist sense, of academic (and other) institutions in the Soviet occupied part of Germany was intensified. As a consequence many people tried to go to West Germany. Hasse accepted a position in Hamburg in 1950, and a number of younger people of his circle went with him. In 1953 H. L. Schmid changed from Berlin to the University of Würzburg and again, a number of people went with him there.

Otto Grün too was among those who followed H. L. Schmid to Würzburg. The latter had been able to find means there for the financial support of Grün. At first Grün became a member of the research center for applied mathematics in Würzburg which H. L. Schmid had newly founded together with Bilharz.[59]

[58] In 1938 Grün had published a paper [Grü38] in which he claimed (among other results) that every representation of a finite group of exponent $m$ can be realized in the field of m-th roots of unity. Schur had conjectured this in 1912 with the group order instead of exponent. However, Grün's proof turned out to be erroneous.

[59] Herbert Bilharz had been, like H. L. Schmid, a graduate student of Hasse. In his Göttingen thesis [Bil37] he had solved Artin's conjecture for primitive roots in the function field case – assuming the Riemann hypothesis for function fields (which was finally verified by A. Weil). Later he went to applied mathematics and worked for a time in the aircraft industry. In Würzburg he held a chair for applied mathematics.

Later, after the early death of H. L. Schmid in 1956, Grün could be supported through a teaching job (*Lehrauftrag*) for group theory at the University of Würzburg, which he received almost regularly for several years. There are still people living who have attended Grün's lecture courses, or at least have tried to do so. The story is that each semester Grün announced a lecture on group theory, and after 2-3 hours every student had dropped out because of Grün's "awkwardness in the presentation of material" (which Hasse had already observed in 1939). After that, Grün was happy to be able to turn to his research without having to worry about lectures.

Between 1954 and 1961 Grün attended every group theory meeting in Oberwolfach; these meetings were directed by Reinhold Baer, one of them by Jean Dieudonné. Since participation in Oberwolfach meetings is possible by personal invitation only, this shows that his results were appreciated by the international group theory community. Four times Grün presented talks at those meetings (1955, 59, 60, 61). The abstracts of those talks are still available in the Oberwolfach abstract books (*Vortragsbücher*), they show that Grün talked about the results which he had obtained in his papers. But as some participants of those meetings remember, his style of lecturing had not improved.

## 8 Epilogue

In 1955 Grün was 67 years. It became clear that something had to be done to secure for him some retirement pension.[60] This was difficult since he never had held a regular position in a university. In the archives of Würzburg University I have found a number of documents, between 1955 and 1962, written by the Mathematics Department Head, with the intention to obtain some kind of retirement pay for Grün.

In order to back those efforts, some leading group theorists were asked to write their opinion on Grün. Let us cite excerpts of those opinions, all dated in 1955, in order to put into evidence that Grün was respected as a group theorist throughout the world:

F. W. LEVI, Berlin (Freie Universität): Es ist Herrn Grün gelungen, neue Methoden für die Erforschung der endlichen Gruppen zu entwickeln und dadurch dieses Gebiet neu zu erschließen. Schon seine ersten Ergebnisse haben Aufsehen unter den Algebraikern erregt und sind schnell in die Literatur, sogar in Lehrbücher übergegangen. Seit dieser Zeit hat er unermüdlich weiter gearbeitet, wichtige Ergebnisse erzielt und dadurch anderen Mitarbeitern den Weg zu neuer Forschung geebnet. ... Herr Grün ist Autodidakt, hat nie ein Lehramt bekleidet, aber er ist ein echter Gelehrter, und zwar ein Gelehrter von großer wissenschaftlicher Bedeutung.

*Grün succeeded to develop new methods for the investigation of finite groups and thus to open this field from a new viewpoint. Already his first results have attracted great attention among algebraists and were quickly included into the literature, even into textbooks. Since then he has ever continued to work, he has obtained important results and thus opened the way for the research of other mathematicians. ... Grün is self-educated, has never had a teaching position, but he is a true scholar with great scientific standing ...*

R. BAER, University of Illinois, Urbana: O. Grün ist unzweifelhaft einer der führenden Gruppentheoretiker unserer Zeit. ... In der fundamentalen Arbeit über die endlichen $p$-Gruppen ist es ihm gelungen, die Ph. Hallsche Theorie der regulären $p$-Gruppen auf beliebige $p$-Gruppen

[60] In a letter of Grün to Hasse of August 29, 1955, Grün writes that he gets only 160 DM monthly.

auszudehnen, den dabei entstehenden neuen Phänomenen Rechnung zu tragen und dadurch neues Licht auf die Fülle der Erscheinungen in diesem reichen Gebiet zu werfen.

*Without doubt Grün is one of the leading group theorists of our time. ... In the fundamental paper on finite p-groups he succeeded to extend Ph. Hall's theory of regular p-groups to p-groups of arbitrary structure. He was able to deal with the new phenomena which showed up in this process, and thus to throw new light upon the many aspects of this rich mathematical discipline.*

B. H. NEUMANN, Hull: Otto Grün muss heutzutage als einer der bekanntesten und berühmtesten Gruppentheoretiker gelten, und zwar keineswegs nur in Deutschland, sondern überall, wo Mathematik getrieben wird ... In drei so verschiedenartigen Monographien wie "Lehrbuch der Gruppentheorie" von Zassenhaus, "Gruppi astratti" von Scorza und "Teoriya Grupp" von Kurosch werden die Resultate von Grün mehrfach herangezogen.

*Nowadays Otto Grün has to be counted as one of the most prominent group theorists, by no means in Germany only but wherever mathematics is present ... In three quite different monographys like "Lehrbuch der Gruppentheorie" by Zassenhaus, "Gruppi astratti" by Scorza and "Teoriya Grupp" by Kurosh his results are repeatedly used.*

J. DIEUDONNÉ, Evanston, Ill.: ... confirmer tout l'estime et l'admiration que j'ai pour les travaux de M. le Prof. O. Grün. Ses idées sur la théorie des groupes se distinguent par une remarquable originalité et une profondeur peu commune ...

*... the estimation and admiration which I harbor for the works of Prof. O. Grün. His ideas about group theory are distinguished by a remarkable originality and a rarely found depth ...*

W. MAGNUS, New York University: Grün ist ein Mathematiker von wohlbegründetem internationalen Ansehen. Seine Arbeiten zur Gruppentheorie werden von mathematischen Autoren aller Länder zitiert, und einige der von Herrn Grün gefundenen Resultate gehören zum bleibenden Bestand der Gruppentheorie, was darin zum Ausdruck kommt, dass sie in allen modernen Lehrbüchern dargestellt werden (z. B. Zassenhaus, Kurosch) ...

*Grün is a mathematician of well founded international standing. His papers are cited by mathematical authors of all countries, and some of his results belong to the perpetual stock of group theory, which is evidenced by the fact, that they are treated in all modern textbooks (e.g., Zassenhaus, Kurosh) ...*

H. ZASSENHAUS, McGill Univ., Montreal: Im Bereiche der mathematischen Forschung dieses Jahrunderts ist mir kein anderes Beispiel der Entdeckung eines hervorragenden Mathematikers im vorgerückten Alter bekannt geworden. Im neunzehnten Jahrhundert hat es die Fälle von Sophus Lie und Weierstrass gegeben ... Durch seine Arbeiten hat sich Otto Grün einen Namen als ausgezeichneter tiefforschender deutscher Mathematiker gemacht, den ich in England und in den Vereinigten Staaten immer wieder mit Achtung und Bewunderung habe nennen hören.

*In the realm of mathematical research I do not know any other example of an excellent mathematician who was discovered in his midlife years only. In the 19th century there were the cases of Sophus Lie and Weierstrass ... Through his work Otto Grün has become a well known name as a German mathematician, doing deep research. I have heard mention his name again and again in England and in the United States with respect and admiration ...*

It is not clear from the Würzburg documents whether the initiative on behalf of Grün was successful. I am afraid it was not.

In any case, Grün returned to (West-)Berlin, his home town, in the year 1963 when he was 75. After that date there were still some letters exchanged between Grün and Hasse but they were restricted mainly to birthday greetings and the like. All the time Grün continued to respect Hasse as his teacher, the one who opened mathematics for him, and he expressed his thanks and admiration for Hasse in his letters.

Starting from 1971 we find in Grün's letterhead the title of "Professor". Perhaps we can conclude from this that he had obtained from the government this official title and, we hope, finally some adequate retirement pension in view of his achievements.

In October 1974 Grün died at the age of 86. Among Hasse's papers I found a brief obituary, about half a page, dated October 10, 1974. But I do not know where it had been published; perhaps it was a newspaper clip. There was no obituary in the *Jahresbericht of the DMV of which Grün was a member since 1939.*

## References

[ACH65] N. C. Ankeny, S. Chowla, and H. Hasse. On the class-number of the maximal real subfield of a cyclotomic field. *J. Reine Angew. Math.*, 217:217–220, 1965.

[Art29] E. Artin. Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz. *Abh. Math. Semin. Univ. Hamb.*, 7:46–51, 1929.

[BHN32] R. Brauer, H. Hasse, and E. Noether. Beweis eines Hauptsatzes in der Theorie der Algebren. *J. Reine Angew. Math.*, 167:399–404, 1932.

[Bil37] H. Bilharz. Primdivisoren mit vorgegebener Primitivwurzel. *Math. Ann.*, 114:476–492, 1937.

[Bra34] H. R. Brahana. Prime power abelian groups generated by a set of conjugates under a special automorphism. *Amer. Journ. Math.*, 55:553–584, 1934.

[Bur02] W. Burnside. On an unsettled question in the theory of discontinuous groups. *Quart. Journ. Math.*, 33:230–238, 1902.

[Bur11] W. Burnside. *Theory of groups of finite order.* Cambridge Univ. Press, 2 edition, 1911. XXIV + 512 p.

[CE56] H. Cartan and S. Eilenberg. *Homological Algebra.* Princeton Univ. Press, 2 edition, 1956. XII + 390 p.

[Che31] C. Chevalley. Relation entre le nombre de classes d'un sous corps et celui d'un surcorps. *C. R. Acad. Sci., Paris*, 192:257–258, 1931.

[Deu68] M. Deuring. Imaginäre quadratische Zahlkörper mit der Klassenzahl 1. *Invent. Math.*, 5:169–179, 1968.

[Fre85] G. Frei. Helmut Hasse (1898-1979). *Exp. Math.*, 3:55–69, 1985.

[Fur08] Ph. Furtwängler. Über die Klassenzahlen Abelscher Zahlkörper. *J. Reine Angew. Math.*, 134:91–94, 1908.

[Fur29] Ph. Furtwängler. Beweis des Hauptidealsatzes für die Klassenkörper algebraischer Zahlkörper. *Abh. Math. Semin. Univ. Hamb.*, 7:14–36, 1929.

[Grü34a] O. Grün. Über Substitutionsgruppen im Galoisfeld. *J. Reine Angew. Math.*, 170:170–172, 1934.

[Grü34b] O. Grün. Zur Fermatschen Vermutung. *J. Reine Angew. Math.*, 170:231–234, 1934.

[Grü35] O. Grün. Beiträge zur Gruppentheorie I. *J. Reine Angew. Math.*, 174:1–14, 1935.

[Grü36] O. Grün. Über eine Faktorgruppe freier Gruppen. *Deutsche Math.*, 1:772–782, 1936.

[Grü38] O. Grün. Gruppentheoretische Untersuchungen. *Deutsche Math.*, 3:547–555, 1938.

[Grü40] O. Grün. Zusammenhang zwischen Potenzbildung und Kommutatorbildung. *J. Reine Angew. Math.*, 182:158–177, 1940.

[Grü45] O. Grün. Beiträge zur Gruppentheorie II. *J. Reine Angew. Math.*, 188:165–169, 1945.

[Grü48a] O. Grün. Beiträge zur Gruppentheorie III. *Math. Nachr.*, 1:1–24, 1948.

[Grü48b] O. Grün. Berechnung des elektrischen Feldes bei einer gewissen Materialverteilung. *Math. Nachr.*, 4:419–433, 1948.

[Grü53] O. Grün. Beiträge zur Gruppentheorie V. Über endliche p-Gruppen. *Osaka Math. J.*, 5:117–146, 1953.

[Has26a] H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. I: Klassenkörpertheorie. *Jahresbericht D. M. V.*, 35:1–55, 1926.

[Has26b] H. Hasse. Neue Begründung der komplexen Multiplikation I: Einordnung in die allgemeine Klassenkörpertheorie. *J. Reine Angew. Math.*, 157:115–139, 1926.

[Has30a] H. Hasse. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. II: Reziprozitätsgesetz.* B. G. Teubner, 1930. IV + 204 S.

[Has30b] H. Hasse. Die Normenresttheorie relativ-Abelscher Zahlkörper als Klassenkörpertheorie im Kleinen. *J. Reine Angew. Math.*, 162:145–154, 1930.

[Has31] H. Hasse. Neue Begründung der komplexen Multiplikation. II. Aufbau ohne Benutzung der allgemeinen Klassenkörpertheorie. *J. Reine Angew. Math.*, 165:64–88, 1931.

[Has32] H. Hasse. Theory of cyclic algebras over an algebraic number field. *Trans. Am. Math. Soc.*, 34:171–214, 1932.

[Has33a] H. Hasse. Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper. Insbesondere Begründung der Theorie des Normenrestsymbols und Herleitung des Reziprozitätsgesetzes mit nichtkommutativen Hilfsmitteln. *Math. Ann.*, 107:731–760, 1933.

[Has33b] H. Hasse. Vorlesungen über Klassenkörpertheorie. Preprint, Marburg. [Later published in book form by Physica Verlag Würzburg (1967)], 1933.

[Has52] H. Hasse. *Über die Klassenzahl abelscher Zahlkörper.* Akademie-Verlag, Berlin, 1952. Reprint 1985 with an introduction of J. Martinet.

[Hee52] K. Heegner. Diophantische Analysis und Modulfunktionen. *Math. Zeitschr.*, 56:227–253, 1952.

[Her32] J. Herbrand. Sur les classes des corps circulaires. *Journ. de Math. (9)*, 11:417–441, 1932.

[Hig56] G. Higman. On finite groups with exponent five. *Proc. Cambridge Philos. Soc.*, 52:381–390, 1956.

[Hil97] D. Hilbert. Die Theorie der algebraischen Zahlkörper. *Jahresber. Dtsch. Math. Ver.*, 4:I–XVIII u. 175–546, 1897.

[Hup67] B. Huppert. *Endliche Gruppen.* Springer, Berlin, 1967. XII, 793 p.

[Iya34] S. Iyanaga. Zum Beweise des Hauptidealsatzes. *Abh. Math. Semin. Univ. Hamb.*, 10:349–357, 1934.

[JL98] W. Jehne and E. Lamprecht. Helmut Hasse, Hermann Ludwig Schmid and their students in Berlin. In H. B. W. Begehr et al., editor, *Mathematics in Berlin.*, pages 143–149, Berlin, 1998. Berliner Mathematische Gesellschaft., Birkhäuser.

[Kos55] A. Kostrikin. Solution of a weakened problem of Burnside for exponent 5. (Russian. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 19:233–244, 1955.

[Kum50] E. Kummer. Allgemeiner Beweis des Satzes, dass die gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Primzahl-exponenten $\lambda$, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoullischen Zahlen nicht vorkommen. *J. Reine Angew. Math.*, 40:130–138, 1850.

[Leh74] D. H. Lehmer. Harry Schultz Vandiver, 1882–1973. *Bull. American Math. Soc.*, 80:817–818, 1974.

[Lem97] F. Lemmermeyer. On 2-class field towers of some imaginary quadratic number fields. *Abh. Math. Sem. Hamburg*, 67:205–214, 1997.

[Leo58] H.-W. Leopoldt. Zur Struktur der $\ell$-Klassengruppe galoisscher Zahlkörper. *J. Reine Angew. Math.*, 199:165–174, 1958.

[Mag30] W. Magnus. Über diskontinuierliche Gruppen mit einer definierenden Relation. (Der Freiheitssatz.). *J. Reine Angew. Math.*, 163:141–165, 1930.

[Mag34] W. Magnus. Über den Beweis des Hauptidealsatzes. *J. Reine Angew. Math.*, 170:235–240, 1934.

[Mag35] W. Magnus. Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring. *Math. Annalen*, 111:259–280, 1935.

[Mag37] W. Magnus. Über Beziehungen zwischen höheren Kommutatoren. *J. Reine Angew. Math.*, 177:105–115, 1937.

[Mag50] W. Magnus. A connection between the Baker-Hausdorff formula and the problem of Burnside. *Ann. Math. II.*, 52:111–126, 1950.

[Rib79] P. Ribenboim. *13 Lectures on Fermat's Last Theorem.* Springer, New York, Heidelberg, Berlin, 1979. xvi, 302 p.

[Roh98] H. Rohrbach. Helmut Hasse and Crelle's Journal. *J. Reine Angew. Math.*, 500:5–13, 1998.

[Roq04] P. Roquette. The Riemann hypothesis in characteristic $p$, its origin and development. Part 2. the first steps by Davenport and Hasse. *Mitt. Math. Ges. Hamburg*, 22:1–69, 2004.

[Sch02] I. Schur. Neuer Beweis eines Satzes über endliche Gruppen. *Sitz. Ber. Preuss. Akad. Wiss. Berlin*, 1902:1013–1019, 1902.

[Sch35] A. Scholz. Die Kreisklassenkörper von Primzahlpotenzgrad und die Konstruktion von Körpern mit vorgegebener zweistufiger Gruppe ii. *Math. Ann.*, 110:633–649, 1935.

[Sch37] A. Scholz. Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung. i. *Math. Zeitschr.*, 42:161–188, 1937.

[Sch87] N. Schappacher. Das mathematische Institut der Universität Göttingen 1929–1950. In Heinrich Becker and andere, editors, *Die Universität Göttingen unter dem Nationalsozialismus.*, pages 345–373. K. G. Saur, 1987.

[Spe27] A. Speiser. *Die Theorie der Gruppen von endlicher Ordnung. Mit Anwendungen auf algebraische Zahlen und Gleichungen sowie auf die Kristallographie.* Die Grundlehren der mathematischen Wissenschaften mit besonderer Berücksichtigung ihrer Anwendungsgebiete Bd. 5. J. Springer, Berlin, second edition, 1927. IX + 251 S. mit 38 Abb.

[Tho59] J. Thompson. Normal p-complements for finite groups. *Math. Zeitschr.*, 1959.

[Van29] H. S. Vandiver. On Fermat's Last Theorem. *Transactions Amer. Math. Soc.*, 31:613–642, 1929.

[Van41] H. S. Vandiver. On improperly irregular cyclotomic fields. *Proc. Nat. Acad. Sci. U.S.A.*, 27:77–83, 1941.

[vdW31] B. L. van der Waerden. *Moderne Algebra. Unter Benutzung von Vorlesungen von E. Artin und E. Noether. Bd. II.* Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete Bd. 24. Springer, Berlin, 1931. VII + 216 S.

[Wie40] H. Wielandt. p-Sylowgruppen und p-Faktorgruppen. *J. Reine Angew. Math.*, 182:180–193, 1940.

[Wit37] E. Witt. Treue Darsellung Liescher Ringe. *J. Reine Angew. Math.*, 177:105–115, 1937.

[Yam97] K. Yamamura. Maximal unramified extensions of imaginary quadratic number fields of small conductors. *J. Théorie des Nombres de Bordeaux*, 9:405–448, 1997.

[Zas35a] H. Zassenhaus. Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen. *Abh. Math. Semin. Univ. Hamb.*, 11:187–220, 1935.

[Zas35b] H. Zassenhaus. Über endliche Fastkörper. *Abh. Math. Semin. Univ. Hamb.*, 11:187–220, 1935.

[Zas37] H. Zassenhaus. *Lehrbuch der Gruppentheorie. Bd. 1.*, volume 21 of *Hamburg. Math. Einzelschriften*. B. G. Teubner, Leipzig, Berlin, 1937. VI, 152 S.

[Zas39] H. Zassenhaus. Über Liesche Ringe mit Primzahlcharakteristik. *Abh. Math. Semin. Univ. Hamb.*, 13:1–100, 1939.

# Computational Group Theory

**Bettina Eick**

## Abstract


- Mathematics Subject Classification: 20-02, 20-04, 68 W 30
- Keywords and Phrases: Group Theory, Algorithms, Computation


This article is an introduction and a survey on the methods and aims of computational group theory. It reports on the current state of the art, some of its highlights, and some of its applications in topics like Galois theory, cryptography and crystallography.

Eingegangen: 18. 4. 2005 (überarbeitet 4. 6. 2005)

Bettina Eick, Institut Computational Mathematics, TU Braunschweig, 38106 Braunschweig

DMV
JAHRESBERICHT DER DMV

## 1 Introduction

Groups play a central role in algebra and mathematics. They formalize the concept of symmetry and have applications ranging from the insolubility of the quintic equation to crystallography and cryptography.

Computational group theory is a modern branch of group theory. It includes the development of algorithms for the computational investigation, construction and classification of groups, their implementation and their complexity analysis. An important aim in computational group theory is the application of algorithms to solve open problems with the help of computers.

There are two major computer algebra systems available which can serve as a basis for implementations and as a source of available algorithms: the GAP system [62] and the MAGMA system [9]. Both systems contain a broad variety of group theoretic algorithms and various data libraries. Both systems are widely used by the mathematical research community and they are distributed to over 600 campuses world wide.

Computational group theory is divided into various subareas. Some of them correspond to the main representations of groups: permutation groups, finitely presented groups and matrix groups. Also, there are specialized algorithms available for certain classes of groups such as nilpotent or polycyclic groups. Further, algorithms to classify certain types of groups play a role in computational group theory.

This article can only give an overview on some of the many topics in computational group theory. For further details and background see the handbook of computational group theory by Holt et. al. [30] as well as to the conference proceedings [4, 11, 12, 23, 24, 36, 5] and the survey articles [55, 42]. Sections 2–6 of this article describe some of the main subareas of computational group theory and Sections 7–9 contain some applications.

## 2 Permutation Groups

Suppose that a subgroup $G$ of a symmetric group $S_n$ is given by a set of generators $\{g_1, \ldots, g_l\}$. The central problem in computational permutation group theory is to determine the structure of $G$. This includes, for example, the computation of the order of $G$, the investigation of all or of specific parts of the subgroup structure of $G$, or the computation of the automorphism group of $G$.

The algorithmic theory of permutation groups is well-developed and a large variety of methods is available. Many of the recently developed permutation group algorithms are at the same time the most practical algorithms for implementations and also have the best known complexity. The book by Seress [56] gives a state of the art description of permutation group methods.

A particular strength of permutation groups is that groups of quite large order can be defined by a small generating set. Hence only a small amount of data is needed to store a large object. It is a central aim to be able to investigate very large groups and thus listing the elements of a group or similarly large amounts of data should be avoided.

## 2.1 Base and strong generating set

The fundamental ideas for computations with permutation groups are due to Sims [58]. They are based on the following definition.

**1 Definition:** Let $G \leq S_n$ and $B = (\beta_1, \ldots, \beta_m)$ a sequence of points in $\{1, \ldots, n\}$. Let $G_i = Stab_G(\beta_1, \ldots, \beta_{i-1})$ the pointwise stabilizer of $\beta_1, \ldots, \beta_{i-1}$ for $1 \leq i \leq m$.

a) $B$ is called a *base* for $G$ if $G_{m+1} = \{1\}$ holds.
b) $S \subseteq G$ is called a *strong generating set* for $G$ with respect to $B$ if $G_i = \langle S \cap G_i \rangle$ holds for $1 \leq i \leq m$.

If a base and a strong generating set for $G$ are given, then the orbits $\beta_i^{G_i}$ can be computed readily. It follows that the order $|G|$ can be read off as

$$|G| = \prod_{i=1}^{m} [G_i : G_{i+1}] = \prod_{i=1}^{m} |\beta_i^{G_i}|.$$

The determination of the orbits $\beta_i^{G_i}$ also yields a transversal $T_i$ of $G_{i+1}$ in $G_i$. Thus every element $g$ of $G$ can be written uniquely as $g = t_m \cdots t_1$ with $t_i \in T_i$. This decomposition can be determined algorithmically: first, determine $t_1 \in T_1$ with $\beta_1^g = \beta_1^{t_1}$. Then $h = gt_1^{-1} \in G_2$. Now apply the method recursively to $h$ and obtain $h = t_m \cdots t_2$. It follows that $g = ht_1 = t_m \cdots t_2 \cdot t_1$ as desired. This process is called *sifting*.

The sifting algorithm can also be used for membership testing: given $g \in S_n$, we try to sift $g$ as outlined above. If at any step in this method $\beta_i^h \notin \beta_i^{G_i}$, then $g \notin G$ follows. If at the end of the sifting process $h \neq 1$, then $g \notin G$ follows also. Otherwise $g \in G$ holds.

A base and strong generating set can be computed effectively in a permutation group given by generators. This is the most fundamental among all methods for permutation groups; see [56] for a detailed account.

Further applications of bases and strong generating sets include, for example, the computation of the derived and the lower central series and finding the pointwise stabilizer of subsets of $\{1, \ldots, n\}$.

## 2.2 Further algorithms for permutation groups

Many other effective algorithms for permutation groups are based on the determination and use of a system of imprimitivity for the considered group. These methods use a divide and conquer approach to reduce the considered problem to computations with primitive permutation groups. These algorithms include those for the determination of a composition series and the computation of Sylow subgroups.

However, there are also algorithmic problems for permutation groups where no efficient algorithm for their solution is known. These problems include, for example, the computation of the centralizer of an element and the intersection of two subgroups. Backtrack methods are used to solve these problems.

## 2.3 Examples and applications

Methods for permutation groups have initially been invented and designed for the explicit construction and investigation of finite simple groups. For example, Leon and Sims [38] used them to construct the Baby monster $B$ and thus obtained a first (computer dependent) proof for the existence of this sporadic simple group. The Baby monster $B$ is a group of order

$$2^{41} \cdot 3^{13} \cdot 5^{6} \cdot 7^{2} \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$$

and it was constructed as a permutation group on 13 571 955 000 points.

There are also applications of permutation groups outside group theory. An example is the investigation of games. For example, one can readily determine that the symmetry group of Rubik's cube has order $2^{27} \cdot 3^{14} \cdot 5^{3} \cdot 7^{2} \cdot 11$. This computation only takes a few milliseconds on an average computer nowadays, see for example [53]. Note that the order translates to the number of different states that Rubik's cube has.

It is also possible to investigate whether certain permutations of the cube's faces are possible. For example, one can readily prove that it is impossible to flip just one edge of the cube, while one can flip two edges simultaneously. The original idea of the cube was to find a sequence of turns of the faces that will transform the cube back into its original state. It is worth noting that the currently available permutation group methods are not able to solve all instances of this problem in a reasonable amount of time.

# 3 Finitely Presented Groups

A finite presentation for a group $G$ consists of a set of abstract generators $\mathcal{G} = \{g_1, \ldots, g_l\}$ and a set of relators $\mathcal{R} = \{r_1, \ldots, r_m\}$; every relator $r_i$ is a word in the generators and their inverses. The group $G$ is then defined as $F/K$ where $F$ is the free group on $\mathcal{G}$ and $K$ is the normal subgroup of $F$ generated by $\mathcal{R}$. One can think of $G$ as the largest group which has a set of generators satisfying the relations $r = 1$ for $r \in \mathcal{R}$.

Again, the central problem in this area is: given a group $G$ defined by a finite presentation, determine the structure of $G$. However, one should be far less ambitious in the finitely presented group case than, for example, in the permutation group case.

In 1911 Dehn [13] asked the question whether the following problems can be solved in a finitely presented group:

- *Word problem:* Given a word $w$ in $\mathcal{G}$, decide whether $w = 1$ holds in $G$.
- *Conjugacy problem:* Given two words $w$ and $v$ in $\mathcal{G}$, decide whether $w^g = v$ holds in $G$ for some $g \in G$.
- *Isomorphism problem:* Given two finitely presented groups, decide whether they are isomorphic.

It was proved 1955 by Novikov [47] that the word problem is not decidable in a finitely presented group. Consequently, the other two problems and many other related algorithmic problems are also undecidable in finitely presented groups. Thus computations with finitely presented groups are generally difficult.

Nonetheless, there are various algorithmic approaches available for such groups. The book by Sims [60] provides a detailed account on these methods. In the following we give a basic introduction to some of the fundamental ideas of these methods.

## 3.1 Quotient methods

Suppose that $G = \langle \mathcal{G} \mid \mathcal{R} \rangle$ is given. The aim of the quotient methods is to analyze certain quotients of $G$. The simplest instance of these methods is the abelian quotient method. Its aim is to determine the isomorphism type of the largest abelian quotient $G/G'$. We include a brief outline of this method in the following. Recall that every relator $r \in \mathcal{R}$ is a word in the generators and their inverses: $r = g_{i_1}^{e_1} \cdots g_{i_s}^{e_s}$ for certain $e_j \in \mathbb{Z}$. First, determine for $r$ its corresponding collected word $\overline{r} = g_1^{a_1(r)} \cdots g_l^{a_l(r)}$ where $a_k(r)$ is the sum of all $e_j$ with $i_j = k$. Then, define the following matrix

$$A = \begin{pmatrix} a_1(r_1) & \cdots & a_l(r_1) \\ \vdots & & \vdots \\ a_1(r_m) & \cdots & a_l(r_m) \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \in \mathbb{Z}^{l \times \max\{l,m\}}.$$

A Smith normal form computation on $A$ can now be used to exhibit the isomorphism type of $G/G'$ as the following theorem shows; see [60], Chapter 8, for a proof.

**2 Theorem:** *Let $b_1, \ldots, b_l$ be the diagonal entries of the Smith normal form for $A$. Then $G/G' \cong \mathbb{Z}/b_1\mathbb{Z} \times \cdots \times \mathbb{Z}/b_l\mathbb{Z}$.*

Hence the isomorphism type of $G/G'$ can be determined by linear algebra methods. More sophisticated methods can be used to determine other types of quotients of $G$. For example, in [45] the computation of nilpotent quotients is described and in [40] Groebner basis methods over group rings are employed to determine polycyclic quotients. Various finite quotient methods can be found in [50, 46, 43].

## 3.2 The order of a finitely presented group

Suppose that $G = \langle \mathcal{G} \mid \mathcal{R} \rangle$ is given. An approach for computing the order of $G$, provided it is finite, has been invented 1936 by Todd and Coxeter [64]. The basic idea is to determine successively a faithful permutation representation for $G$ using the action of $G$ by multiplication on its elements or on cosets of a subgroup. If $G$ is finite, then this process terminates and yields $|G|$. If $G$ is infinite, then this process does not terminate. Most recent investigations and implementations of this method are due to Havas [27].

An alternative to the Todd-Coxeter approach is the Knuth-Bendix term-rewriting process; see [59]. This process tries to determine a confluent rewriting system for the group $G$ and thus the order of $G$. The process terminates if $G$ is finite, but if $G$ is infinite, then the process may or may not terminate. Usually, the Todd-Coxeter approach is more effective than the Knuth-Bendix process.

### 3.3 Some further algorithms for finitely presented groups

The low-index subgroup algorithm lists all subgroups of a given index in a finitely presented group. This method is based on similar ideas as the Todd-Coxeter approach, see [60]. Approaches towards testing isomorphism or non-isomorphism have been described by Holt and Rees [32].

There are various special classes of finitely presented groups which allow significantly better algorithms to compute with them. For example, free groups [8], automatic groups [22, 21] and polycyclicly presented groups, see Section 4, are of this type.

### 3.4 Examples and applications

A major motivation for computations with finitely presented groups comes from topology; in particular, from the study of fundamental groups. An explicit example of a collection of groups arising from topology has been given by Cavicchioli and investigated by Hulpke [33]: The computation shows also that even though there is no algorithm to decide whether or not a finitely presented group is infinite, an interplay between various methods for finitely presented groups can often be used to determine that a given finitely presented group is infinite.

An impressive application of the finite quotient methods lies in the determination of restricted Burnside groups. The Burnside group $B(l, e)$ is the largest group on $l$ generators with exponent $e$. Zelmanov's famous theorem [65] asserts that $B(l, e)$ has a maximal finite quotient: the restricted Burnside group $R(l, e)$.

For exponents 2 and 3, it is known that $B(l, e) = R(l, e)$ and the groups can be constructed by theoretical investigations. For $e > 3$, the explicit construction of $R(l, e)$ for specific values of $l$ and $e$ is an interesting computational problem. The solvable quotient and $p$-quotient methods are the main tools that have been employed for this purpose. We refer to [43] for an overview and to [48] for the latest achievements. A table with the orders of the known restricted Burnside groups for $e > 3$ is included below.

| $l$ | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| $\|R(l,4)\|$ | $2^{12}$ | $2^{69}$ | $2^{422}$ | $2^{2728}$ |
| $\|R(l,5)\|$ | $5^{34}$ | $5^{2282}$ | | |
| $\|R(l,6)\|$ | $2^{28} \cdot 3^{25}$ | | | |
| $\|R(l,7)\|$ | $7^{20416}$ | | | |

# 4 Polycyclic Groups

For polycyclic groups there exists a special collection of effective algorithms which are based on the internal structure of the groups, and not on any specific representation.

**3 Definition:** A group $G$ is *polycyclic* if there exists a series $G = G_1 \trianglerighteq \ldots \trianglerighteq G_{n+1} = \{1\}$ such that every factor $G_i/G_{i+1}$ is cyclic.

Again, the central problem in this field is: given a polycyclic group $G$, determine the structure of $G$. A large number of algorithms is available for this purpose. For example, the order of $G$ can be determined readily, all kinds of specific subgroups can be calculated and, if $G$ is finite, then the automorphism group of $G$ can be computed effectively.

The class of polycyclic groups includes the finite solvable groups, the finitely generated nilpotent groups and in particular the groups of prime-power order. Basic introductions to computations with polycyclic groups are described in [60] and [30]. A more complete account is given in [18].

Despite the fact that there are various effective algorithms available for polycyclic groups, there are also some interesting open problems in this field, mostly for the case of infinite polycyclic groups. For example, it is not known whether there exists an algorithm for computing a minimal generating set of an infinite polycyclic group. Also, in [54] it is proved that automorphism groups of polycyclic groups can be determined algorithmically, but an effective algorithm with implementation is only available for finite polycyclic groups [61].

## 4.1 Polycyclic sequences and presentations

Algorithms for polycyclic groups are based on their internal structure and hence this structure needs to be exhibited in an algorithmically useful way.

**4 Definition:** Let $G = G_1 \trianglerighteq \ldots \trianglerighteq G_{n+1} = \{1\}$ be a polycyclic series. Let $g_i \in G$ with $G_i/G_{i+1} = \langle g_i G_{i+1} \rangle$. Then $\mathcal{G} = (g_1, \ldots, g_n)$ is a *polycyclic sequence* for $G$.

Polycyclic sequences are the fundamental tool on which all algorithms for polycyclic groups are based. They yield that $G_i = \langle g_i, \ldots, g_n \rangle$ and thus $\mathcal{G}$ generates $G$. The following lemma yields an important property of polycyclic sequences.

**5 Lemma:** *Let $\mathcal{G} = (g_1, \ldots, g_n)$ be a polycyclic sequence for $G$ and $r_i = [G_i : G_{i+1}]$. Then every element $g \in G$ can be written uniquely as $g = g_1^{e_1} \cdots g_n^{e_n}$ with $e_i \in \mathbb{Z}$ and $0 \leq e_i < r_i$ if $r_i < \infty$.*

Hence polycyclic sequences induce a map $\varphi : G \to \mathbb{Z}^n : g \mapsto (e_1, \ldots, e_n)$. Many algorithms with subgroups and factor groups in polycyclic groups are obtained by translating algorithms for $\mathbb{Z}^n$ via $\varphi$ into a non-commutative version for $G$.

Polycyclic groups admit very compact finite presentations to define them: the polycyclic presentations. These presentations have a polycyclic sequence $\mathcal{G}$ as set of abstract generators and their relators have the form:

$$
\begin{array}{rcl}
g_i^{r_i} & / & g_{i+1}^{e_{i,i+1}} \cdots g_n^{e_{i,n}} \\
g_j^{-1} g_i g_j & / & g_{j+1}^{f_{i,j,j+1}} \cdots g_n^{f_{i,j,n}} \text{ for } i > j \\
g_j g_i g_j^{-1} & / & g_{j+1}^{l_{i,j,j+1}} \cdots g_n^{l_{i,j,n}} \text{ for } i > j
\end{array}
$$

These presentations allow effective computations with the groups they define. In particular, the word problem is effectively solvable in such presentations.

## 4.2 Further algorithms for polycyclic groups

Polycyclic groups allow us to compute effectively with factor groups. This is used for many methods in combination with the following theorem.

**6 Theorem:** *Every polycyclic group $G$ has a normal series $G = N_1 \trianglerighteq \ldots \trianglerighteq N_{l+1} = \{1\}$ such that every factor $N_i/N_{i+1}$ is either free abelian or elementary abelian.*

Many algorithms for polycyclic groups proceed by induction on such a normal series. They assume that the desired object is computed in $G/N_l$ and they seek to extend this solution to $G$.

In the induction step we exploit that the conjugation action of $G/N_l$ on $N_l$ induces a homomorphism $\psi : G/N_l \to Aut(N_l) \cong GL(d, R)$ where $N_l \cong R^d$ for $R = \mathbb{Z}$ or $R = \mathbb{F}_p$. The homomorphism $\psi$ together with the cocycle class $\sigma \in H^2(G/N_l, N_l)$ describing $G$ as an extension of $G/N_l$ by $N_l$ determine $G$ completely. Thus the induction step reduces to computations with matrix representations and cohomology groups of $G$.

This type of approach is used, for example, for computing conjugacy classes of elements and subgroups and for computing the automorphism group if $G$ is finite.

## 4.3 Examples and applications

Polycyclic presentations are a very compact description for polycyclic groups. This is essential for the computation of restricted Burnside groups as in Section 3.4. These are determined as polycyclicly presented groups and this is currently the only representation which allows us to determine such large groups.

Algebraic number fields can be used to produce interesting examples of infinite polycyclic groups. Let $K$ be an algebraic number field with maximal order $O$ and unit group $U$. Then $U$ acts by multiplication from the right on the additive group $O$ and thus one can define the semidirect product $G = O \rtimes U$. As $O \cong \mathbb{Z}^n$ for some $n \in \mathbb{N}$ and $U$ is a finitely generated abelian group by Dirichlet's theorem, it follows that $G$ is polycyclic. Computations with this type of polycyclic group translate to computations with algebraic number fields.

## 5 Matrix Groups

The development of algorithms for matrix groups is a currently very active field of research. The central aim is similar to the permutation group topic: given $G = \langle g_1, \ldots, g_l \rangle \leq GL(d, R)$ for some commutative ring $R$, determine the structure of $G$.

The available methods for this purpose depend heavily on the considered ring $R$. Thus this area of algorithmic group theory is divided up further in various subtopics. At current, mainly the finite fields $R = \mathbb{F}_q$ and $R \in \{\mathbb{Z}, \mathbb{Q}\}$ or algebraic extensions of $\mathbb{Q}$ are investigated.

### 5.1 Finite fields

If $R = \mathbb{F}_q$ is a finite field, then $GL(d, \mathbb{F}_q)$ is finite. In this case $G$ has a faithful permutation representation of degree $q^d - 1$ by acting on the elements of $\mathbb{F}_q^d \setminus \{0\}$. However, the degree of this representation is often too large to allow a practical application of this permutation representation and hence algorithms for matrix groups of large degree or field try to avoid the use of this representation.

Most effort in this field is currently concentrated on the *matrix group recognition project*. The aim of this project is to develop practical and efficient algorithms to determine a composition series for $G$ and to recognize the simple factors of this series. The classification of finite simple groups and properties of the finite simple groups play a central role in this project.

As a fundamental basis for the recognition of a matrix group the following theorem by Aschbacher [2] is used. See also [31].

**7 Theorem:** (Aschbacher) *Let $G \leq GL(n, q)$ for $q = p^l$ and let $V = \mathbb{F}_q^n$ and $Z = Z(GL(n, q))$. Then one of the following holds:*

(1) *$G$ acts reducibly on $V$.*
(2) *$G$ acts imprimitively on $V$.*
(3) *$G$ preserves a tensor decomposition of $V$.*
(4) *$G$ preserves a symmetric tensor power decomposition of $V$.*
(5) *A conjugate of $G$ embeds into $\Gamma L(n/m, q^m)$, the group of semilinear maps.*
(6) *A conjugate of $G$ embeds into $GL(n, p^e)Z$ where $e \mid l$.*
(7) *$G$ normalizes an irreducible extraspecial or symplectic type group.*
(8) *$H' \leq G \leq HZ$ for a classical group $H$ on $V$.*
(9) *$G/(G \cap Z)$ is almost non-abelian simple.*

The first aim in the matrix group recognition project is now to determine the Aschbacher class of $G$. Randomized methods are a fundamental tool for this purpose. Every Aschbacher class gives either rise to some reduction of the original problem or it proves that the considered group is almost simple. A second aim in the matrix group recognition project is then to identify a simple group in the list of all finite simple groups. Solutions to this problem are based on methods from representation theory. We refer to [37] for further details.

### 5.2 Algebraic number fields

The finitely generated subgroups of $GL(d, K)$ for an algebraic number field $K$ fall into two classes by the following theorem of Tits [63]. A group is called virtually solvable *if it contains a solvable normal subgroup of finite index.*

**8 Theorem:** (Tits alternative) *Let $K$ be a field and let $G \leq GL(d, K)$ finitely generated. Then $G$ is virtually solvable or $G$ contains a non-abelian free subgroup.*

The 'Tits class' of a given finitely generated group $G \leq GL(d, K)$ for an algebraic number field $K$ can be computed, see [3, 6].

The case when $G$ contains a non-abelian free subgroup can be considered the "wild" case. For example, it is known that in such groups the conjugacy problem is in general undecidable, see [41], page 42. Consequently, computations with such groups are difficult and at current there is only little machinery available for them.

The case that $G$ is virtually solvable is somewhat "tamer". The class of virtually solvable groups contains the virtually polycyclic groups as a large subclass. By [3], we can determine a polycyclic presentation for polycyclic normal subgroup of finite index in virtually polycyclic matrix groups and this allows computations with these groups.

However, that at current it is not known how to check whether a finitely generated virtually solvable matrix groups is virtually polycyclic. Neither are there methods for computations with solvable, non-polycyclic groups available.

### 5.3 Examples and applications

Almost crystallographic groups are a generalization of crystallographic groups which arise in topology from the study of certain manifolds, see [14]. These groups are finitely generated virtually nilpotent and they arise naturally as matrix groups over $\mathbb{Q}$. Hence the approach described in Section 5.2 applies to them. This has been used successfully [15] to compute with these groups.

Matrix groups over finite fields play a role in the construction and investigation of finite simple groups. If possible, these groups are investigated by permutation groups methods. However, there are sporadic groups which are better represented by matrices. Groups of this type are the Janko group $J_4$ and the Monster group $M$. The Monster $M$ has order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

It can be represented by 196 882 dimensional matrices over $\mathbb{F}_2$ and its smallest known faithful permutation representation has degree 97 239 461 142 009 186 000. Computations with permutation representations of $M$ are currently impossible, while a matrix representation has been explicitly constructed and it has been used for certain (very limited) computations, see [29].

# 6 Classifications of Groups

The classification and the explicit determination of all groups of a certain type is often a natural computational problem. It usually requires various highly effective computational methods for groups of different representations. Hence such classifications are often high-level applications of computational group theory.

## 6.1 The groups of "small" order

The central aim in this topic is to determine for a given order $n$ an explicit list of groups such that every group of order $n$ is isomorphic to exactly one group in the list. This problem has been initiated in 1854 by Cayley and it has received much attention since; see [7] for an overview and a history.

Starting around 1990 this topic has become a computational topic. First, Newman and O'Brien developed an algorithm to compute all groups of a given prime-power order $p^n$. This algorithm was successfully used to determine the groups of order $2^n$ for $n \leq 9$ and a variation was used to count the 49 487 365 422 groups of order $2^{10}$. Then, Besche and Eick developed an effective algorithm to determine all groups of any given order $n$. These two algorithms have been employed to construct explicitly all 423 164 062 groups of order at most 2000 except $2^{10}$.

Interestingly, the classification of groups by order is also mentioned in Alan Turing's definition of a computer [28]: "*There will positively be no internal alterations to be made even if we wish suddenly to switch from calculating the energy levels of the neon atom to the enumeration of groups of order 720.*"

A more general aim is to classify all groups whose whose order has a certain factorization. For example, Hölder classified the groups whose order has at most three prime factor. More recently, in [44] the groups of order $p^6$ for a prime $p$ are determined and [16] yields the groups of cubefree order.

## 6.2 Transitive and primitive groups

Here the central aim is to determine for a given degree $n$ an explicit list of transitive or primitive subgroups of the symmetric group $S_n$ such that every transitive or primitive subgroup of $S_n$ is conjugate to exactly one group in the list. Also this topic has a long history; see [57] for a history and further references for the primitive group case.

The transitive groups of degree at most 31 have been determined by Hulpke [35]. The underlying idea of this construction is to reduce from transitive groups to primitive groups by investigating systems of imprimitivity. Thus the construction of transitive groups is based on the classification of primitive groups.

The primitive groups of degree at most 2500 have been listed by Roney-Dougal [52]. This construction is based on the O'Nan-Scott theorem which divides the primitive permutation groups into two types: those with solvable socle and those with insolvable socle. The primitive groups with solvable socle are affine; that is, they are of the form

$C_p^n \rtimes K$ where $K$ embeds as irreducible subgroup into $Aut(C_p^n) = GL(n,p)$. Hence their determination translates into algorithms for matrix groups and relies on representation theory. The primitive groups with insolvable socle are split up further by the O'Nan-Scott theorem; see [39] for details.

The solvable primitive groups are listed up to degree 6560 in [20]. These groups are all affine and thus their determination relies on representation theory for finite solvable groups.

## 7 Galois Theory

Galois' famous discovery that '*an irreducible polynomial* $f(x) \in \mathbb{Q}[x]$ *is solvable by radicals if and only if its Galois group* $G_f$ *is solvable*' is one of the mile-stones in algebra. The discovery leads directly to a computational problem: given an irreducible $f(x) \in \mathbb{Q}[x]$, check whether it is solvable by radicals and if so, then determine its roots as radicals.

For this purpose we first determine the Galois group $G_f$ of $f(x)$. This Galois group has a natural representation as a transitive subgroup of the symmetric group $S_n$ where $n = deg(f)$. There are various methods available for computing $G_f$, see for example [34, 25]. Most of them reduce the problem of computing the Galois group to the problem of determining the transitive subgroups of $S_n$. Thus the classification obtained in Section 6.2 plays a fundamental role in this problem.

Once the Galois group $G_f$ is available as a permutation group in $S_n$, it is comparatively easy to check whether $G_f$ is solvable. The available methods for permutation groups, see Section 2, facilitate an efficient check for this purpose.

Now it remains to translate the solvability of $G_f$ back into computing radicals for $f(x)$. This can be done by essentially translating the proof of Galois' theorem into an algorithm. However, to obtain an effective algorithm, various technical details need to be addressed. For example, an efficient method for factoring polynomials over an algebraic extension of $\mathbb{Q}$ is necessary as well as various other computational methods for permutation groups and algebraic number fields.

See [26, 17] for descriptions of algorithms to solve a polynomial by radicals.

## 8 Groups and Cryptography

Cryptography is one of the currently most active and most prominent areas of computational algebra. The central problem is that $A$ (Alice) wants to send a secret message $s$ to $B$ (Bob) via an insecure channel. Hence the message has to be encoded such that only $B$ can read it, but nobody else catching the message $s$ can. For this purpose a *one-way function* $f$ is used. Such a function has the property that $f(s)$ is easily computable, but $f^{-1}(t)$ is not.

There are various one-way functions known which are based on features of number theory. A well-known one is used to build the RSA cryptosystem: this is based on the fact that the product of two primes $p$ and $q$ is easy to compute, but factoring a product of two large primes into its factors is difficult.

Recently, new one-way-functions have been suggested which are based on non-commutative groups. One is the *Arithmetica key exchange* protocol, see [1]. Let $G$ be a finitely generated group with solvable word problem. Let $S$ and $T$ be two finitely generated subgroups of $G$ and let $\{s_1, \cdots, s_n\}$ and $\{t_1, \cdots, t_m\}$ be generating sets for $S$ and $T$, respectively. These objects are all publicly available. Then

- Alice chooses a secret element $a \in S$ written as word in the generators $a = s_{i_1}^{a_1} \cdots s_{i_l}^{a_l}$ and publishes $t_1^a, \ldots, t_m^a$.
- Bob chooses a secret element $b \in T$ written as word in the generators $b = t_{i_1}^{b_1} \cdots t_{i_h}^{b_h}$ and publishes $s_1^b, \ldots, s_n^b$.

Then Alice and Bob can both compute the commutator $[a, b]$ and use this as key:

$$\begin{aligned} [a,b] &= (b^a)^{-1} b = (t_{i_h}^a)^{-b_h} \cdots (t_{i_1}^a)^{-b_1} \cdot b && \text{computable for Bob} \\ &= a^{-1} a^b = a^{-1} \cdot (s_{i_1}^b)^{a_1} \cdots (s_{i_l}^b)^{a_l} && \text{computable for Alice} \end{aligned}$$

However, to determine $[a, b]$ based on the published data, one needs to find $a$ and $b$. These can be obtained by solving the conjugacy problem in $G$ and finding an element which conjugates $t_i$ on $t_i^a$ for $1 \leq i \leq m$ and an element which conjugates $s_j$ on $s_j^b$ for $1 \leq j \leq n$.

Hence it is now the aim to find groups $G$ with effectively solvable word problem and hard (or perhaps even unsolvable) conjugacy problem. Currently, various types of groups $G$ are under investigation in this respect.

## 9 Algorithms in Crystallography

Crystallographic groups are the symmetry groups of crystals. The interest in these groups arises from their applications in chemistry and physics. These groups occur naturally as rational matrix groups. By Bieberbach's famous theorems, there are only finitely many isomorphism types of crystallographic groups for any fixed dimension. It is natural computational problem to list the crystallographic groups in small dimensions.

This problem has been investigated by group theorists and crystallographers very early on. By 1900 the crystallographic groups of dimension at most 3 had been determined. The following table shows the numbers of groups for the currently classified dimensions, see [10] for the dimension at most 4 and [51] for the dimensions 5 and 6.

| dimension | number of groups |
|---|---:|
| 1 | 2 |
| 2 | 17 |
| 3 | 219 |
| 4 | 4 783 |
| 5 | 222 018 |
| 6 | 28 927 922 |

Algorithmic methods for investigating crystallographic groups are also of interest. For example, given a space group $G$ of small dimension, one wants to identify $G$ in the data-library of all crystallographic groups of that dimension and compute structure details about $G$. We refer to [19] and [49] for further methods.

## References


[1] I. Anshel, M. Anshel, and D. Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*, 6:287–291, 1999.

[2] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76:469–514, 1984.

[3] B. Assmann and B. Eick. Computing polycyclic presentations of polycyclic matrix groups. *Accepted by J. Symb. Comput.*, 2005.

[4] M. D. Atkinson, editor. *Computational group theory (Durham 1982)*. Academic Press, 1984.

[5] G. Baumslag, D. Epstein, R. Gilman, H. Short, and C. Sims, editors. *Geometric and Computational Perspectives on Infinite Groups*. Dimacs Series, volume 25. Amer. Math. Soc., 1996.

[6] R. Beals. Improved algorithms for the Tits alternative. In W. M. Kantor and A. Seress, editors, *Groups and Computation III*, pages 63–77. (DIMACS, 1999), 2001.

[7] H. U. Besche, B. Eick, and E. A. O'Brien. A millenium project: constructing small groups. *Internat. J. Algebra Comput.*, 12:623–644, 2002.

[8] A. V. Borovik and A. G. Myasnikov, editors. *Computational and experimental group theory (Baltimore 2003)*. Amer. Math. Soc., 2003.

[9] W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system I: The user language. *J. Symb. Comput.*, 24:235–265, 1997.

[10] H. Brown, R. Bülow, J. Neubüser, H. Wondratschek, and H. Zassenhaus. *Crystallographic Groups of Four-Dimensional Space*. John Wiley, New York, 1978.

[11] J. J. Cannon, editor. *Computational group theory I*. Volume 9 of J. Symb. Comput., 1990.

[12] J. J. Cannon, editor. *Computational group theory II*. Volume 12 of J. Symb. Comput., 1990.

[13] M. Dehn. Über unendliche diskontinuierliche Gruppen. *Math. Ann.*, 71:116–144, 1911.

[14] K. Dekimpe. *Almost-Bieberbach Groups: Affine and Polynomial Structures*, volume 1639 of *Lecture notes in Math.* Springer, 1996.

[15] K. Dekimpe and B. Eick. Computational aspects of group extensions and their applications in topology. *Exp. Math*, 11, 2002.

[16] H. Dietrich and B. Eick. Groups of cube-free order. *Accepted by J. Alg.*, 2005.

[17] A. Distler. Ein Algorithmus zum Lösen einer Polynomgleichung durch Radikale. Diplomarbeit, TU Braunschweig, 2005.

[18] B. Eick. Algorithms for polycyclic groups. Habilitationsschrift, Universität Kassel, 2001.

[19] B. Eick, F. Gähler, and W. Nickel. Computing maximal subgroups and Wyckoff positions of space groups. *Acta Cryst. A*, 53:467–474, 1997.

[20] B. Eick and B. Höfling. The solvable primitive permutation groups of degree at most 6560. *LMS J. Comput. Math.*, 6:29–39, 2003.

[21] D. B. Epstein, J. W. Cannon, D. F. Holt, S. V. Levy, M. S. Paterson, and W. P. Thurston. *Word processing in groups*. Jones and Bartlett, 1992.

[22] D. B. Epstein, D. F. Holt, and S. Rees. The use of Knuth-Bendix methods to solve the word problem in automatic groups. *J. Symb. Comput.*, 12:397–414, 1991.

[23] L. Finkelstein and W. M. Kantor, editors. *Groups and Computation*. Dimacs Series, volume 11. Amer. Math. Soc., 1991.

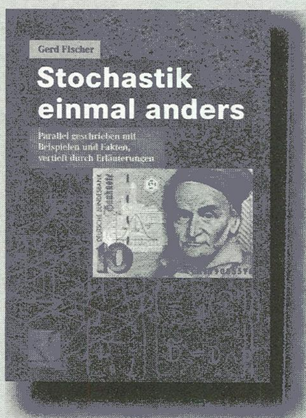
[24] L. Finkelstein and W. M. Kantor, editors. *Groups and Computation II*. Dimacs Series, volume 28. Amer. Math. Soc., 1997.

[25] K. Geissler and J. Klüners. Galois group computation for rational polynomials. *J. Symb. Comput.*, 30:653–674, 2000.

[26] G. Hanrot and F. Morain. Solvability by radicals from an algorithmic point of view. In *ISSAC 2001*, pages 175–182. ACM, 2001.
[27] G. Havas. Experiments in coset enumeration. In A. Seress and W. M. Kantor, editors, *Groups and Computation III*, pages 183–192. (DIMACS, 1999), 2001.
[28] A. Hodges. *Alan Turing, the enigma of intelligence*. Unwin Paperbacks, 1985.
[29] P. E. Holmes and R. A. Wilson. A new computer construction of the Monster using 2-local subgroups. *J. London Math. Soc.*, 67:349–364, 2003.
[30] D. F. Holt, B. Eick, and E. A. O'Brien. *Handbook of Comutational Group Theory*. Discrete Mathematics and its Applications. CRC Press, 2005.
[31] D. F. Holt, C. R. Leedham-Green, E. A. O'Brien, and S. Rees. Computing matrix group decompositions with respect to a normal subgroup. *J. Alg.*, 184:818–838, 1996.
[32] D. F. Holt and S. Rees. Testing for isomorphism between finitely presented groups. In *Groups, combinatorics and geometry*, pages 459–475. (Durham, 1990), Cambridge University Press, 1990.
[33] A. Hulpke. Investigating Cavicchioli's groups with GAP. Examples under www.gap-system.org, 1994.
[34] A. Hulpke. Techniques for the computation of Galois groups. In B. H. Matzat, G.-M. Greuel, and G. Hiss, editors, *Algorithmic Algebra and Number Theory*, pages 65–77, 1999.
[35] A. Hulpke. Constructing transitive permutation groups. *J. Symb. Comput.*, 39:1–30, 2005.
[36] W. M. Kantor and A. Seress, editors. *Groups and Computation III*. Walter de Gruyter, 2001.
[37] C. R. Leedham-Green. The computational matrix group project. In A. Seress and W. M. Kantor, editors, *Groups and Computation III*, pages 229–247. (DIMACS, 1999), 2001.
[38] J. S. Leon and C. C. Sims. The existence and uniqueness of a simple group generated by $\{3,4\}$-transpositions. *Bull. Amer. Math. Soc*, 83:1039–1040, 1977.
[39] M. W. Liebeck, C. E. Praeger and J. Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. (Series A)*, 44:389–396, 1988.
[40] E. H. Lo. A polycyclic quotient algorithm. *J. Symb. Comput.*, 25:61–97, 1998.
[41] C. F. Miller. *On group-theoretic decision problems and their classification*. Princeton University Press, 1971.
[42] J. Neubüser. An invitation to computational group theory. In *Groups in Galway/St. Andrews 1993*, London Math. Soc. Lecture, pages 457–475. Cambridge University Press, 1995.
[43] M. F. Newman and E. A. O'Brien. Application of computers to questions like those of Burnside, II. *Internat. J. Algebra Comput.*, 6:593–605, 1996.
[44] M. F. Newman, E. A. O'Brien, and M. R. Vaughan-Lee. Groups and nilpotent lie rings whose order is the sixth of a prime. *J. Alg.*, 278:383–401, 2003.
[45] W. Nickel. Computing nilpotent quotients of finitely presented groups. In *Geometric and computational perspectives on infinite groups*, Amer. Math. Soc. DIMACS Series, pages 175–191, 1995.
[46] A. C. Niemeyer. A finite soluble quotient algorithm. *J. Symb. Comput.*, 18:541–561, 1994.
[47] P. S. Novikov. On the algorithmic unsolvability of the word problem in group theory. *Trudy Mat. Inst. im. Steklov*, 44:143 pages, 1955.
[48] E. A. O'Brien and M. R. Vaughan-Lee. The 2-generator restricted Burnside group of exponent 7. *Internat. J. Algebra Comput.*, 12:575–592, 2002.
[49] J. Opgenorth, W. Plesken, and T. Schulz. Crystallographic algorithms and tables. *Acta. Cryst.*, A54:517–531, 1998.
[50] W. Plesken. Towards a soluble quotient algorithm. *J. Symb. Comput.*, 4:111–122, 1987.
[51] W. Plesken and T. Schulz. Counting crystallographic groups in low dimensions. *Experiment. Math.*, 9:407–411, 2000.
[52] C. Roney-Dougal. The primitive groups of order at most 2500. *Submitted*.
[53] M. Schönert. Analyzing Rubik's cube with GAP. Examples under www.gap-system.org, 1993.
[54] D. Segal. Decidable properties of polycyclic groups. *Proc. London Math. Soc.* (3), 61:497–528, 1990.
[55] A. Seress. An introduction to computational group theory. *Notices Amer. Math. Soc.*, 44:671–679, 1997.

[56] A. Seress. *Permutation group algorithms*. Cambridge University Press, 2003.
[57] M. W. Short. *The primitive soluble permutation groups of degree less than 256*, volume 1519 of *Lecture Notes in Math.* Springer, 1992.
[58] C. C. Sims. Computational methods in the study of permutation groups. In J. Leech, editor, *Computational problems in abstract algebra*, pages 169–183. Pergamon Press, 1970.
[59] C. C. Sims. The Knuth-Bendix procedure for strings as a substitute for coset enumeration. *J. Symb. Comput.*, 12:439–442, 1991.
[60] C. C. Sims. *Computation with finitely presented groups*. Cambridge University Press, Cambridge, 1994.
[61] M. J. Smith. *Computing automorphisms of finite soluble groups*. PhD thesis, Australian National University, Canberra, 1995.
[62] The GAP Group. GAP – *Groups, Algorithms and Programming, Version 4.4*. Available from http://www.gap-system.org, 2004.
[63] J. Tits. Free subgroups in linear groups. *J. Algebra*, 20:250–270, 1972.
[64] J. A. Todd and H. S. M. Coxeter. A practical method for enumerating cosets of a finite abstract group. *Proc. Edinburgh Math. Soc.*, 2:26–34, 1936.
[65] E. I. Zelmanov. On the restricted Burnside problem. In *Proceedings of the International Congress of Mathematicians, Kyoto, 1990*, pages 395–402. Math. Soc. Japan, Tokyo, 1991.

# So versteht man die Stochastik leicht




Gerd Fischer

**Stochastik einmal anders**

Parallel geschrieben mit Beispielen und Fakten, vertieft durch Erläuterungen

2005. VIII, 327 S. Br. EUR 24,90
ISBN 3-528-03967-1

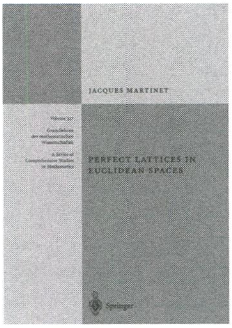
## INHALT

Beschreibende Statistik - Wahrscheinlichkeitsrechnung - Schätzen - Testen von Hypothesen - Anhang: Ergänzungen und Beweise

## DAS BUCH

Eine Einführung in die Fragestellungen und Methoden der Wahrscheinlichkeitsrechnung und Statistik (kurz Stochastik) sowohl für Studierende, die solche Techniken in ihrem Fach benötigen, als auch für Lehrer, die sich für den Unterricht mit den nötigen fachlichen Grundlagen vertraut machen wollen.
Der Text hat einen besonderen Aufbau - als Trilogie ist er in Beispiele, Fakten und Erläuterungen aufgeteilt.
Was überall in der Mathematik gilt, ist noch ausgeprägter in der Stochastik: Es geht nichts über markante Beispiele, die geeignet sind, die Anstrengungen in der Theorie zu rechtfertigen. Um dem Leser dabei möglichst viele Freiheiten zu geben, ist der Text durchgehend parallel geführt: links die Beispiele, rechts die Fakten.

vieweg
Abraham-Lincoln-Straße 46
D-65189 Wiesbaden
Fax 0611.78 78-420




J. Martinet
**Perfect Lattices in Euclidean Spaces**

Berlin u. a., Springer, 2003, 523 S., € 89,95

Das Buch „Perfect lattices in Euclidean spaces" ist eine überarbeitete und erweiterte Übersetzung der 1996 erschienenen französischen Ausgabe „Les réseaux parfaits des espaces euclidiens". Beide Werke sind aus Martinets langjähriger Erfahrung in Forschung und Lehre in der Theorie der euklidischen Gitter gewachsen. Sie sind auch für interessierte Nicht-Fachleute und Studenten zugänglich, wobei Vorkenntnisse in linearer Algebra weitestgehend ausreichen.

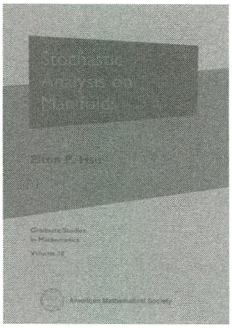
Eines der Hauptziele der Gittertheorie ist die Konstruktion dichter Gitter, wobei die Dichte eines Gitters als die Dichte der zugehörigen Kugelpackung definiert ist. Die Dichtefunktion hat auf dem Raum der Ähnlichkeitsklassen $n$-dimensionaler Gitter nur endlich viele lokale Maxima, sogenannte *extreme* Gitter. Eine über 100 Jahre alte Theorie charakterisiert extreme Gitter als solche, die *perfekt* und *eutaktisch* sind. Bis auf Ähnlichkeit gibt es nur endlich viele perfekte Gitter im $n$-dimensionalen euklidischen Raum. Ein zentrales Thema von Martinets Buch ist der Voronoi-Algorithmus zur Bestimmung aller Ähnlichkeitsklassen perfekter Gitter. Dieser grundlegende Algorithmus hat nicht nur gitterspezifische Anwendungen.

Nach einer kurzen Einführung in die wesentlichen Begriffe der Gitter in euklidischen Räumen und der Charakterisierung extremer Gitter gibt Martinet explizite Konstruktionen für die in verschiedenen Bereichen der Mathematik bedeutungsvollen Wurzelgitter und deren nahe Verwandte an. Diese Beispiele ermöglichen es ihm, mit klassischen kombinatorischen Methoden und ohne Benutzung des Voronoischen Algorithmus, die perfekten Gitter bis zur Dimension 5 zu klassifizieren. Der Voronoi-Algorithmus wird erst im darauffolgenden Kapitel beschrieben und benutzt um die mit dem Computer erzielten Ergebnisse in Dimension 6 und 7 zu begründen. Während es in Dimension 7 bis auf Ähnlichkeit nur 33 perfekte Gitter gibt, ist es in Dimension 8 praktisch nicht mehr möglich, alle perfekten Gitter zu bestimmen: die fast 11 000 bekannten perfekten Gitter in Dimension 8 sind durch Variationen des Voronoischen Algorithmus konstruiert worden, auf die in späteren Kapiteln des Buches eingegangen wird. Ungleichungen aus der Geometrie der Zahlen erlauben es dennoch zu beweisen, dass das Wurzelgitter $E_8$ das dichteste 8-dimensionale Gitter ist. Ein Werkzeug, u.a. für die Klassifikation dualextremer Gitter, d. h. der Gitter, bei denen das Produkt der Dichte des Gitters und seines dualen Gitters ein lokales Maximum annimmt, sind die *minimalen Klassen*, die den Raum der Gitter in gegebener Dimension pflastern. Zwei Gitter liegen in der gleichen minimalen Klasse, wenn sie die gleichen kürzesten Vektoren haben. Jedes perfekte Gitter bildet eine Klasse für sich, und jede minimale Klasse enthält höchstens ein eutaktisches Gitter. Die minimalen Klassen (und somit auch die eutaktischen Gitter) sind bis zur Dimension 5 bekannt, für Dimension 1–4 bestimmt Martinet sie in seinem Buch. All diese Begriffe haben Verallgemeinerungen auf gewisse Teilräume des Raums aller Gitter, wie zum Beispiel Gitter mit vorgegebener Symmetriegruppe oder mit festem niedrigerdimensionalen Teilgitter. In einem Anhang wird knapp auf die kürzlich von B. Venkov mit Hilfe von sphärischen Designs definierten stark perfekten Gitter eingegangen. Zu dieser Theorie ist die Monographie 37 in L'Enseignement Mathématique (2001) erschienen, die auch eine Ausarbeitung einer Vorlesung von B. Venkov enthält. Diese Vorlesung ist von Martinets homepage in

Bordeaux erhältlich, wo man auch Grammatrizen der bekannten perfekten Gitter und Errata zu beiden Büchern findet.

Das Werk ist ein exzellentes Lehrbuch und das einzige moderne Lehrbuch auf seinem Gebiet: Beginnend mit den grundlegenden Resultaten aus der Geometrie der Zahlen, welche in konkreten Situationen angewandt werden, führt es den Leser bis zu den neuesten Ergebnissen der Gruppe um Jacques Martinet. Dabei achtet Martinet sehr auf konkrete Beispiele und zieht dort, wo dies sinnvoll ist, explizite konstruktive Beweise dem reinen Verweis auf Computerberechnungen vor. Zu jedem Kapitel gibt Martinet zahlreiche Übungsaufgaben an, gefolgt von interessanten historischen Bemerkungen und Verweisen auf weiterführende Originalliteratur. Auch Nicht-Experten werden Freude daran finden, dieses Buch beispielsweise als Grundlage für eine Vorlesung zu benutzen.

Aachen G. Nebe




E. P. Hsu
**Stochastic Analysis on Manifolds**
Grad. Studies in Math. 38

Providence, Am. Math. Soc., 2002, 281 S., $ 44,–

Dieses Buch gibt eine Einführung in die Stochastische Analysis auf Riemannschen Mannigfaltigkeiten und ist dem Zusammenspiel von Brownscher Bewegung und Differentialgeometrie gewidmet, wie es in der Analysis von Laplaceoperatoren zutage tritt. Ähnlich wie auf einer Mannigfaltigkeit $M$ zu einem Vektorfeld $A_0 \in \Gamma(TM)$ ein Fluss gehört, läßt sich einem Differentialoperator $L$ zweiter Ordnung, etwa von der Form $L = A_0 + \sum_{i=1}^{r} A_i^2$ mit $A_i \in \Gamma(TM)$, ein stochastischer Fluss zuordnen, mit dem Unterschied, dass der Anteil zweiter Ordnung nunmehr dafür sorgt, dass die Flusslinien $t \mapsto X_t(\omega)$ von einem Zufallsparameter $\omega$ abhängen, derart dass sie zwar noch stetig, aber an keiner Stelle mehr differenzierbar sind. Im Mittel sind die Flusslinien jedoch differenzierbar, und die Ableitung von $t \mapsto \mathbb{E}[f(X_t)]$ an der Stelle $t = 0$ liefert den Operator $Lf$ für (beschränkte) glatte Funktionen $f$ auf $M$. Die Pfade der Brownschen Bewegung sind in diesem Sinn die Flusslinien des Laplace-Beltrami-Operators. Dies erklärt, warum sich Lösungen analytischer Probleme, die mit dem Laplaceoperator oder seinen Verallgemeinerungen in Verbindung stehen, oft explizit in Begriffen der Brownschen Bewegung gewinnen lassen. Während sich bei diesem Zusammenspiel von Analysis und Stochastik der Analytiker in der Regel dafür interessiert, was im Mittel passiert, gilt das Augenmerk des Stochastikers verstärkt dem pfadweisen Verhalten.

Elton Hsu's Buch gliedert sich in 8 Kapitel, wovon die letzten vier unabhängig voneinander gelesen werden können, und beginnt mit der Konstruktion von Diffusionen zu gegebenem Operator $L$ als Lösungen stochastischer Differentialgleichungen. Stochastische Differentialgleichungen auf Mannigfaltigkeiten kann man extrinsisch, intrinsisch oder lokal in Karten behandeln. Als Einstieg wird in Kapitel 1 der extrinsische Zugang mittels Whitney-Einbettung in den euklidischen Raum gewählt, wobei wie üblich mit Hilfe der Itôformel verifiziert wird, dass bei Start auf der eingebetteten Untermannigfaltigkeit die Lösung bis zur Lebenszeit auf ihr verbleibt. Zwar ist diese Methode geeignet, Brownsche Bewegungen zu konstruieren, jedoch sind die sich ergebenden Gleichungen lediglich für parallelisierbare Mannigfaltigkeiten kanonisch. Die intrinsische Konstruktion geht über das Orthonormalbasenbündel $O(M)$ der Riemannschen

Mannigfaltigkeit $M$ und benutzt die Tatsache, dass $TO(M) \to O(M)$ trivial ist (es wird durch die standardhorizontalen und standardvertikalen Vektorfelder auf $O(M)$ trivialisiert). Man konstruiert dabei als Lösung einer stochastischen Differentialgleichung eine Diffusion zu Bochner's horizontalem Laplaceoperator auf $O(M)$, die sich zu einer Brownschen Bewegung auf $M$ projiziert. Diese auf Eells-Elworthy-Malliavin zurückgehende Methode der stochastischen Abwicklung euklidischer Brownscher Bewegungen verallgemeinert die klassische Cartan-Abwicklung differenzierbarer Kurven und liefert $M$-wertige Brownsche Bewegungen, zusammen mit dem Paralleltransport längs der Pfade. Nach dem gleichen Schema definiert man für Mannigfaltigkeiten mit Zusammenhang die stochastische Abwicklung von stetigen Semimartingalen und den horizontalen Lift auf das Basenbündel. Martingale auf $M$ sind dabei die stochastischen Abwicklungen von lokalen euklidischen Martingalen. Sie beschreiben driftfrei fluktuierende stochastische Prozesse und sind relativ zu einem linearen Zusammenhang auf $M$ definiert. Dem entspricht die Tatsache, dass es für einen Differentialoperator $L$ zweiter Ordnung auf einer Mannigfaltigkeit keine kanonische Zerlegung in einen Anteil erster und zweiter Ordnung gibt: ein linearer Zusammenhang auf $M$ ist äquivalent einer solchen Spaltung, und Martingale sind dann die Diffusionen (Flusslinien) zu den Operatoren rein zweiter Ordnung. Das bekannteste Beispiel eines Martingals ist die Brownsche Bewegung, deren probabilistisches Verhalten an die metrische Struktur Riemannscher Mannigfaltigkeiten gekoppelt ist. Stochastische Abwicklung, horizontale Lifts und Martingaltheorie, zusammen mit der Integration von 1-Formen und Bilinearformen längs Semimartingalen, werden in Kapitel 2 ausführlich erörtert, während Kapitel 3 und 4 die Ergebnisse auf den Fall der Brownschen Bewegung und den Laplace-Beltrami-Operator spezialisieren. Die Itôformel für den Distanzprozess der Brownschen Bewegung zu einem fixierten Punkt wird in der allgemeinen Form mit Lokalzeit auf dem Schnittort abgeleitet; dabei wird der Einfluss von Krümmung auf den Radialprozess eingehend untersucht. Aus der Tatsache, dass der Wärmeleitungskern die Übergangsdichte der Brownschen Bewegung beschreibt, ergeben sich als Anwendung elementare Vergleichssätze für den Wärmeleitungskern $p(t, x, y)$ einer Riemannschen Mannigfaltigkeit. Kapitel 5 behandelt Probleme im Zusammenhang mit der Kurzzeitasymptotik von $p(t, x, y)$, wobei neben der klassischen asymptotischen Entwicklung für benachbarte Punkte $x, y$ eine allgemeine Methode für entfernte und zueinander konjugierte Punkte entwickelt wird. Varadhan's Formel $\lim_{t \downarrow 0} \ln p(t, x, y) = -d(x, y)^2/2$ wird für beliebige Punkte einer vollständigen Mannigfaltigkeit abgeleitet. Schließlich werden Abschätzungen für die logarithmische Ableitung erster und zweiter Ordnung des Wärmeleitungskerns gegeben; als Anwendung erhält man die Semimartingaleigenschaft der Brownschen Brücke.

Kapitel 6 enthält typische, das Langzeitverhalten der Brownschen Bewegung betreffende Betrachtungen. Bekanntlich legen asymptotische Eigenschaften der Brownschen Bewegung für $t \uparrow \infty$ den Raum der (beschränkten) harmonischen Funktionen auf $M$ fest. Im Gegensatz zum $\mathbb{R}^n$ sind Cartan-Hadamard-Mannigfaltigkeiten $M$, deren Schnittkrümmung zwischen zwei negativen Konstanten liegt, reichhaltig mit beschränkten harmonischen Funktionen ausgestattet. Betrachtet man die Eberlein-O'Neill-Kompaktifizierung $\bar{M} = M \cup M(\infty)$ von $M$, die durch Hinzunahme idealer Punkte bei $\infty$ entsteht, welche Äquivalenzklassen geodätischer Kurven repräsentieren, so kann man sogar das Dirichletproblem bei $\infty$ zu lösen, d. h. Randwerte von $M(\infty)$ harmonisch auf $M$ fortsetzen. Zerlegt man nämlich in globalen Polarkoordinaten auf $M$ Brownsche Bewegung in Radialteil und Winkelkomponente, so strebt der Radialteil gegen unendlich, während der Winkelprozess auf der Sphäre einen nichttrivialen Limes besitzt. Die Eintrittsmaße der Brownschen Bewegung in den Horizont bei $\infty$ definieren eine harmonische Maßklasse, aus der man wie beim klassischen Dirichletproblem mittels Integration die harmonischen Fortsetzungen erhält. Obere Krümmungsschranken sind dabei nötig, damit Brownsche Bewegung mit einer gewissen Geschwindigkeit schließlich Kompakta verläßt, während untere Schranken dazu dienen, mittels Winkelvergleichssätzen die Oszillationen der Winkelkomponente zu kontrollieren. Die konstanten Krümmungsschranken können aber erheblich abgeschwächt werden; die hier gegebenen Bedingungen für die Lösbarkeit des Dirichletproblems gehen auf Originalarbeiten des Autors zurück.

Martingale und Brownsche Bewegungen als driftfreie Zufallsbewegungen verknüpfen globale und lokale Geometrie von Mannigfaltigkeiten: im Verhalten für große Zeiten erfassen sie globale Eigenschaften der Mannigfaltigkeit, während ihr Kurzzeitverhalten durch die lokale Geometrie gesteuert wird. Dabei ergibt sich die Notwendigkeit, nicht nur Prozesse auf Mannigfaltigkeiten zu untersuchen, sondern die Betrachtung auf darüberliegende Bündel auszudehnen. So liftet man beim stochastischen Zugang zur Theorie der harmonischen Differentialformen die Brownsche Bewegung in geeigneter Weise auf die äußere Algebra des Kotangentialbündels und untersucht die Asymptotik des gelifteten Prozesses für $t \uparrow \infty$. Analoges gilt für *small-time heat equation problems*, wie etwa dem in Kapitel 7 behandelten stochastischen Zugang zur Indextheorie (Gauß-Bonnet-Chern, Atiyah-Singer). Hier wertet man die Asymptotik für $t \downarrow 0$ eines gewissen deformierten Paralleltransports längs Brownscher Schleifen in einem Cliffordbündel über $M$ aus. Die lokale Indexdichte errechnet sich dann auf einfache Weise als Erwartungswert der Superspur dieser „random holonomy“ bei Kontraktion der Brownschen Brücke zum konstanten Loop. Der Vorteil der stochastischen Methode ist, dass man die Superspur unter dem Erwartungswert auf dem Niveau von Zufallsvariablen auswerten kann; die entscheidenden Rechnungen reduzieren sich dadurch auf elementare lineare Algebra und die sogenannten „fantastic cancellations“ verlieren viel von ihrer Mystik.

Kapitel 8 schließlich gibt eine Einführung in die Stochastische Analysis auf Pfad- und Schleifenräumen über einer kompakten Mannigfaltigkeit. Unter anderem wird Driver's partielle Integrationsformel für den Gradientenoperator auf dem Pfadraum hergeleitet.Weitere Themen betreffen Gradientenformeln vom Bismutschen Typ, eine Version der Clark-Ocone-Formel für die Riemannsche Brownsche Bewegung, logarithmische Sobolevungleichungen auf dem Pfadraum und Hyperkontraktivität.

Der Austausch von Ideen zwischen Geometrie und Stochastik hat zweifelsohne beide Gebiete stimuliert. Aus richtungsweisenden Arbeiten sind große Theorieapparate gewachsen; etwa aus P. Malliavin's Zugang zu Hörmander's Hypoelliptizitätssatz ist ein umfassender Differentialkalkül auf dem Wienerraum entstanden (heute meist Stochastische Variationsrechnung oder kurz *Malliavin-Kalkül* genannt), aus J.-M. Bismut's stochastischem Beweis des Atiyah-Singer Indextheorems hat sich ein grundlegendes Instrumentarium von Techniken zur asymptotischen Entwicklung von Wärmeleitungskernen auf Vektorbündeln entwickelt. Aus der Sicht der Stochastik kann man schon heute sagen, dass die geometrische Methode das Gebiet revolutioniert hat. Trotzdem gelten Methoden der Stochastischen Differentialgeometrie nach wie vor als schwer zugänglich – und zwar in gleicher Weise für Stochastiker wie für Differentialgeometer. Nicht zuletzt mangelt es an grundlegenden Lehrbüchern, die man Vorlesungen oder Seminaren zugrundelegen könnte.

Das vorliegende Buch beabsichtigt kein Referenzwerk der Stochastischen Analysis auf Mannigfaltigkeiten oder auch nur eines Teilgebiets hiervon zu sein. Es ist konzipiert als Textbook für den graduate Studenten mit soliden Kenntnissen der euklidischen Stochastischen Analysis – insofern ist es aus der Perspektive des Stochastikers geschrieben. Der Zugang wird Nicht-Stochastikern aber dadurch erleichtert, dass konsequent die etablierte moderne Sprache der Differentialgeometrie verwendet und auf Nicht-Standard-Begriffsbildungen verzichtet wird. Geometrische Objekte (wie Zusammenhang, Jacobifeld, Schnittkrümmung) werden in der Regel ad hoc eingeführt und fortschreitend entwickelt; trotzdem dürften einschlägige Vorkenntnisse die Lektüre erheblich erleichtern. Geometrische Beweisschritte sind gelegentlich knapp abgehandelt, wobei sich an einigen Stellen auch Ungenauigkeiten eingeschlichen haben (z. B. am Ende des Beweises des Laplace-Vergleichssatzes 3.4.2 hinsichtlich der unteren Schranke). Insgesamt ist das Buch aber sehr sorgfältig geschrieben und gibt in der Regel vollständige Beweise, wenngleich es hohe Anforderungen an den Leser stellt. Überschneidungen mit vorhandenen Monographien (Elworthy [2], Emery [3], Ikeda-Watanabe [4] oder Malliavin [5]) sind gering, was nicht zuletzt für die Reichhaltigkeit dieses rasch expandierenden Gebiets spricht. Elton Hsu's Buch bietet zweifelsohne einen attraktiven Einstieg. Wer bei der Lektüre die nunmehr erstmals einem größeren Publikum zugänglichen Vorlesungen [1] von Élie Cartan an der Sorbonne 1926–27 zu Rate zieht, wird staunen, mit welcher Weitsicht Cartan's *méthode du repère mobile* vieles vorwegnimmt, was sich mehr ein halbes Jahrhundert später als entscheidende Weichenstellung beim Aufbau der Riemannschen Stochastischen Geometrie herauskristallisiert hat.

## References

[1] E. Cartan, *Riemannian geometry in an orthogonal frame.* From lectures delivered by Élie Cartan at the Sorbonne in 1926–27. Translated from the 1960 Russian edition with a foreword by S. S. Chern. World Scientific Publishing Co., Inc., River Edge, NJ, 2001.

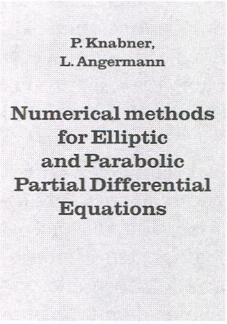
[2] K. D. Elworthy, *Stochastic Differential Equations on Manifolds.* London Math. Soc. Lecture Notes Series 70. Cambridge University Press, Cambridge, 1982.

[3] M. Emery, *Stochastic calculus in manifolds,* Springer-Verlag, Berlin, 1989.

[4] N. Ikeda and S. Watanabe, *Stochastic Differential Equations and Diffusion Processes.* Second Edition. North Holland Publ. Comp., Amsterdam, 1989.

[5] P. Malliavin, Stochastic analysis, Grundlehren der Mathematischen Wissenschaften, vol. 313, Springer-Verlag, Berlin, 1997.

Poitiers A. Thalmaier




P. Knabner,
L. Angermann
**Numerical methods for Elliptic and Parabolic Partial Differential Equations**

Berlin u. a., Springer, 2003, 424 S., € 79,95

Ich verwende dieses Lehrbuch, bzw. die bereits 2000 erschienene deutsche Ausgabe, zusammen mit [D] und [M] als Grundlage zur Vorbereitung von Vorlesungen auf dem Gebiet der Numerik partieller Differentialgleichungen. Ich möchte daher mit einer kurzen Abgrenzung des Stoffes des vorliegenden Lehrbuches zu [D] und [M] beginnen. Jedes dieser drei Bücher schafft es, den Bogen von der mathematisch präzisen Einführung der Methode der Finiten Elemente bis hin zu Anwendungen in der Strömungs- und Festkörpermechanik zu spannen. Auf die zentralen Themen wie die Eigenschaften verschiedener Finite-Element-Ansätze, adaptive Gitterverfeinerungstechniken sowie iterative Verfahren (inklusive Mehrgitterverfahren) zur Lösung der resultierenden Gleichungssysteme wird jeweils in gebotener Ausführlichkeit eingegangen. Dabei verwenden Brenner und Scott [M] durchweg eine etwas abstraktere Darstellung und beschäftigen sich detaillierter mit Approximationseigenschaften bezüglich verschiedener Normen inklusive Sobolev-Normen gebrochener Ordnung. Bei Braess [D] wird auf die Anwendung auf Modelle elastischer Verformungen in der Festkörpermechanik hingearbeitet, die dann im letzten Kapitel ausführlich behandelt wird. Auch das vorliegende Buch orientiert sich an einer Thematik aus den Anwendungen, wobei es sich hier um Strömungs-, Transport- und Reaktionsprozesse in porösen Medien handelt, die in einem einleitenden Kapitel 0 behandelt werden. Das Lehrbuch von Knabner und Angermann hat aber noch eine Reihe weiterer Besonderheiten zu bieten, die es zu einer wertvollen Bereicherung der Literatur auf diesem Gebiet machen.

Zunächst fällt auf, dass sehr viel Wert auf die Motivation der benötigten mathematischen Objekte gelegt wird. Ein Beispiel ist die Einführung eines geeigneten Funktionenraumes für die Variationsformulierung der Poisson-Gleichung und, damit verbunden, der schwachen Ableitung in Kapitel 2. Hier werden die Lücken anderer Ansätze sukzessiv ausgeräumt, bis sich am Ende (natürlich) der Sobolev-Raum $H^1(\Omega)$ ergibt. Ein anderes Beispiel betrifft die Interpretation von Randbedingungen in Sobolev-Räumen und die Formulierung eines Spursatzes in Kapitel 3. Diese Art der didaktischen Aufbereitung des Stoffes kommt dem kritischen Leser im Selbststudium ebenso entgegen wie sie sich für eine spannende Form der Vorlesung eignet. In Kapitel 4 wird neben der Thematik von a posteriori Fehlerschätzern und adaptiver Verfeinerung auch ein Überblick der für die Praxis relevanten Konstruktion von Ausgangstriangulierungen gegeben. Kapitel 5 ist den iterativen Verfahren zur Lösung der aus der Diskretisierung resultierenden linearen Gleichungssysteme gewidmet. Da die betrachteten Anwendungen teilweise auf nichtsymmetrische Matrizen führen, werden auch Krylov-Verfahren für solche Probleme behandelt. Ebenso fehlen natürlich auch Mehrgitterverfahren als in der Regel effizienteste Klasse von Lösern nicht.

Neben Finite-Element-Methoden, denen der größte Anteil des Buches gewidmet ist, werden auch Finite-Differenzen-Methoden (Kapitel 1) und Finite-Volumen-Methoden (Kapitel 6) eingehend diskutiert. Parabolische Anfangs-Randwertprobleme werden ausführlich in Kapitel 7 behandelt. Dabei wird der Zugang über die vertikale Linienmethode genommen, wobei detailliert auf die Besonderheiten bei der Verwendung finiter Differenzen, finiter Elemente bzw. finiter Volumen zur Ortsdiskretisierung eingegangen wird. In Kapitel 8 beschäftigen sich die Autoren mit der iterativen Lösung nichtlinearer Gleichungssysteme mittels Newton-Verfahren. Hierbei steht die Anwendung auf semilineare elliptische und parabolische Differentialgleichungen, wie sie im einführenden Kapitel als Modellgleichungen für Strömungs-, Transport- und Reaktionsprozesse in porösen Medien eingeführt wurden, im Mittelpunkt. Ebenfalls über diese Modelle wird die Problematik der konvektionsdominierten Probleme eingeführt, zu denen in Kapitel 9 geeignete Diskretisierungsmethoden (Stromlinien-Diffusion, Finite-Volumen und Lagrange-Galerkin) behandelt werden. Eine Fülle von Übungsaufgaben verschiedener Schwierigkeitsstufen zu allen Kapiteln sind zur Ergänzung des Stoffes eingefügt.

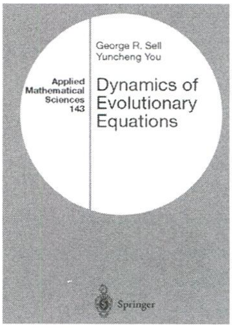
Mit der Ausrichtung ihres Lehrbuchs an einer Anwendungsthematik und dem Aufbau über das Einbeziehen vieler motivierender Grundüberlegungen ist den Autoren ein überzeugendes Werk gelungen. Zusammen mit [D] und [M] ist es ein unverzichtbarer Bestandteil für jeden auf diesem Gebiet arbeitenden Dozenten und sowohl für Studierende als auch für aktive Wissenschaftler in diesem Bereich zum Selbststudium sehr zu empfehlen.

## Literatur

[Bra01] Dietrich Braess. *Finite Elements: Theory, Fast Solvers, and Applications in Solid Mechanics.* Cambridge University Press, Cambridge, 2nd edition, 2001.

[BS02] Susanne C. Brenner and L. Ridgway Scott. *The Mathematical Theory of Finite Element Methods*. Springer, New York, 2nd edition, 2002.

Hannover G. Starke




G. R. Sell, Y. You
**Dynamics of Evolutionary Equations**
App. Math. Sciences 143

Berlin u. a., Springer Verlag, 2002, 670 S., € 94,95

In den letzten 40 Jahren hat sich die Theorie der Evolutionsgleichungen zu einer leistungsfähigen Methode zur mathematischen Behandlung von Problemen mit einer Zeit-Dynamik entwickelt. Eine große Stärke dieser Theorie liegt in ihrer Fexibilität, die es erlaubt von der Natur her sehr verschiedene Problemklassen mit der gleichen Methodik behandeln zu können. Partielle Differentialgleichungen wie Reaktions-Diffusionsgleichungen, nichtlineare Wellen- und Schrödinger-Gleichungen, Konvektions-Diffusionsgleichungen, speziell die Navier-Stokes-Gleichung, u. a., fallen ebenso in den Rahmen dieser Theorie, wie auch Funktional-Differentialgleichungen oder Integro-Differentialgleichungen vom Volterra-Typ.

Ziel der vorliegenden Monographie *is to prepare an entrée for scholars who are beginning their journey into the world of dynamical systems, especially in infinite dimensional spaces* (Zitat). Der Titel des Buches verspricht eine allgemeine Darstellung des momentanen Standes der Theorie der Evolutionsgleichungen. Allerdings hätte das Adjektiv *semilinear* im Titel erscheinen sollen, da mit Ausnahme von Kapitel 2 stets semilineare Gleichungen betrachtet werden, also Gleichungen der Form

$$(1) \quad \dot{u} + Au = F(u),$$

wobei $-A$ der Generator einer $C_0$-Halbgruppe im Banachraum $W$, also linear, und $F : D(A^\alpha) \to W$ lokal-lipschitz mit $\alpha \in [0, 1)$ ist. Der nichtlineare Anteil in der Gleichung ist daher in dieser Monographie stets von *niederer Ordnung*.

**Zum Inhalt des Buches:** Nach einem kurzen historischen Exkurs beginnt das Buch in Kapitel 2 mit einer Einführung in die Theorie der Halbflüsse auf vollständigen metrischen Räumen. Im Mittelpunkt steht hier der Begriff des globalen Attraktors, dessen Eigenschaften eingehend studiert werden. Es werden zwei Resultate über Existenz globaler Attraktoren bewiesen. Kapital 3 enthält eine Darstellung der Theorie linearer $C_0$-Halbgruppen. Die Sätze von Hille und Yosida sowie von Lumer und Phillips werden bewiesen – letzterer leider nur in Hilberträumen – und es werden differenzierbare und analytische Halbgruppen diskutiert. Sektorielle Operatoren und deren gebrochene Potenzen werden eingeführt und die Momenten-Ungleichung wird bewiesen – leider nur in Hilberträumen. Die Resultate werden zur Illustration auf lineare Diffusionsgleichungen, die Stokes-Gleichung und die Wellengleichung angewandt.

In Kapitel 4 werden lineare inhomogene Gleichungen mittels des Duhamelschen Prinzips studiert und verschiedene Lösungsbegriffe diskutiert. Diese Ergebnisse finden zur Behandlung der semilinearen Gleichung (1) Verwendung. Anwendung der in den ersten Kapiteln entwickelten Theorie auf konkrete partielle Differentialgleichungen werden in den folgenden zwei Kapiteln gegeben. Diese umfassen Reaktions-Diffusionsgleichungen, nichtlineare Wellengleichungen, Konvektionsgleichungen wie z. B. Burgers Gleichung, die Kuramoto-Shivashinsky Gleichung und die Cahn-Hillard Gleichung.

Der Navier-Stokes Gleichung ist ein ganzes Kapitel gewidmet. In Kapitel 7 werden die stabile und die instabile Mannigfaltigkeiten für autonome semilineare parabolische Gleichungen an einem hyperbolischen Equilibrium konstruiert, Existenz von Zentrumsmannigfaltigkeiten und das Reduktionsprinzip in Equilibrien mit Trichotomien bewiesen. Ein Abschnitt befasst sich mit der Asymptotik von Gradientensystemen und Morse-Zerlegungen, und ein weiterer mit dem Verhalten eines Halbflusses in der Nähe von normal-hyperbolischen invarianten Mannigfaltigkeiten. Schließlich behandelt das letzte Kapitel die Konstruktion von Intertialmannigfaltigkeiten. Jedes Kapitel (mit Ausnahme des Ersten) enthält einen Abschnitt mit Übungsaufgaben und einen mit Kommentaren und weiteren Zitaten. Einige funktionalanalytische Grundlagen sind in fünf Anhängen zusammengestellt. Das Literaturverzeichnis ist zwar umfangreich, muss aber dennoch als subjektiv angesehen werden, da verschiedene Autoren, die wichtige Beiträge zur Theorie der Evolutionsgleichungen geliefert haben, nur sehr selektiv oder gar nicht zitiert werden.

Bei der Durchsicht des Buches sind mir leider auch diverse gravierende mathematische Fehler aufgefallen, der Leser sei also gewarnt. Hier zwei Beispiele: Corollary 38.8 ist falsch, denn eine $C_0$-Gruppe ist nur dann differenzierbar, wenn ihr Generator beschränkt ist. Theorem 38.3 ist ebenso ein *wishful thinking theorem*, da der Rand des Gebiets $\Omega \in \mathbb{R}^n$ nur als Lipschitz vorrausgesetzt wird. Selbst im Fall $n = 2$ und $m = 1$ ist für solche Gebiete die Inklusion $D(A_p) \subset W^{2,p}(\Omega)$ i. a. *falsch*. Das Resultat ist aber richtig, wenn man $\partial\Omega \in C^{2m}$ fordert. Fehler dieser Art sind sehr ärgerlich und sollten in einem solchen Werk nicht vorkommen. Der von manchen Kollegen verfolgten Haltung *ja, es gibt Schwächen, aber im Großen und Ganzen stimmts ja* muss ich hier widerpsrechen! Unbeaufsichtigt kann man dieses Buch keinem Studenten in die Hand geben.

Dem oben zitiertem Anspruch wird diese Monographie im Hinblick auf semilineare Probleme zwar einigermaßen gerecht, der Leser wird aber trotzdem nicht umhin kommen, weitere Literatur zu Rate zu ziehen. Um eine kleine Auswahl ergänzender Bücher anzugeben, sei für die lineare Theorie auf die Bücher von Arendt et al. (Birkhäuser 2001) und Engel & Nagel (Springer, GTM 194, 2000) verwiesen, und für parabolische Gleichungen auf die Monographien von Amann (Birkhäuser 1995) und Lunardi (Birkhäuser 1995). Die Theorie der wichtigsten Klasse, nämlich die der quasilinearen Gleichungen kommt leider nur am Rande vor, wie auch weitere moderne Entwicklungen der Theorie fehlen, z.B. werden die Theorie maximaler Regularität, und die Lojasiewicz-Simon-Theorie nicht einmal erwähnt.

**Fazit:** Trotz der genannten Schwächen ist diese Monographie eine wertvolle Ergänzung der bestehenden Literatur und wird zu einer wichtigen Referenz für die Theorie semilinearer Evolutionsgleichungen werden, insbesondere hinsichtlich asymptotischem Verhalten. Allerdings möchte ich davor warnen, Resultate aus diesem Werk unkritisch zu übernehmen.

Halle — J. Prüß

ISSN 0012-0456