Olga Taussky (Mrs. John Todd) was born in what is now Czechoslovakia and was educated at the University of Vienna, where she received a Ph.D. in 1930 as a student of Philip Furtwängler. She held early positions at the Universities of Göttingen, Vienna, Cambridge, and London; and she was at Bryn Mawr College in 1934–1935 with Emmy Noether. During World War II she was a scientific officer at the Ministry of Aircraft Production in England. Afterwards she joined the National Bureau of Standards and then moved to Caltech where she became a professor in 1971. She has done extensive research in algebraic number theory, matrix theory, and topological algebra.

Some Noncommutativity Methods in Algebraic Number Theory

OLGA TAUSSKY

This article will not deal with classical Galois theory, nor K-theory, nor Langlands theory. It is an autobiographic piece by request, dealing with global aspects. It is split into the following sections:

1. The principal ideal theorem, class field towers, Theorem 94, capitulation.
2. Integral matrices.
3. Conclusion.

Literature

The existence of the two sets:
Reviews in Number Theory, ed. W. J. Le Veque, 6 vols., Amer. Math. Soc., Providence, R.I., 1976
which covers the period 1940–1972, and
Reviews in Number Theory, 1973–1983, ed. Richard K. Guy, 6 vols., Amer. Math. Soc., Providence, R.I., 1984
simplifies my bibliographical tasks.

I will accordingly usually give detailed references only to material issued prior to 1940 and to items which appear specially relevant to my treatment.

1. The principal ideal theorem, class field towers, Theorem 94, capitulation

A most impressive experience happened to me in my student days. A very important problem had been solved, and my thesis teacher was involved too. I became involved too and could not tear myself away from it for years and even returned to it temporarily a few years ago. At that time when my teacher Ph. Furtwängler had not yet found a suitable problem for me the news came through that Emil Artin in Hamburg had reduced the famous principal ideal theorem, at that time only a conjecture, to a problem on finite metabelian groups. Artin had found an explicit correspondence between the ideal class group of the ground field and the Galois group of the Hilbert class field with respect to the ground field. The Hilbert class field is the largest relative abelian and unramified extension of the ground field. The class field of the class field, the second class field, has as Galois group with respect to the ground field a metabelian group, with abelian commutator subgroup, and quotient group with respect to the commutator subgroup a group isomorphic to the class group of the ground field. Only p-groups needed to be considered. It is known that in this case the commutator subgroup can be generated by representatives of the quotient group of the commutator subgroup. This is a case of group extension, and the whole problem comes under the title "transfer of groups."

Artin communicated this to Furtwängler who felt that the group theory problem was in his reach. The reason for this optimism lay in the fact that his previous thesis student Otto Schreier, then in Hamburg, had worked on extension of groups and had developed certain relations which enter into this subject. Furtwängler seemed uniquely suited for proving the relation needed.

Furtwängler was a pioneer in class field theory. He had never met Hilbert, but he had studied Hilbert's work which involved as yet unproved statements and conjectures, some of which Furtwängler disproved. One of the latter was the fact that the class field has class number equal to one. The fact that all ideals of the ground field become principal, the so-called Hauptidealsatz (principal ideal theorem) was now reformulated as a group theoretic relation for nonabelian groups. For many weeks one did not see much of Furtwängler. He was a sick man who could not walk well and he used the snow on the streets as an excuse for staying at home. This was very hard on me for he had not given me a subject to work on, but suggested that I try to refind part of what Artin had done, saying that it was easy, which, of course, it was not. I overworked myself when trying to do it. When Furtwängler realized what he had done to me, he finally sat down and introduced me to the machinery he had developed in the meantime. I had no difficulty understanding this and Furtwängler let me reprove the preparatory relations. By the end of the summer Furtwängler announced that he had proved the principal ideal

theorem — via nonabelian p-group work. Although I cannot easily forgive him asking me to reprove part of Artin's ideas and even saying they were not too difficult, I can forgive him for rushing into a proof of the transfer relation which gives the proof of the principal ideal theorem for p-groups as Galois groups. Furtwängler's proof was not liked because it was heavily computational. I defended him when Emmy Noether expressed her feelings about this proof by saying that a first proof gives very much and ought not to be criticized. She reacted in a very friendly manner to my outburst. In due course other proofs emerged, one by Magnus, another one by Iyanaga, a student of Takagi, who had installed himself in Hamburg. There was also Hans Zassenhaus, a pupil of Artin who wrote the first modern book on group theory. Some references are given to others who reproved the principal ideal theorem. Artin published another paper in the *Hamburger Abhandlungen*, vol. 7 (the path breaking one was in vol. 5 — I will never forget this). Artin did indicate that the same method would get information about the subfields of the class field. Furtwängler said that he had now plenty of problems for my thesis. He himself wrote another paper proving the following theorem for $p = 2$:

> Let K be a field with 2-class group type $(2, 2, \ldots, 2)$. Then there exists a basis $c_1, \ldots, c_n$ for the class group such that each c_i becomes principal in a relatively quadratic unramified extension of K.

He then asked me to generalize this for odd p's starting with $p = 3$. However, it turned out that every p needed another condition, attached to $p - 2$, in such a way that $p = 2$ was no exception, only nicer. I only saw Furtwängler's proof when it was published.

E. Artin had heard about my thesis, possibly the first one written on the new ideas created by him. In a letter, handwritten by him, of which I possess a copy, he inquired about my results. However, later he found this investigation futile — when I met him years later he asked me whether I was still working on these hopeless questions. Furtwängler too had realized this in the meantime and withdrew from them turning to geometry of numbers and found many thesis problems there. However, with no other major problem, no class field colleague in the department, I tried to squeeze more out of these questions, with little success.

Hasse followed Hilbert's example and published a "book" inside the journal *Jahresbericht der Deutschen Mathematiker-Vereinigung* in two parts. Furtwängler checked part of his manuscript, but not all of his papers on class field theory are cited. Since Furtwängler was a member of the Vereinigung and was to receive the "book," Hasse suggested to him to give me the "reprint" he would send to him. Hasse, in his article in the Cassels–Fröhlich book, pointed to the work of Scholz and myself, mentioning the difficulty of our investigation. The only time I saw Furtwängler returning to class field theory

was when Takagi visited Vienna and called on Furtwängler. Takagi had by then obtained his famous results characterizing all abelian extensions as class fields. However, even he declined to discuss class field theory. But Takagi did actually listen to my new idea of studying the set of subfields of a given field with respect to which a field is an unramified class field. J. H. Smith generalized my work there. I have also a group-theoretic proof for the fact, proved by Furtwängler by number theory, that a field with class group of order 4 has a class field with cyclic class group. Hence the second class field has class number 1. This theorem had made its way into some group theory books, e.g., W. R. Scott, *Group Theory* (Prentice Hall, 1964).

While I was working on my thesis, a young German, a pupil of Schur, turned up. He was still working on his thesis, I think, which was related to Furtwängler's ideas. I saw him talk to Furtwängler. I gathered that he was very gifted and interested in computing. So when I wanted to find out whether a certain group of order 27 with given relations could be the Galois group of a second class field I wrote to him and asked if he could find a field for which this situation would hold. It did not take long before he supplied me with such a field. It was a cubic subfield of the field product $K_{19}^3 K_{1129}^3$ where K_p^l (p, l prime numbers) is the subfield of degree l of the field of pth roots of unity. His name was Arnold Scholz. In 1930, I went to Königsberg where a meeting of the Deutsche Mathematiker-Vereinigung took place (Hilbert gave a famous lecture on logic there). I gave a lecture on my thesis and met famous people like Noether and Hasse. I recognized Scholz and since our mathematical interests were clearly related (he was a few years older and had already several publications by then) we started a conversation. Soon after I returned to Vienna I had a letter from him suggesting joint work by correspondence, at this time on the field $Q(\sqrt{-3299})$, which has a noncyclic 3-class group of order 27. In connection with this work he wrote an important paper on cubic fields. We added another part to this paper studying the second 3-class groups of certain imaginary quadratic fields. I could be particularly helpful there since my training in number theory had turned out (not with my real preference) more group theoretical than arithmetic. The fields studied were to have 3-class groups of type (3, 3) hence the first class field has its relative Galois group of type (3, 3).

By Hilbert's Theorem 94 at least one ideal class of order 3 becomes principal in each unramified extension field of relative degree 3, a property Scholz called "capitulation," by now generally accepted. In our case it was exactly one class. The pattern of capitulation gave us information on the Galois group of the second 3-class field and even higher ones and it turned out that they came to an end after a finite number.[1] This was information on the

[1] I understand that Gold and his student Brink have found one error in our capitulation table, by computer.

so-called "class field tower." Furtwängler had suggested the problem of finding out whether it had to break down after a finite number of steps. I then suggested the name "group tower" for the set of Galois groups with respect to the ground field of these fields.

I further conjectured that the class field tower had to break down because the group tower had to break down. Scholz did not really believe in this. Anyhow this idea was defeated. The first one to do this was Noboru Ito for $p = 3$. However, Magnus was able to show that arbitrarily long group towers can exist. He invented a very ingenious method for this which on its own is very much appreciated. Later Zassenhaus, a guest at Caltech, showed to C. Hobby, my thesis student, the sketch of a very elegant matrix method which led to infinite 2-group towers apart from a small number of exceptions. Serre succeeded for all cases. However, an infinite class field tower was constructed by Golod and Safarevic. At an international congress Safarevic announced that while people some 20 years earlier had tried to prove the breaking up of the class field tower by group theory he saw a way for contradicting this by group theory.

In 1931, I attended a meeting of the Deutsche Mathematiker-Vereinigung for the second time, of course, also hoping to find a position. It was a very interesting meeting, e.g., Gödel was there, and, of great importance for my future. One of my teachers in Vienna, Hans Hahn, spoke to Professor Courant from Göttingen about helping me. It was a very difficult time for young people. My lecture at that meeting was, of course, in class field theory, and they actually needed somebody at that time with knowledge in that field. There were not many young people with a thesis in class field theory and they were trying to publish Hilbert's collected works, with number theory as volume I. The two editors they had working on editing that book had no training of that kind. Hence I was brought to Göttingen not much later.

Now I want to return to Furtwängler once more. I really have very great feelings of gratitude for him. He might have given me a little thesis problem in number theory. It would have spared me from my sufferings. But being introduced to such a profound mountain of great beauty has lifted me up forever. Furtwängler was a very hardworking and talented man. He had many thesis students and found appropriate thesis subjects for all of them. But he also found subjects for the survey articles which were demanded for students who did not write a thesis, but planned to take up teaching in high schools. Algebraic number theory was merely taught in a 2-hour seminar, himself lecturing, no homework. His ill health prevented him from contacts with the steadily growing abstract algebra developments which took place in Germany under the influence of Schur, Artin, Hasse, Noether, van der Waerden, and others and their flourishing schools. Hence my education in this respect was insufficient. One of our teachers in Vienna, a young and enthusiastic man, Karl Menger, a former colleague of O. Schreier in Hamburg, noticed this

deficiency. He ran a seminar where abstract algebra was studied. He even invited a former thesis student of Emmy Noether, Heinrich Grell, to visit (he was a former colleague of Nöbeling, who was a thesis student and assistant to Menger) to lecture to us. I recall how excited I was when he introduced left and right ideals in rings. I had never heard about them previously. The books by van der Waerden had not yet appeared.

Furtwängler was also hostile to p-adic numbers. I wonder whether he had a dislike for Hensel. He used to say that it was sufficient to use the infinite sequence of congruences which they replace. Furtwängler felt very pleased and honored when he was invited to write the article on "General algebraic number theory" for the new edition of the *Enzyklopädie der mathematischen Wissenschaften.* However, this article was so old fashioned that Hasse and Jehne published a revised edition; Furtwängler had died in the meantime.

So when I came to Göttingen for 1931–1932 not only did I face the hard work of editing Hilbert's work, which contained errors and wrong conjectures, but I was faced with modern abstract algebra of the highest level and had difficulties. There were two very talented young men eagerly awaiting me: One was W. Magnus, a pupil of Dehn in Frankfurt who had worked on infinite groups and his paper on the Freiheitsatz is still very well known, the other H. Ulm, a pupil of Toeplitz who is known for his work on infinite abelian groups. They had not known about class field theory and in addition had little experience in proofreading while Professor Menger made me do quite a bit of such work. In Göttingen I was also asked to attend Courant's course on partial differential equations and grade homework. (Secretly he hoped to win me over to this subject, still the favorite one in the "Courant group." Later, when I was recruited into aerodynamical work in London during WWII, I wished I had learned more about this subject then. I also learned to appreciate its beauty.) However, at that time there was E. Noether, the champion of abstract algebra, waiting for me eagerly. She told me that she and Deuring, her favorite student, had studied class field theory and expressed the hope that her tools of abstract algebra would reprove the current achievements in algebraic number theory. She had frequent visits from Hasse, van der Waerden and, at least once during my stay, E. Artin. She ran a seminar on class field theory in which I lectured too, on cyclic unramified extension fields. There was also Landau who, at least once, made me lecture on Mertens. Emmy was amazed to hear that Hilbert's work contained errors on many levels. She was an editor of part of Dedekind's collected works and felt certain that he made no errors. She discovered that the groups Hilbert associated with the prime ideals in normal fields were already Dedekind's work and insisted that they be renamed as Dedekind–Hilbert groups. She kept on finding more items in Dedekind attributed to others, but once I heard Hasse remarking that she was going too far there. The editing of Hilbert's book

was particularly burdensome (although some people told me to make a lifetime employment out of this) since it was a deadline job, to be completed by Springer for Hilbert's 70th birthday. Hilbert was pleased about his papers being published, but had no wish to be involved in the editing. However, he said to me clearly that his work in algebraic number theory had been more satisfying to him than his other contributions.

Since I knew more mathematicians than my two colleagues did, I wrote to people asking if they knew of any errors in the volume and I received helpful replies. I recall particularly Fueter and Speiser in Zurich. But they also wrote that it was wrong to reproduce the Zahlbericht since its presentation was not the best for algebraic number theory; also Schur did not care for reprinting this volume according to what Emmy, who had seen him during the Christmas vacation, reported. I suppose they preferred the treatment of Dickson in *Algebras and their arithmetics*. Emmy made no comments herself, of course, she was very much attached to Hilbert and anyhow there was no question of rewriting Hilbert's Zahlbericht instead of editing it. I heard Emmy frequently shout out: "Dies muss hyperkomplex bewiesen werden". She herself had a very good year at that time. She had reproved and extended Gauss' Principal Genus Theorem by methods one would later call cohomology. Again I heard her saying ($1 - S = 2$ when $S = -1$) meaning that the operator $1 - S$ leads to squaring when S means "the inverse." She was preparing herself for her 1-hour address at the International Congress at Zurich the same year.

After the Congress I did not see her again until I arrived at Bryn Mawr College in 1934. Among other activities she asked me to present the fundamental items of algebraic number theory to the small class formed by M. Weiss, a group theoretician, Grace Shover, a pupil of MacDuffee (on algebras), Ruth Stauffer, who wrote a thesis under Noether on the integral basis (extending work of Speiser), published in *Amer. J. Math.* **58** (1936) 585–599. The previous year they had studied van der Waerden's book, vol. 1, which had appeared not long before. Now they wanted to study some seminar notes by Hasse. But they had first to revise their number theory. MacDuffee seemed unattached to the big schools like Dickson's, but had worked on algebras on his own. Emmy appreciated him and since she was corresponding with Deuring in Göttingen on the preparation of his book *Algebren* she informed him of MacDuffee's and Grace's thesis publications for his list of references. I met MacDuffee later at meetings of the American Mathematical Society. I will discuss his influence on my work later.

As soon as I started my elementary lectures Emmy flared up and criticized my approaches, which I had taken from Furtwängler, who had taken them from Hilbert. In Göttingen she had not informed me of her feelings. I learned there Emmy's concepts of "cross products" and "factor systems." She cited Artin as saying that the Zahlbericht had held algebraic number theory back for years. Later I was criticized by Mac Lane for not giving Emmy

credit in my article on her when referring to her work in Göttingen. He introduced his student Lyndon to cohomology and was led to the well-known book "Eilenberg and Mac Lane".

Although I have used cohomology in some of my work, I have not used it in algebraic number theory, but I am a great admirer of the paper by Brumer and Rosen.

When at Bryn Mawr I traveled frequently with Emmy to Princeton and increased my knowledge in topological algebra there. This helped me finally to break away from my "hopeless work" in class field theory for the time being.

After Bryn Mawr I went almost straight to Cambridge, England where I was to stay for the next two years. There number theory was the work on the Hardy–Wright book and otherwise analytic number theory. However, I gave a voluntary short course during my last term. Heilbronn, of course, was there after his famous achievement concerning the Gauss conjecture. He was interested in working with me on the influence of the Galois group on the ideal class group. However, I had planned to go on with topological algebra on one hand and, on the other hand look for help from Philip Hall, a known expert on p-groups. While B. H. Neumann had a certain interest in my attempts in topological algebra, P. Hall did not know enough class field theory to help with the group-theoretic problems connected with capitulation.

I myself had no chance of teaching algebraic number theory apart from a brief course on class fields, the year after I had left Cambridge, but visited there for one day each week. It was at that time that Hilbert's Theorem 94 started to fascinate me and I hoped to do something about it some day.

I could only teach algebraic number theory again after I was appointed at Caltech in 1957. (I had an odyssey in my academic life for almost 20 years; it included WW II and heavy employment duties otherwise.) Remembering Emmy's dislike for my presentation of it at Bryn Mawr I promised myself to teach it "the modern way." One day the best student in my class came up to me with a small book in his hand. It was H. Mann's book on the subject. Mann was a thesis student of Furtwängler, like myself, and the student wanted me to follow this, actually very nice, book. Bringing up H. Mann gives me the opportunity of mentioning that I possess a write-up by him in which he points out a list of errors in Hilbert's and Furtwängler's work.

I come now to Hilbert's Theorem 94. It concerns unramified relative cyclic extensions of relative degree a prime p. In such a field an ideal class of the ground field, not in the principal class there, becomes principal. It is an "existence" statement.

Although what I am going to describe now happened much later and is still of great interest, I will discuss it now for two reasons: It is still class field

theory and further it is connected with my thesis and the work of Furtwängler that preceded and my work with Scholz.

Hilbert had erred about his conjecture concerning the class number of the class field, he had not been able to prove the principal ideal theorem, but he had Theorem 94 with a very elegant proof which informs on the capitulation in the class field. Deuring, in his *Zentralblatt* review of my thesis-attached paper in *J. Reine Angew. Math.*, had pointed out that Theorem 94 had not yet been proved by group theory. One day our group theorist M. Hall produced such a treatment. Zassenhaus then played a role in this. He invited me to give a lecture at a so-called Special Session at a meeting of the American Mathematical Society. (He also invited me to become an editor of his newly formed *Journal of Number Theory*. Some recent number-theoretic work of mine had been appreciated by him.) The lecture was supposed to be of computational nature. I decided to study the joint work with Scholz for $p > 3$. There I noticed two new facts turning up:

(a) a certain commutator which turns up with a power $\sum^{p-1} n^2 \equiv 0(p)$ for $p > 3$;

(b) there are 2 cases to be considered. Each cyclic extension of degree p of a field corresponds to a subgroup of the class group of the ground field. The class which capitulates may be contained in this subgroup or it may not. Hence one has these two cases to consider, a fact which is somehow also contained in the group-theoretic proof.

I had the good fortune of having H. Kisilevsky, a student of Iwasawa, working at Caltech by then. Both of us published papers concerning this problem. Kisilevsky interpreted my observations by cohomology. Somehow, since our work the title Hilbert Theorem 94 has become a title for publications. An example for this is the work of Miyake, who published a chain of such papers. There is also an earlier paper by Iwasawa using cohomology on related material.

Examples of work connected with Theorem 94 are still not plentiful. There is a thesis written under the late Bob Smith in Toronto, by S. H. Chang, concerning related matters. Further, Heilbronn's student Callahan's thesis is connected too.

During my stay in Göttingen, Artin came there to give three lectures, to introduce Herbrand's methods to class field theory. I took careful notes, even adding certain items. They were used in lectures very frequently. Finally, Robert Friedman, a student of Tate, translated them into English and they were incorporated into H. Cohn's book *A classical invitation to algebraic numbers and class fields.*

I will now leave the subject of class field theory in this article, apart from a postscript.

LITERATURE BEFORE 1940

E. Artin, Beweis des allgemeinen Reziprozitätsgesetzes, *Abh. Math. Sem. Univ. Hamburg* **5** (1927) 353–363.

——, Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz, *Abh. Math. Sem. Univ. Hamburg* **7** (1930) 46–51.

Ph. Furtwängler, Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers, *Math. Ann.* **63** (1906) 1–37.

——, Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern, *Math. Ann.* **67** (1903) 1–50; **72** (1912) 146–386; **74** (1913) 413–429.

——, Beweis des Hauptidealsatzes für die Klassenkörper algebraischer Zahlkörper, *Abh. Math. Sem. Univ. Hamburg* **7** (1930) 14–36.

——, Über das Verhalten der Ideale des Grundkörpers im Klassenkörper, *Monatsh. Math.* **27** (1916) 1–15.

——, Über eine Verschärfung des Hauptidealsatzes, *J. Reine Angew. Math.* **167** (1932) 379–387.

H. Hasse, Bericht über Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I, Ia, II *Jahresber. d. deutsch. Math. Ver.* **35** (1926) 1–55, **36** (1927), 233–311, Erg. **6** (1930) 1–204.

S. Iyanaga, Zum Beweis des Hauptidealsatzes, *Abh. Math. Sem. Univ. Hamburg* **10** (1934) 349–357.

W. Magnus, Über den Beweis des Hauptidealsatzes, *J. Reine Angew. Math.* **170** (1934) 235–240.

——, Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring, *Math. Ann.* (1935) 259–280.

A. Scholz and O. Taussky, Die Hauptideale der kubischen Klassenkörper imaginärquadratischer Körper: ihre rechnerische Bestimmung und ihr Einfluss auf den Klassenkörperturm, *J. Reine Angew. Math.* **171** (1934) 19–41.

——, Zwei Bemerkungen zum Klassenkörperturm, *J. Reine Angew. Math.* **161** (1929) 201–207.

H. G. Schumann, Zum Beweis des Hauptidealsatzes, *Abh. Math. Sem. Univ. Hamburg* **12** (1938) 42–47 (W. Franz Mitwirkung).

O. Taussky, Über eine Verschärfung des Hauptidealsatzes für algebraische Zahlkörper, *J. Reine Angew. Math.* **168** (1932) 25–27.

——, On unramified class fields, *J. London Math. Soc.* **12** (1937) 85–88.

——, A remark on the class field tower, *J. London Math. Soc.* **12** (1937) 82–85.

SPECIALLY RELEVANT

J. Browkin, On the generalized class field tower, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **11** (1963) 143–145.

J. W. S. Cassels and A. Fröhlich, eds., Algebraic Number Theory. (Proceedings of the Brighton Instructional Conference, Brighton, 1965), Washington, D.C.: Thompson, 1967. [These Proceedings played a considerable part in restimulating activity in Algebraic Number Theory.]

E. S. Golod and I. R. Safarevic, Über Klassenkörpertürme, [In Russian], *Izv. Akad. Nauk SSSR Sér. Mat.* **28** (1964) 261–272. Also see *Amer. Math. Soc. Transl.* Ser. (2) **48** (1965) 91–102.

C. R. Hobby, The derived series of a finite p-group, *Illinois J. Math.* 5 (1961), 228–233.

N. Ito, A note on p-groups, *Nagoya Math. J.* **1** (1950) 115–116.

K. Iwasawa, A note on the group of units of an algebraic number field, *J. Math. Pures Appl.* (9) **35** (1956) 189–192.

H. Kisilevsky, Some results related to Hilbert's Theorem 94, *J. Number Theory* **2** (1970) 199–206.

R. Schoof, Infinite class field towers, *J. Reine Angew. Math.* 372 (1987) 209–220.

J.-P. Serre, Sur une question d'Olga Taussky, *J. Number Theory* **2** (1970) 235–236.

J. H. Smith, A remark on fields with unramified compositum, *J. London Math. Soc.* (2) **1** (1969) 1–2.

O. Taussky, A remark concerning Hilbert's Theorem 94, *J. Reine Angew. Math.* 239/240 (1970) 435–438.

O. Taussky, Arnold Scholz zum Gedächtnis *Math. Nachr.* **7** (1952) 379–386. (This paper discusses the latest ideas of Scholz which were taken up by Jehne and his school. Note also *J. Reine Angew. Math.* **336** (1982) with Scholz's picture, a page on his life and work, a paper by F.-P. Heider and B. Schmithals "Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen" on pp. 1–25.

A. Weil, Sur la théorie du corps de classes, *J. Math. Soc. Japan* **3** (1951) 1–35.

H. Zassenhaus, *Theory of groups*, second edition, New York: Chelsea, 1958.

Postscript to Section 1

Artin's idea for the proof of the principal ideal theorem and O. Schreier's work used by Furtwängler came under the concept of group and field extensions.

The genus field and group, as studied by Fröhlich, is also relevant. It used to be introduced for abelian fields only. However, Fröhlich describes it as the maximal nonramified extension obtained by composing the given field with absolutely abelian fields.

Literature before 1940

C. G. Latimer and C. C. MacDuffee, A correspondence between classes of ideals and classes of matrices, *Ann. Math.* **74** (1933) 313–316.

A. Scholz, Totale Normenreste, die keine Normen sind, als Erzeuger nicht abelscher Körpererweiterungen, *J. Reine Angew. Math.* **175** (1936) 100–107, II, **182** (1940) 217–234.

O. Schreier, Über die Erweiterung von Gruppen I, *Monatsh. f. Math.* **34** (1926) 165–180. II, *Abh. Math. Sem. Hamburg* **4** (1926) 321–346.

SPECIALLY RELEVANT

G. Cornell and M. Rosen, Group-theoretic constraints on the structure of the class group. *J. Number Theory* **13** (1981) 1–11.

Y. Furuta, The genus field and genus number in algebraic number fields, *Nagoya Math. J.* **29** (1967) 281–285.

G. Gras, Extensions abéliennes non ramifiées de degrée premier d'un corps quadratique, *Bull. Soc. Math. France* **100** (1972) 177–193.

K. Hoechsmann, l-extensions, in: *Algebraic Number Theory*, ed. by Cassels and Fröhlich. (Proceedings of the Brighton Instructional Conference, 1965). Washington, D.C.: Thompson, 1967.

H. Koch, Galoissche *Theorie der p-Erweiterungen*; Introduction by I. R. Safarevic. Berlin-New York: Springer and Berlin: VEB Deutscher Verlag der Wissenschatten, 1970. Many references.

B. Mazur and A. Wiles, Class fields of abelian extensions of Q, *Invent. Math.* **76** (1984) 179–330.

K. Uchida, On imaginary Galois extension fields with class number one, *Sugaku* **25** (1973) 172–173.

2. INTEGRAL MATRICES

This brings me to my next section, the one of greatest interest to me. Complications dictated by the circumstances of my life have not always allowed me to devote myself to my favorite subject, number theory. My thesis was mainly in group theory. I was rescued for some time by working with Arnold Scholz. The war, WW II, made a numerical analyst of me in Great Britain and later in the USA (with some exceptional breaks through the influence of MacDuffee's work and collaboration with E. C. Dade and M. Newman). In 1957, I started my work at Caltech. Working with thesis students, postgraduates, temporary colleagues like E. C. Dade, Kisilevsky, Estes, Guralnick, P. Morton, P. Hanlon, and other brilliant visitors was terrific. Some of it was number theory. It was noncommutative and concerned integral matrices. H. Cohn permitted me to add an appendix on integral matrices to his 1978 Springer book; I also contributed to Roggenkamp's 1981 volume, Springer Lecture Notes #882.

In M. Newman's book *Integral matrices* (Academic Press 1972, chapter X, 15), he mentions a theorem (obtained jointly with myself) concerning integral circulants: A unimodular circulant of the form AA', where A is a matrix of rational integers, is equal to CC' where C itself is again a unimodular circulant of rational integers (the theorem itself arose from my idea of generalizing the concept of normal basis). Circulants can be looked upon as "group matrices" under the definition given in my article "A note on group matrices." As Newman mentions, the theorem was generalized to statements for more general groups and finally for all groups by Rips, 1973.

Another concept to be mentioned here is the discriminant matrix, the integral symmetric matrix whose determinant is the discriminant of an algebraic

number field. The quadratic form associated with this matrix is a "trace form." A paper by myself, entitled "The discriminant matrix of an algebraic number field" showed that this matrix has nonnegative signature. This was used by P. E. Conner and R. Perlis, who wrote the book *A survey of trace forms of algebraic number fields* (World Scientific, 1984).

The fact that the unit of finite order in the group ring of the S_3 does not contain a multiple of the unit element (pointed out by myself) was explained by Takahashi. Reiner felt that the article John Todd and myself wrote on integral matrices of finite order (in 1939, with the war to start any moment and us in London) was a pioneering contribution to integral representations. In his later article on this subject he included a long bibliography.

Now I will show some of my other results. Matrices are mathematical objects which by their own nature are connected with noncommutativity. I am now returning to C. C. MacDuffee, whom I had met in 1935 and whose work had a great influence on me. First of all, I learned from him that Poincaré had introduced a connection between ideals and integral matrices. But this was not taken up very much. At some meeting I met Latimer, who also sent reprints. I observed that the two sets had a common element, a joint paper. This paper is not mentioned in Deuring's book *Algebren*, although I feel that both authors, or at least one of them, would have included it in Emmy's parcel. This is one on which I have spent much time and which has definitely become quite popular. I started this with a paper entitled "On a theorem of Latimer and MacDuffee." The reason why Emmy, and perhaps also Deuring, ignored this paper is that it deals with matrices. While algebraists use matrix algebras they tend to look down on matrices. In my early days I did the same. I now applied the work to the ring of integers $\mathcal{O}$ in an algebraic number field F, assuming it to be of the form $Z[\alpha]$, α assumed the zero of an irreducible monic polynomial $f(x)$ of degree n. The theorem concerns all integral $n \times n$ matrices A for which $f(A)$ is the zero matrix and their division into classes $\{S^{-1}AS\}$ under unimodular integral similarity S. It can be shown that there is a 1-1 correspondence between these matrix classes and the ideal classes in $\mathcal{O}$. Hence the number of matrix classes is finite. The work of Latimer and MacDuffee which is applied to algebras is much more complicated, and MacDuffee's papers are much more complicated for the same reason. I then found an independent proof. I spent extra effort on this since I encountered only people (some of high standards) who thought that there was only one class, i.e., integral matrix roots of $f(x)$ were unimodularly similar. (However, Zassenhaus has done related work on integral representations.) While Latimer and MacDuffee let it go at that, I built up a theory related to this theorem which is much cited and applied. The theorem was even generalized to abstract rings (see D. Estes and R. Guralnick), and Barry Mazur gave me a more modern proof.

I showed that the principal ideal class corresponds to the class of the companion matrix, the inverse ideal class to the class of the transposed matrix.

(A. Fröhlich, in his 1983 *Ergebnisse* book, has a generalization of the latter fact.) On the other hand a matrix is similar to its transpose. This is elaborated in my 1966 *Annalen* paper. Let

$$S^{-1}AS = A'$$

A with irreducible characteristic polynomial. Then S is symmetric and can be expressed as

$$S = (\operatorname{trace} \lambda\alpha_i\alpha_k)$$

where $\lambda \in Q(\alpha)$, where α is a characteristic value of A with characteristic vector $\alpha_1, \ldots, \alpha_n$. The paper contains further results. More generally, since the matrices which enter all classes are all zeros of the same polynomial they must all be similar, but not via unimodular matrices, in general. I connected this question with another concept of MacDuffee, not in the same context. This concerns "Ideal Matrices." I will return to this after discussion of three other items:

(1) I investigated matrix classes which contain symmetric matrices. (This is in connection with D. K. Faddeev's and also E. Bender's work on polynomials with symmetric matrix roots.)

(2) If the maximal order is not generated by a single element, then one can replace the matrix classes by classes of integral representations of the maximal order under unimodular similarity.

(3) When studying matrices one rarely bothers about the numbers which turn up inside the matrix, with the exception of the companion matrix. However, Ochoa in Madrid, Spain, did bother and he found that under circumstances (studied by Rehm) sparse matrices of the following type can occur in a matrix class

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ & \cdots & & \cdots & & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ b_1 & 0 & 0 & \cdots & 0 & b_2 \end{bmatrix}$$

I now return to the concept of ideal matrix, again for ideals in the maximal order and quite complicated in MacDuffee's work. I begin with the definition.

Let $\mathcal{O}$ have the basis $\omega_1, \ldots, \omega_n$ and let $\alpha_1, \ldots, \alpha_n$ be the basis of an ideal in $\mathcal{O}$ and A an integral matrix for which

$$A \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

Then A is called an ideal matrix with respect to the bases chosen. If the bases are altered then A is replaced by UAV where U, V are unimodular. Since A can be transformed into Smith normal form by U's and V's it tells much about the ideal. My paper "Ideal Matrices I" explains how the 'quotient' of

two ideal matrices leads to a similarity between different matrix classes. I have by now written four papers on ideal matrices. However, MacDuffee's ideals did more for me. For he showed that mapping the elements of an ideal in the maximal order into the ring $Z^{n\times n}$ (assuming the underlying field of degree n), a principal ideal ring, the ideal matrix turns up as gcrd or gcld of the respective maps.

This led to a paper[2] in which I was able to show that principal or nonprincipal can be replaced by commutativity or noncommutativity. The fact that $Z^{n\times n}$ is a euclidean ring and that there is a procedure for finding gcrd or gcld by computation is of help for numerical work here.

There is a book by C. Chevalley where he studied a more general situation. He assumed his matrices to have entries from a field k, commutative or not, and showed that the arithmetic can be brought down to arithmetic in k. This leads to the study of ideals in the matrix algebra. He points out that the case of k commutative was treated also by V. Korinek.

My work on ideal matrices was picked up by others, the first one by a student of Don Lewis at Ann Arbor, Michigan, Burgie Wagner, in "Ideal matrices and ideal vectors," later by S. K. Bhandari and V. C. Nanda, in "Ideal matrices for relative extensions" and S. K. Bhandari, in "Ideal matrices for Dedekind domains."

In particular they had studied my paper "Integral Matrices II," in which I tried to find information on the ideal matrix for the product of two ideals in the maximal order, in terms of the ideal matrices of the factors. Well, it is not just the product! A factor U, a certain unimodular matrix has to be inserted between A and B. In India they introduced the concept of the "AUB Theorem."

My contribution to integral matrices started to grow steadily after I entered Caltech in 1957. So when I was asked to give a one-hour lecture at an AMS meeting I felt ready to give a lecture entitled "Integral Matrices."

Among my papers on integral matrices I want to point out some subsets.

(α) The first subset is motivated by a theorem for fields.

While any square matrix with elements in a field k can be expressed as the product of two symmetric ones, with elements in k, this is not always true for integral elements, although one factor, say the first one, can be expressed this way.

The question arose: when can both factors be expressed over Z? In a paper dedicated to C. L. Siegel's 70th birthday, by invitation from *Acta Arithmetica*, I solved this for $n = 2$ and received an appreciative letter from Siegel, who was a student of Frobenius and quite devoted to matrix theory. I wrote another paper on this subject, this one at the suggestion and partial advice of my former student E. Bender. This particular problem has led to interesting details.

[2]This paper has slight inaccuracies in the presentation.

Let $A = (a_{ik})$ be the matrix to be represented. Then associate with it the quadratic form

$$a_{12}x^2 + (a_{22} - a_{11})xy - a_{21}y^2 \tag{1}$$

However, for the problem considered a second quadratic form turns up. It was shown that it is the square of the first one. They both have as discriminant the discriminant of the matrix A.

It can then be shown that the second form is in a form class whose order is a divisor of 2. This implies that the matrix A has to be in a matrix class whose order is 1, 2, 4. In addition there are some exceptional form classes involved. The first example of this was given by D. Estes and H. Kisilevsky. van der Waerden, who had heard me lecture about this, stated that it would be congruent to (1). But later he told me in two letters that it was the negative square of the first one. His paper received a fairly long review in *Mathematical Reviews* and Cassels from Cambridge, England, asked me to send him a copy of these lectures; they were not yet published, but bound as reports. He said: "but this is Gauss' duplication of a quadratic form," and then he added, "but it is rather weird."

My further work includes three papers with titles:

"Norms from quadratic fields and their relations to noncommuting 2×2 matrices."

(β) Paper II has the subtitle "The principal genus"; Paper III has the subtitle "A link between the 4-rank of the ideal class groups in $Q(\sqrt{m})$ and in $Q(\sqrt{-m})$".

(γ) Let A, B be noncommuting 2×2 integral matrices, with at least one of them, say A, with eigenvalues in $Q(\sqrt{m})$, but not in Q. Then

$$\det(AB - BA) = -\text{norm}\,\lambda,\ \lambda \in Q(\sqrt{m})$$

If both matrices have eigenvalues not in Q, then this can lead to an intersection of norms from two different quadratic fields.

This last theorem was studied by several people and Zassenhaus reproved and elaborated it via cyclic algebras in 1977.

(δ) Another result is:

> Let A be a 2×2 integral matrix with eigenvalues in $Q(\sqrt{m})$, m not a square. Let $XAX^{-1} = A'$ where $'$ denotes transpose. Then $-\det X = \text{norm}\,\lambda, \lambda \in Q(\sqrt{m})$.

This is proved in my paper "Ideal matrices 1." Dennis Estes studied (α), (γ), and (δ) via Galois cohomology and a generalized Latimer and MacDuffee correspondence. In connection with my paper "Ideal Matrices III" an application to Galois modules and group matrices was made in the case where the field is normal, with a normal basis also for the integers and even the ideal is to have a normal basis. (The last two conditions are not always satisfied, of course.)

The 1982 Dekker book edited by me contains a review and elaboration of some of the items mentioned here.

There is also a paper from 1979 "A diophantine problem arising out of similarity classes of integral matrices" which was generalized by R. Guralnick in a much-appreciated paper in *J. Number Theory.*

I want to close with mentioning two later papers:

"Some noncommutative methods in algebraic number theory," a paper connected with my 1982 lecture at the symposium honoring Emmy Noether's 100th birthday. It has many references. It also uses central polynomials and is attached to Noether's work on the principal genus.

"Composition of binary integral quadratic forms via integral 2×2 matrices and composition of matrix classes." [Equation (16) in this paper is misleading, but it is explained by the footnote and the equations that follow.] While composition of binary quadratic forms was introduced by Gauss, the matrix approach can be generalized to all dimensions. (This will be mentioned again under problems.)

Integral Matrices before 1940

E. Artin, Zur Arithmetik hyperkomplexer Zahlen, *Abh. Math. Sem. Hamburg* **5** (1928), 261–289.

C. Chevalley, *L'-arithmétique dans les algèbres de matrices*, ASI **323**, (1936), Hermann, Paris.

V. Korinek, Une remarque concernant l'arithmétique des nombres hypercomplexes, *Mém. Soc. Roy. Sci. Bohême* (1931) NR 4, 1–8.

H. Poincaré, Sur un mode nouveau de représentation géométriques des formes quadratiques définies ou indéfinies, *J. École Polytech. Cah.* **47** (1880) 177–245.

Specially relevant

(apart from items mentioned inside the section)

E. Bender, Classes of matrices and quadratic fields, *Linear Algebra and Appl.* **1** (1968) 195–201.

A. Buccino, Matrix classes and ideal classes. *Illinois J. Math.* **13** (1969) 188–191. (He bases his work on a general integral domain.)

D. Maurer, Invariants of the trace-form of a number field, *Linear and Multilinear Algebra* **6** (1978/1979) 33–36.

M. Newman, Symmetric completions and products of symmetric matrices, *Trans. Amer. Math. Soc.* **186** (1973) 191–210 (1974). (Generalizes Taussky's work on factoring integral matrices.)

W. Plesken and M. Pohst, On maximal finite irreducible subgroups of $GL(n, Z)$ II. The six-dimensional case, *Math. Comput.* **31** (1977) 552–573. (Uses the theorem of Latimer and MacDuffee.)

H. P. Rehm, On Ochoa's special matrices in matrix classes, *Linear Algebra and Appl.* **17** (1977) 181–188.

I. Reiner, Integral representations of cyclic groups of prime order, *Proc. Amer. Math. Soc.* **8** (1957) 142–146. (Uses the theorem of Latimer and MacDuffee.)

J.-P. Serre, L'-invariant de Witt de la forme $Tr(x^2)$, *Comment. Math. Helv.* **59** (1984) 651–676.

O. Taussky, On the similarity transformation between an integral matrix with irreducible characteristic polynomial and its transpose, *Math. Ann.* **166** (1966) 60–63.

D. I. Wallace, Conjugacy classes of hyperbolic matrices in SL(n, Z) and ideal classes in an order, *Trans. Amer. Math. Soc.* **283** (1984) 177–184. (Uses the theorem of Latimer and MacDuffee.)

W. C. Waterhouse, Scaled trace forms over number fields, *Arch. Math.* **47** (1986) 229–231.

3. Conclusion

I finish with brief, largely bibliographical, comments on three topics related to my theme and a short list of problems.

Galois modules

Here Fröhlich and his colleagues Taylor, Bushnell, Ullom, Queyrut,... are leaders. He himself wrote the 1983 Ergebnisse volume *Galois module structure in algebraic number fields.*

In his article in the 1981 Dekker book, *Emmy Noether, A tribute to her Life and Work*, he says that he will concentrate on Galois module structure. He considers her work there as ahead of her time and the developments came 40 years later. He refers to his paper in 1976, "Module conductors and module resolvents." I feel flattered to notice that he refers to a 1956 paper by M. Newman and myself (discussed in chapter 2) and to a much-cited paper by Leopoldt from 1959. As I pointed out earlier, our problem is now settled for all groups. The Durham 1977 *Proceedings* are heavily loaded with relevant material. In his 1976 lecture at the Kyoto number theory conference in honor of Takagi he speaks about Hermitian Galois module structure.

Galois algebras seem to have been introduced by Hasse in 1948. The 1981 thesis of J. Brinkhuis, written under supervision by Fröhlich, refers to this reference. Fröhlich himself has a paper on this and so has Maurer, a paper entitled "... Stickelberger's criterion on Galois algebras and tame ramifications in algebraic number fields."

The use of quaternions

A number of results are mentioned here:

(1) Venkov, B. On the arithmetic of quaternions (Russian): H. P. Rehm makes use of this paper to give a proof of a famous theorem of Gauss concerning the number of representations of an integer $n > 1, \equiv 1, 2(4)$ as a sum of three squares.

(2) The 1981 Caltech thesis of P. Hanlon studies Rehm's work and finds an application of quaternions to the study of imaginary quadratic ring class groups.

(3) A paper by T. R. Shemanske on ternary quadratic forms and the class number of imaginary quadratic fields.

Use of central polynomials

The concept of central polynomials over a field was suggested by Kaplansky, *Amer. Math. Monthly* **77** (1970). Central polynomials were then constructed by E. Formanek, *J. Alg.* **23** (1972) and by Y. P. Razmyslov, *Transl. USSR Izv.* **7** (1973).

The Formanek version was used in O. Taussky, From cyclic algebras of quadratic fields to central polynomials, *J. Austral. Math. Soc.* **28** and Some noncommutative methods in algebraic number theory, *Proc. of Symp. in Honor of Emmy Noether's* 100*th birthday*.

Problems

Problem I. In the section on Integral Matrices I report mainly on the 2×2 case—however, in my paper on composition of quadratic forms I include the $n \times n$ case. Gauss did not have matrix theory, hence his work on quadratic forms had to stop there. In my paper "From cyclic algebras of quadratic fields to central polynomials" I also study $n > 2$. Although my papers on Ideal Matrices and the Latimer and MacDuffee theorem contain results for $n \geq 2$, my work on factoring an integral 2×2 matrix into the product of two symmetric integral factors has not been generalized so far. Hence I pose this as a problem.

Problem II. In the 1964 Caltech thesis of my student L. L. Foster, the following special case of a problem was studied leading to diophantine problems and other interesting observations:

Given two integral $n \times n$ matrices A, B (may be depending on parameters), in what fields can the eigenvalues of A, B lie (for special values of the parameters)? See *Pac. J. Math.* **18** (1966), 97–110.

Problem III. My work on $\det(AB - BA)$ for A, B integral 2×2 matrices, both with irrational eigenvalues in $Q(\sqrt{m})$, resp. $Q(\sqrt{n})$ leads to a noncommutative statement for the intersection of elements in these fields which are norms. I suggest more work on this.