The Riemann hypothesis in characteristic p, its origin and development

Part 3. The elliptic case.

Peter Roquette (Heidelberg)

Version of Sep 18, 2006

Abstract

We report on the gradual evolvement and the structure of Hasse's second proof of the Riemann hypothesis for elliptic curves over finite fields. The main feature of this proof is the rebuilding of the theory of complex multiplication by purely algebraic means, thereby making it available for curves over fields of arbitrary characteristic $p \geq 0$. We also report on Deuring's subsequent work on the structure of endomorphism rings of elliptic curves in characteristic p, including the supersingular case. Our sources are not only the published papers but also other documents like letters, manuscripts and lecture notes which we have found in several archives. The article is written such that it can be read independently of Parts 1 and 2 of the same series.

Contents

1 Introduction

This is the third part of a larger work on the history of the Riemann hypothesis for function fields, the fourth and fifth part will follow later. Parts 1 and 2 have appeared in [Roq02] and [Roq04].

In Part 2 we had reported on how Hasse had been motivated by Davenport and Mordell to work on the problem of counting the number of polynomial congruences. When Hasse visited Hamburg in November 1932 he had a conversation with Artin who pointed out to him that this problem is closely connected, and in some sense equivalent, to the Riemann hypothesis for function fields. Four months later, in March 1933, Hasse succeeded with a proof of the Riemann hypothesis[1] in the elliptic case. As described in Part 2, his first proof used a lifting procedure, lifting an elliptic curve over a finite base field to an elliptic curve in characteristic 0 with complex multiplication, and then applying class field theory. That proof, however, was never fully published since, in the process of writing down the proof, it became clear to Hasse that one could work directly in characteristic p, without using the detour via characteristic 0.

In this Part 3 we shall report on Hasse's new proof, its structure and its gradual evolvement. Our report covers approximately the years 1933-1943, and it includes the subsequent work of other mathematicians during that time period, notably that of Deuring.

Because of lack of sufficient time *we have decided to restrict this report to the elliptic case*, leaving the discussion of the Riemann hypothesis for function fields of higher genus to the next parts.

As with Parts 1 and 2, we have written this Part 3 in such a way that it can be read independently.

Remark: In the preparation of this paper we have used not only published material but also the information contained in personal documents like letters, manuscripts etc. All those documents which we cite are contained in the *Handschriftenabteilung* of Göttingen University Library, except when we explicitly mention another source. As a general rule, letters which were addressed to Hasse can be found in Göttingen, whereas letters which Hasse wrote to other people are preserved at other places (if preserved at all). Letters from Hasse to Mordell we have found in the archives of King's College, and those from Hasse to Davenport at Trinity College, both in Cambridge, England.

Although quite a number of letters from the Hasse correspondence is preserved, the reader should be aware that, on the other hand, quite another number of letters seems to be lost. What we have found does not constitute a complete set of the Hasse correspondence.

Acknowledgements: We are grateful to Günther Frei for a number of valuable discussions and comments. Patrick Morton has carefully and critically read the manuscript and been of help to streamline our English.

[1] Here and in the following, when we talk about the "Riemann hypothesis", we always mean the Riemann hypothesis for function fields over a finite base field.

1.1 The Hamburg Lectures

In January 1934 Artin had heard about Hasse's new proof of the Riemann hypothesis for elliptic function fields, and he invited Hasse for a series of talks in Hamburg, in order for Hasse to explain his new ideas. Let us cite from Artin's letter, dated January 17, 1934:[2]

> Lieber Herr Hasse! Hätten Sie Lust in diesem Semester zu uns zu Gastvorträgen zu kommen? Sie könnten sprechen worüber Sie Lust haben. Vielleicht die schönen Ergebnisse über die Riemannsche Vermutung? Sie sind doch das schönste, was seit Jahrzehnten gemacht worden ist. Meine Hörer würde das sehr interessieren ... Es wäre nett wenn Sie sich auf eine Woche frei machen könnten aber zur Not sind wir mit weniger auch zufrieden. In Erwartung Ihrer Zustimmung mit vielen herzlichen Grüssen von Haus zu Haus: Ihr Artin.
>
> *Dear Mr. Hasse! Would you like to visit us in this semester for colloquium talks? You may talk about what you like. Perhaps the beautiful results on the Riemann hypothesis? These are the most beautiful things which have been done during the past decades. My audience would be very much interested ... It would be nice if you could come for a whole week but if necessary we would settle with less. Looking forward to your positive reply I am with many kind regards: your Artin.*

This letter puts into evidence that Artin continued to be quite interested in the problem of the Riemann hypothesis for function fields, which he had started in his 1921 thesis but had never touched in his later publications.

Hasse accepted the invitation, and in February 1934 he delivered four 2-hour lectures in Hamburg.

The "audience" which Artin had in mind were probably the members of his seminar. But the lectures were announced as public, and certainly there were other people too attending Hasse's lectures. Very likely the following persons were present:

- *Max Zorn.* He had obtained his Ph.D. in 1930 with Artin who considered him as one of his most brilliant students. Thereafter he got a position at the University of Halle as an assistant to H. Brandt, the successor of Hasse there. In 1932 he had quit his position and moved to Hamburg again. 1933 there appeared his paper in the *Hamburger Abhandlungen* showing that the thesis [Hey29] of Käte Hey (the first Ph.D. student of Artin) could be interpreted so as to yield a proof of the Local-Global-Principle for algebras; this paper [Zor33] had received great interest among the people working in class field theory, including Emmy Noether and Hasse. In 1934 Zorn emigrated to the USA. (Today his name is known through Zorn's Lemma).

[2] Artin used to have an intense exchange of letters with Hasse. The edition of the full Artin-Hasse correspondence 1923-1934 with commentaries is in preparation and will (hopefully) soon be published, jointly with Günther Frei.

Hamburgische Universität
Allgemeines Vorlesungswesen

Auf Einladung der Mathematisch-Naturwissenschaftlichen Fakultät hält Herr

Professor Dr. Hasse

aus Marburg

am 5., 6., 8. und 9. Februar 1934, von 17-19 Uhr

im **Hörsaal des Mathematischen Seminars**, Rothenbaumchaussee 21-23

Vorträge über

„Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern".

Der Eintritt ist frei.

Figure 1: *Announcement of Hasse's Hamburg Lectures*

- *Wei-Liang Chow* who had studied in Göttingen with Emmy Noether but now planned to change to Leipzig in order to work with van der Waerden. He resided mainly in Hamburg (where he had found his later wife Margot) and, as reported by Chern [Cea96], kept close contact to Artin.[3]
- *Hans Petersson.* He had been a Ph.D. student of Hecke. Now he held a position as "Privatdozent" at Hamburg University. He had lectured on class field theory a year ago. He was a referee for the Chevalley-Weil paper [CW34] which also appeared in the *Hamburger Abhandlungen* of the current year 1934. That paper gives an important contribution to the algebraic theory of function fields; it is evident that this topic is closely connected to the program of Hasse which he presented in his Hamburg lectures.
- *Harald Nehrkorn*, a Ph.D. student of Artin of 1933 who in his thesis [Neh33] provided algebraic proofs of Artin's class number relations. In the 1935 volume of the *Hamburger Abhandlungen* he published a paper jointly with Chevalley on class field theory [CN35], going a big step towards a purely algebraic foundation of Artin's reciprocity law.
- *Heinz Söhngen*, another Ph.D. student of Artin, of 1934. His thesis [Söh35] is about complex multiplication, expanding a former paper of Hasse. (Later he went to applied mathematics.)
- *Walter Landherr*, also a Ph.D. student of Artin of 1934. His thesis [Lan35] dealt with simple Lie rings over $\mathfrak{p}$-adic fields.

[3] Chern himself was probably not present at Hasse's lectures; according to his own testimony he came to Hamburg in October 1934.

- *Hans Zassenhaus*, still another Ph.D. student of Artin of 1934, working in group theory. Even before he received his Ph.D. degree, his name became known through his explicit proof [Zas34] of the Jordan-Hölder-Schreier theorem in group theory (the butterfly-lemma). From the beginning of his mathematical career he was very active in group theory; from the years 1934 to 1938 we have counted 7 published important papers, including his text book [Zas37] which for a long time was considered "the" classical introduction to group theory.
- *Erich Kähler*, a former Ph.D. of Blaschke, who had done his *Habilitation* in 1929, the same year as Hans Petersson. His interest was mainly with differential geometry.
- *Erich Hecke* and *Wilhelm Blaschke*, Artin's colleagues in Hamburg.[4]

This list of names, certainly not complete, shows that Hasse met a highly competent and interested audience in Hamburg.[5]

The notes of Hasse's 1934 Hamburg lectures were published in the same year in the *Hamburger Abhandlungen* [Has34a]. In these notes he expounds the main ideas of his theory of "meromorphisms" of elliptic function fields, i.e., rational mappings of the corresponding elliptic curve. And he shows that and how this leads to a proof of the Riemann hypothesis in the elliptic case.

In the introduction to his notes Hasse strongly expresses his belief that the Riemann hypothesis holds not only for elliptic fields but quite generally for arbitrary function fields over finite base fields. He says:

> Ich führe im folgenden die Theorie für den einfachsten nichttrivialen Spezialfall, nämlich den Fall der elliptischen Funktionenkörper, in großen Zügen durch, etwa ebenso, wie vor 36 Jahren Hilbert zuerst die Theorie der quadratischen Relativkörper als einfachsten Fall seiner später skizzierten allgemeinen Theorie der abelschen Relativkörper entwickelte, immer schon die Verallgemeinerung im Auge habend.
>
> *I am going to sketch the theory for the simplest non-trivial special case, i.e., the case of elliptic function fields – similarly to the way that Hilbert, 36 years ago, first developed the theory of relative quadratic fields as the simplest case of his general theory of relative abelian fields, which he outlined later, his view always being directed towards the generalization.*[6]

As reported in Part 2, one year earlier Hasse had already given a talk in Hamburg, in November 1932 , about problems on diophantine congruences which are

[4] In a letter of February 26, 1934 from Blaschke to Hasse he mentions a portrait photo of Hasse which had recently been obtained and which he had sent him. This may have been the same photo which appeared in volume 10 of the *Hamburger Abhandlungen.*

[5] In Part 1 we had stated that *Shokichi Iyanaga* was present at these Hamburg lectures of Hasse in 1934. That statement was based on an oral communication by Prof. Iyanaga. In the meantime, however, after some exchange of letters it has turned out that Iyanaga had been present at Hasse's colloquium talk in Hamburg in December 1932 but not in January 1934, when he was staying in Paris together with Claude Chevalley. I have corrected my former statement in Part 2 (page 33) already.

[6] Hasse refers to Hilbert's papers [Hil99] and [Hil02]. See also Hasse's comments to Hilbert's papers on algebraic number theory [Has32].

closely connected to the Riemann hypothesis. At that time he did not yet fully believe in the general validity of the Riemann hypothesis for arbitrary function fields. It is quite remarkable that now, one year later, he is entirely convinced.[7] Hasse explains that his proof is based on the algebraic theory of function fields as developed by F. K. Schmidt [Sch31] which in turn, as Hasse points out, was modeled after the ideas of Hensel-Landsberg [HL02]. He says about this method:

> . . . Methode, an deren Verallgemeinerungsfähigkeit der Kenner der algebraischen Funktionentheorie und insbesondere des algebraischen Gerüsts der Theorie der Abelschen Funktionen nicht zweifeln wird.
>
> *. . . method, whose capability for generalization will not be doubted by anyone who is familiar with the algebraic theory of functions and in particular with the algebraic framework of the theory of abelian functions.*

Hasse's belief into the general validity of the Riemann hypothesis was strengthened in his discussions with Artin. We conclude this from a letter of Hasse to his friend Davenport dated February 12, 1934, shortly after his return from Hamburg. In this letter Hasse reports about his visit to Hamburg and his further plans. We read:

> *Hamburg was a complete success from every point of view . . . From what Artin and I found when considering the possibilities of generalisation to higher genus, it becomes only a matter of patience to do this. The general line is fully obvious now. The addition theorem is generalisable in a purely algebraic form . . . I am going to carry through all the details without bothering about any more special cases now.*

As it turned out, it required more than patience before the Riemann hypothesis could be proved for function fields of higher genus. But we see here Hasse's optimism, and at the same time his aim: Namely to develop the theory of the Jacobian in a purely algebraic manner, i.e., without lift to characteristic 0 and referring to the analytic theory there, as he had done in his first proof for the elliptic case. When he says that he will not bother any more about special cases, then he refers to his joint paper with Davenport [DH34] where they treated the special case of what today are called the "Davenport-Hasse" fields, which are generated by the generalized Fermat equation $ax^m + by^n = c$ (or similar equations) over a finite field.[8]

Hasse's lecture series in February 1934 was perhaps one of the last major events in the great history of the Mathematics Seminar of Hamburg, the last before the Seminar too was finally hit by the disastrous policy of the Nazi government in Germany. From its foundation in 1920 it had been possible to attract mathematicians of high standing to Hamburg University. In those years the Mathematical Seminar in Hamburg had gained recognition world wide. And when in 1933 the Göttingen mathematical scene was destroyed due to political

[7] He was already convinced on April 28, 1933 when he submitted his preliminary announcement to the *Göttinger Nachrichten* [Has33a]. See Part 2, section 5.4.

[8] We shall discuss that paper in Part 4.

events, then it seemed for a short while that Hamburg could take over the former role of Göttingen in the mathematical world. In this sense, Chern says in [Cea96]:

> *The decline of Göttingen had the effect of elevating Hamburg to a leading mathematical center in Germany. . . The leading attraction was Emil Artin, the young professor who gave excellent lectures and whose interest extended over all areas of mathematics.*

But it is well known that Hamburg too was soon affected by the Nazi politics, although perhaps not as severe as it had hurt Göttingen. And Artin emigrated to the USA in 1937.[9] (Chern had left for Paris in 1936.)

Let us close this section with a citation from a letter, dated December 1, 1934, which Hermann Weyl wrote to Hasse. Weyl had moved from Göttingen to Princeton[10] in 1933 and Hasse had become his successor (not without encouragement by Weyl himself). From the correspondence Hasse – Weyl we conclude that Weyl remained interested in the development of the mathematical scene in Göttingen, and he appreciated that Hasse reported to him about it. In one of those reports, it seems, Hasse had sent him a reprint of his Hamburg lecture notes [Has34a], and he commented this as follows:

> Ihre Hamburger Vorträge über komplexe Multiplikation habe ich noch nicht ganz verstanden, aber doch genug, um fühlen zu können, wie wichtig es ist, dass Sie in dieser fruchtbaren Richtung weiterarbeiten.
>
> *I have not yet fully understood your Hamburg lectures on complex multiplication, but sufficiently well in order to feel how important it is that you continue to work in this seminal direction . . .*

1.2 Our sources

Hasse's Hamburg lecture notes contain only a sketch of his new proof of the Riemann hypothesis in the elliptic case. He admits that he had not yet been able to fill in all details. In the following years he simplified and streamlined his ideas. He published an updated announcement in November 1935 in the *Göttinger Nachrichten* and in the same month he submitted his final proof with all details to *Crelle's Journal* where it appeared 1936 in volume 175, divided into three parts I, II, III.

Although Hasse's orginal motivation was the proof of the Riemann hypothesis, in the course of his work there emerged a broader project: He wished to establish a solid basis for the theory of elliptic function fields, in particular those with finite base fields. The endomorphism ring of those function fields should be fully understood, in particular the arithmetic properties of the Frobenius endomorphism. And all this with an eye on possible generalization to higher genus.

[9] Wußing has described the circumstances of Artin's leaving Hamburg. See his forthcoming article in the *Festschrift* in honour of M. Folkerts which is scheduled to appear in spring 2007.

[10] On Weyl's departure from Göttingen see, e.g., [FS92].

The foundation which Hasse could build upon was quite narrow. As we have reported in Part 1, the general arithmetic theory of function fields had been developed in the 1920s mainly by Artin, Emmy Noether and F. K. Schmidt, the latter adding the Riemann-Roch theorem as well as the analytic theory of the zeta functions. However, large parts of the theory were still lacking, parts we are familiar with today. For instance, the theory of differentials and the residue theorem had to be established also for characteristic p. Same for the ramification theory of cyclic extensions, in particular those of degree p or p-power, using the Artin-Schreier theory. And class field theory, and more. Thus when we observe the activities of Hasse and his collaborators after 1934, they were busy investigating the theory of function fields of characteristic p at large, not narrowly confined to the Riemann hypothesis.

This implies that we have to report also on those papers which are not exclusively aimed at the proof of the Riemann hypothesis. We shall see that many of the facts which we know and use today, regarding them as more or less evident or at least "well known", that these facts had been discovered in those years between 1933 and 1943 as part of Hasse's project. But as said above already, here we shall be content to report on those results only which have some bearing, direct or indirect, on *elliptic* fields. The project for fields of higher genus will be covered in Part 4 and beyond.

A decisive turn in the development was given in 1936 by Deuring who in a letter to Hasse started his algebraic theory of correspondences modeled after the classical paper of Hurwitz of 1886 [Hur86]. Deuring's aim was to develop methods suitable to approach the Riemann hypothesis for function fields of arbitrary genus, beyond the elliptic case. Hasse immediately realized the potential of Deuring's approach; he reported briefly on it at the IMU conference in Oslo 1936 and helped Deuring to prepare a publication in Crelle's Journal which appeared in two parts 1937 and 1940. It was clear from the start that Deuring's methods and results would be of considerable importance – although in the end it turned out that A. Weil, who had been informed by Hasse about Deuring's ideas, was the first to be able to establish the necessary details and thus arrive at the proof of the Riemann hypothesis for curves of higher genus. These papers by Deuring will be discussed in detail in later parts.

It seems not so well known that Deuring's work contained new and important results also for the elliptic case. His ideas led to substantial simplifications and improvements of Hasse's treatment. Moreover, he started his investigations at the point where Hasse had stopped; he was able to continue Hasse's work on elliptic function fields and arrive at precise and complete results on their endomorphism rings. This was done in several papers between 1940 and 1947. When we have said above that Hasse wished to "fully understand the structure of the endomorphism rings" then we can report that Deuring, following the road opened by Hasse, succeeded in doing this.

The following overview of our sources may be useful to the reader:

1934 Hamburg lecture notes: Published in the *Hamburger Abhandlungen* [Has34a]. They contain only a sketch of Hasse's new ideas, which in several respects were still incomplete.

1934 Cyclic fields: Theory of cyclic extensions of algebraic function fields, in particular with finite base fields. Including Artin-Schreier extensions and class field theory. [Has34d]

1934 Differentials: Exposition of the formal theory of differentials of an algebraic function field, including the theorem of the residues. [Has34c]

1934 Unramified cyclic extensions: The paper [Has34b] appeared in the same volume of Crelle's Journal as the two above mentioned papers. The existence of unramified cyclic extensions of degree p of a function field of characteristic p has important consequences for the structure of the p-torsion of its divisor class group and, as a consequence, for its endomorphism ring. This paper contains the definition of what today is called the "*Hasse-invariant*" A of an elliptic function field. Later in 1936 this was generalized (jointly with Witt) to function fields of arbitrary genus; this leads to the "*Hasse-Witt matrix*" [HW36].

1935 Göttingen report: In the *Göttinger Nachrichten* [Has35] Hasse announced his full proof (second version) of the Riemann hypothesis in the elliptic case.

1935 Behrbohm: A note by H. Behrbohm, a student in Hasse's seminar, systematizing Hasse's arguments in paper (III) below, about the structure of the endomorphism ring [Beh35].

1936 Davenport: This paper [Dav36] contains a partial result towards Hasse's "norm-addition formula" as formulated and proved in paper (III) below. In fact, Hasse had been inspired to look for his norm-addition formula by this result of Davenport.

1936 Higher differentials: In his paper (I) below, Hasse had to use certain determinants of higher derivatives and differentials, and therefore he had to develop this theory to be applicable in arbitrary characteristic. The paper was published in Crelle's Journal in the same volume as (I) but preceding it. The theory was streamlined and extended in two subsequent papers by Teichmüller and F. K. Schmidt respectively, so that there are three papers in short succession on this topic:

(a) Hasse's original paper [Has36a].
(b) The exposition by Teichmüller [Tei36] appearing 1936 in the same volume 175 of Crelle's Journal as (a).
(c) A systematic generalization by F. K. Schmidt and Hasse one year later [Has37a].

It does not seem to be generally known that this universal theory of higher derivatives and differentials had been originally created for use in the proof of the Riemann hypothesis.

1936 Crelle papers: A sequence of three papers by Hasse in volume 175 of *Crelle's Journal*, submitted already in 1935, with full proofs for the elliptic case. The titles are:

(I) The structure of the torsion group. [Has36b]
(II) Meromorphisms and endomorphisms. [Has36c]
(III) Structure of endomorphism ring and Riemann hypothesis. [Has36d]

1936 Oslo lecture: Hasse's text of an invited lecture at the International Congress of Mathematicians in Oslo [Has37b] .

1937/40 Deuring's Theory of Correspondences: This brought about a decisive turn in the direction of research towards the Riemann hypothesis for function fields of arbitrary genus. [Deu37], [Deu40]. Here we shall discuss those results only which are relevant for the elliptic case.

1941 Endomorphism rings: Deuring had determined all possible domains which can appear as endomorphism rings of elliptic function fields, in particular the non-commutative ones [Deu41a]. This important paper appeared in the *Hamburger Abhandlungen.* In connection with this paper Deuring published three other papers:

1941 Normal forms: Deuring discussed normal forms and absolute invariants of elliptic fields, for all characteristics including $p = 2$ and $p = 3$ [Deu41b]. He needed this in his 1941 paper on endomorphism rings.

1942 Good reduction: On several occasions in the work of Hasse and Deuring, there appeared a situation which today we would call "good reduction" of algebraic function fields or curves. In his paper [Deu42] Deuring developed a coherent general theory of good reduction which covered all special cases which were encountered so far. Although this paper appeared one year later than the 1941 paper on endomorphism rings, it was completed earlier, and Deuring used it in an essential way in his study on endomorphism rings.

1943 Miscellaneous: Deuring's paper [Deu47] collects some facts on elliptic function fields which he had observed in the preparation of his 1941 paper on endomorphism rings.[11]

Occasionally we shall cite those papers with their names shown above in boldface, instead of their bibliographical code [. . .].

In addition to the above we shall use several other documents: manuscripts, papers and also letters, in particular the letters from the correspondence of Hasse with his friend Davenport. Also from the correspondence of Hasse with Deuring, F. K. Schmidt, A. Weil, Lefschetz. These documents, which will be cited in due course, allow us to have a glimpse on the gradual rise of ideas and visions before they were condensed into a publication – an invaluable asset for those who are interested in the history aspect of mathematics.

Remark: All the cited letters are contained in the *Handschriftenabteilung* of the Göttingen University (Cod. Ms. H. Hasse), except if explicitly stated otherwise. The letters from Hasse to Davenport are contained in the archives of Trinity College, Cambridge.

1.3 The task

For Hasse, a "function field" $F|K$ was a finitely generated field extension of transcendence degree 1, such that K is algebraically closed in F. He assumed that the base field K is perfect but in fact all his arguments work under the

[11] This paper is often cited as having appeared in 1947. But in fact it had appeared in 1943 already. However, due to difficulties in war time and the years afterwards, the full volume of *Hamburger Abhandlungen*, consisting of several fascicles, could be completed in 1947 only and this is the reason for the late official date for [Deu47].

weaker assumption that $F|K$ is conservative which means that the genus of $F|K$ is preserved under extension of the base field K.[12] The genus g of $F|K$ is defined algebraically, according to the well known paper by F. K. Schmidt 1931. (See [Sch31]. We have discussed this paper in section 5 of Part 1.)

Hasse defines $F|K$ to be *elliptic* if $g = 1$, with the additional condition that there exists a prime divisor P of degree 1. This additional condition is trivially satisfied if K is algebraically closed. Hasse knew that it is also satisfied if the base field K is finite, due to "F. K. Schmidt's theorem".[13]

The Riemann hypothesis is concerned with function fields $F|K$ over a finite base field K. The zeta function of $F|K$ is defined due to F. K. Schmidt [Sch31] as follows:

$$\zeta(s) = \prod_P \frac{1}{1 - \frac{1}{|P|^s}} = \sum_A \frac{1}{|A|^s}$$

where P ranges over the prime divisors of $F|K$ and $|P|$ is the order of the residue field modulo P, and where A ranges over the integral divisors with $|A|$ being defined by linearity. s denotes a complex variable. Introducing the new variable $t = q^{-s}$ (where $q = |K|$ is the order of the base field) it turns out that $\zeta(s)$ is a rational function of t of the form

$$\zeta(s) = \frac{L(t)}{(1-t)(1-qt)} \qquad\qquad (t = q^{-s})$$

where $L(t)$ is a polynomial of degree $2g$, of the form

$$L(t) = 1 - (q + 1 - N)t + \cdots + q^g t^{2g}\,.$$

Here and in the following, N denotes the number of prime divisors of degree 1 of the function field $F|K$. It is convenient to consider the reciprocal polynomial

$$L^\star(t) = t^{2g} - (q + 1 - N)t^{2g-1} + \cdots + q^g$$

The Riemann hypothesis asserts that all zeros of $\zeta(s)$ are situated on the line $Re(s) = \frac{1}{2}$ in the complex plane. This is equivalent to saying that all zeros of $L^\star(t)$ are situated on the circle $|t| = \sqrt{q}$.

In the eliptic case the polynomial $L^\star(t)$ is quadratic:

$$L^\star(t) = t^2 - (q + 1 - N)t + q = (t - \pi)(t - \overline{\pi}) \tag{1}$$

and the Riemann hypothesis asserts that the roots $\pi, \overline{\pi}$ have the same absolute value: $|\pi| = |\overline{\pi}|$. It was already well established that it would suffice to show:[14]

$$|N - q - 1| \leq 2\sqrt{q} \tag{2}$$

[12] The terminology "conservative" seems to have been coined by Artin in his Princeton lectures of 1947/48.

[13] See Part 1, section 5.2.2. Hasse knew that for $K = \mathbb{Q}$, there are function fields of genus 1 with no prime divisor of degree 1. But for some time it remained an open question whether the smallest prime divisor degree in an elliptic function field is bounded (as it is in the case of function fields of genus $g > 1$). This was settled in 1957 by Shafarevich [Sha57] who showed that such a bound does not exist for $g = 1$.

[14] See Part 1, section 6.3.

not only for the given base field with q elements but also for any base field extension.

In order to do this Hasse was going to identify the roots π, $\overline{\pi}$ of $L^\star(t)$ with elements in a certain ring M which he called the *ring of multipliers*; today it is called the *endomorphism ring*. Hasse obtained it by a purely algebraic construction from the data of the given elliptic function field $F|K$. From the structure of this ring M he was able to deduce the validity of (2).

The guiding principle for the construction of M was the analogy to the classical, analytically based theory of complex multiplication. In fact, in his first proof (which we have reported on in Part 2) Hasse directly used the classical theory, after lifting the given function field to a suitable function field in characteristic zero which admits complex multiplication. But now he had discovered that the somewhat cumbersome lifting process[15] can be avoided, and that the ring M can be constructed directly also in characteristic p, in complete analogy to the classical case. On November 11, 1933 he wrote to Davenport:

> *...I really think I ought to publish this new proof and not my old analytical one, particularly with regard to the fact that the new proof is nothing else than a translation of every step (really every!) of my old proof into algebraic language.*

We see that Hasse set out to transfer the analytically based theory of complex multiplication into his algebraic framework.

One of the driving forces in the development of Mathematics[16] is the use of *analogies*. If a problem refers to a situation which is seen to be quite analoguous to another situation which has been studied already, then it makes sense to try to use the concepts and methods which had been developed in that other situation – possibly with some changes adapting to the new situation. For Hasse and his contemporaries (including Artin in his thesis [Art24a], [Art24b]) the analogue to the notion of "function field" was "number field". Accordingly, the theory of function fields was modeled quite in analogy to the theory of number fields, with the notions of prime divisor, divisor class, class number etc. being prominent. Today this analogy has been formalized through the notion of "global field" defined by the Artin-Whaples axioms [AW45]; this notion comprises both types of fields, number fields as well as function fields over finite base fields.

On the other hand, the people working on function fields at that time were quite aware of the fact that there was another analogy which could profitably be used in the theory of function fields, namely the analogy to the theory of complex valued meromorphic functions on compact *Riemann surfaces*. This was first put into evidence in the classical paper by Dedekind and Weber [DW82],

[15] The lifting process was regarded as "cumbersome" from the level of knowledge in the 1930s. Later, after Deuring had developed the systematic theory of "good reduction", the lifting process became quite straightforward and natural. Perhaps Hasse would not have started to establish complex multiplication in characteristic p if he would have had Deuring's theory already available. On the other hand, Deuring had developed his theory of good reduction in order to simplify Hasse's lifting method, which then served him to algebraize the classical theory of complex multiplication in characteristic 0, including the relevant theorems of class field theory.

[16] And not only of Mathematics.

and further exploited heavily in F. K. Schmidt's paper [Sch31]. Much of the work of Hasse on elliptic function fields (and on function fields of higher genus too) is motivated by the attempt to exploit this second analogy, in order to arrive at a theory of "complex multiplication" which, on the one hand, is modeled after the analogy with the complex analytic case, but on the other hand fits into the framework of abstract algebra and hence is suitable for the investigation of the Riemann hypothesis in characteristic p.

There is a third analogy, namely the *geometric* viewpoint. In fact, the geometric language has now penetrated large areas of algebra and arithmetic; the reason for this can perhaps be seen in its great flexibility and adaptability to various situations. In this setup a "function field" $F|K$ is considered as the field of rational functions on an algebraic curve Γ defined over K. Notation: $F = K(\Gamma)$. Instead of prime divisors P which belong to the valuations of the function field, it is common to talk about points of the respective curve Γ. In this connection the curve Γ is assumed to be smooth, so that indeed the local rings of its points are valuation rings.

In today's abstract algebraic geometry two biregularly equivalent algebraic curves are usually considered to be isomorphic, and accordingly they are identified if feasible. In this sense the conservative function fields $F|K$ are in bijective correspondence to the complete smooth irreducible curves Γ defined over K, such that $F = K(\Gamma)$. Thus from today's viewpoint there is no essential difference between the arithmetic-analytic analogies in Hasse's time, and the geometric analogy in our time.

For Hasse and his contemporaries, however, the situation was different. At that time the modern "geometric" viewpoint was not yet sufficiently established. For instance, the curves defined by the equations $y^2 = x^3 - 1$ and $y^2 = x^4 - x$ were considered as two *different* elliptic curves which can be transformed into each other by birational transformations – whereas today, within the algebraic framework we would regard these equations as two possibilities to explicitly generate the *same* abstract curve. It is true that Hasse in his proofs had occasionally to use a suitable generation of the function field in question, i.e., he had to work with curves given explicitly by equations, and to manipulate with the coordinates of the points of these curves. But in every such case he did not hesitate to express his *dislike* of such procedure on the ground that it would be desirable to find another proof which works with abstract notions. He used the terminology "invariant" notions by which he meant birationally invariant. Such proof would be, in his view, more adequate and lucid.[17]

As we can see from the Hasse-Noether correspondence [LR06], it was largely the contact with Emmy Noether which had induced Hasse to accept and prefer the abstract algebraic view point.

It is well known that in Hasse's time there were already strong attempts, by Emmy Noether, van der Waerden and others, to put Algebraic Geometry on a strictly algebraic footing in the sense of "Modern Algebra" as understood at the

[17] To avoid misunderstandings we would like to point out that, of course, the connection between algebraic geometry and the theory of function fields had been observed much earlier already. (Compare, e.g., [Fre06] where Gauss' work in this direction is discussed.) What Hasse wished to establish, and is generally accepted today, is an *invariant* framework of geometric notions.

time. But these attempts were not yet pushed far enough to be of conceptual help in the proof of the Riemann hypothesis, mainly because the latter required base fields of characteristic $p > 0$ which were outside the realm of classical algebraic geometry. In fact, Hasse's work on the algebraic theory of function fields contributed essentially to the development of the abstract foundation of algebraic geometry.

At the time of his Hamburg lecture, i.e., in 1934, Hasse probably did not yet know about the relevant developments of the Italian school of algebraic geometry, which could have led him to exploit the analogies to algebraic geometry for his project. Instead he relied on the analogies to number fields on the one hand, and to the analytic theory of complex multiplication on the other hand. It was only gradually that Hasse became aware of the fact that the results of the Italian school could be of use if suitably algebraized. As far as we can deduce this from the Hasse correspondence, this began through letters from Emmy Noether, O. F. G. Schilling, A. Weil and S. Lefschetz in the years 1934-36. Later, Hasse was actively seeking contact to Italian geometers in order to get more information. But this was part of Hasse's attempts to approach the Riemann hypothesis for higher genus; we shall report on this in more detail in Part 5.

Nevertheless, in the following discussion we shall freely use today's geometrical terminology whenever we believe that, up to the notations and terminology, this reflects faithfully Hasse's ideas – their origin and their gradual development.

1.4 Summary

In January 1934 Artin invited Hasse for a series of lectures in Hamburg, for he had heard that Hasse had a new proof of the Riemann hypothesis for elliptic curves over finite fields. Hasse accepted and his lecture notes were published the same year in the "Hamburger Abhandlungen". Hasse's first proof (which we have described in Part 2) had run a detour from characteristic p to characteristic 0 where he could use the analytically based classical theory of complex multiplication and its class field theory. In contrast the new second proof proceeded entirely in characteristic p and did not use complex analysis. Given an elliptic curve over a finite field, the problem was to find the solutions of the corresponding L-polynomial, which is a quadratic polynomial with integer coefficients. Hasse did not use the geometric language to which we are accustomed today; instead he used the language of function fields in analogy to number fields.

2 Algebraic uniformization

2.1 The addition of points

Hasse's abstract theory of complex multiplication refers to an elliptic function field $F|K$ whose base field K is supposed to be *algebraically closed* but otherwise arbitrary, in particular it could be of characteristic $p > 0$. It is in the very last part only that K is assumed to be the algebraic closure of a finite field $\mathbb{F}_q$ of order q, and $F|K$ to be a base field extension of an elliptic function field $F_q|\mathbb{F}_q$.

In that situation the Frobenius operator π and its conjugate $\overline{\pi}$ are introduced and studied.[18]

We may write $F = K(\Gamma)$ where Γ is an elliptic curve (always assumed to be smooth and complete). By "point" of F we mean a K-rational point of Γ except if explicitly said otherwise. (Let us repeat once again that Hasse did not use the geometric analogy. Although he sometimes used the terminology "point" he understood that, by definition, this was a prime divisor belonging to a valuation of $F|K$.)

Besides points we also consider divisors A of F which are defined as formal products of prime divisors, i.e., points. Divisor operation is written as multiplication. Divisor equivalence is understood modulo principal divisors and is denoted by $\sim$.

After fixing a point of reference P_0, the assignment $P \to \frac{P}{P_0}$ yields a bijection between the set of all points and the divisor classes of degree 0 of F; this is a consequence of the Riemann-Roch theorem for genus $g = 1$.[19]

Since the divisor classes of degree 0 form a group, this bijection defines a group operation for the points of F. Explicitly: The new operation for prime divisors, which is written as addition, is defined by the formula:

$$\frac{P+Q}{P_0} \sim \frac{P}{P_0} \cdot \frac{Q}{P_0} \,. \tag{3}$$

The zero element of this group is P_0.

In geometric language, the relation (3) establishes an isomorphism of the curve Γ with its Jacobian, after fixing a point of reference P_0. But note (again) that Hasse did not have this vocabulary at his disposal; he did not talk about the "Jacobian" of Γ but, instead, referred to the "group of divisor classes of degree 0".

There are well known explicit formulas describing the addition of points. Suppose, for instance, that the characteristic is $p > 3$, then Γ can be given by an equation in Weierstrass form:

$$\Gamma: \qquad y^2 = 4x^3 - g_2 x - g_3 \qquad \text{with} \qquad \Delta = g_2^3 - 27 g_3^2 \neq 0 \,. \tag{4}$$

As point of reference we take the point at infinity. The other points are then given by their coordinates (x, y). Now, the group operation (3) is explicitly given by the so-called *addition formula*

$$x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \tag{5}$$

$$y_3 = -\frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1) - y_1 \tag{6}$$

if $P_3 = P_1 + P_2$. (In case when one of the P_1, P_2, P_3 equals the point of reference, this formula has to be modified suitably.)

[18] For this see section 2.5.

[19] Instead of $\frac{P}{P_0}$ one could also write PP_0^{-1}. But Hasse preferred the writing $\frac{P}{P_0}$ which we wish to follow here.

Hasse's formula (3) reflects these classical addition formulas but, and this is his main point, it is formulated in an algebraically invariant fashion, without recourse to an explicit representation by coordinates. In his Crelle paper (I) we find the following statement:

> Mit Hinblick auf die Aufgabe der Verallgemeinerung der ganzen Theorie auf beliebiges Geschlecht g vermeide ich es absichtlich, soweit nur irgend möglich, spezielle explizite Formeln oder Kenntnisse für elliptische Körper auzunutzen ... Der ganze Aufbau der Theorie hat jetzt rein strukturellen Charakter.
>
> *In view of the problem to generalize the whole theory to arbitrary genus g I purposely avoid, as far as possible, using explicit formulae or presupposing any knowledge about elliptic fields... The layout of the whole theory is now of purely structural character.*

Hasse admits that in this way his proofs may look somewhat abstract for those who are interested in the elliptic case only. But he adds that the abstract formulation makes it possible to deal quite naturally with every characteristic p, including $p = 2$ and $p = 3$. In his first proof (which we had discussed in Part 2) Hasse had worked with the explicit addition formula (5) for the coordinates; accordingly he had to assume $p > 3$. This explains why now he expressly states that the characteristics 2 and 3 are included. Well, in his Hamburg notes he still had to assume $p > 2$ but in his 1935 Göttingen report [Has35] he was already able to include $p = 2$ too.

For us, such a statement as cited above seems quite obvious. But we are used today to an abstract foundation of algebraic geometry, based on commutative algebra without explicit recourse to coordinates and polynomial equations. As said above already, at Hasse's time this was not so, and Hasse had somehow to justify his "abstract" notions and proofs. We have the impression that Hasse included this "justification" as a result of his discussions with his friend Harold Davenport, for the latter was by no means convinced yet of the power and lucidity of the abstract method.

The construction of Γ as an 1-dimensional abelian variety, as given in (3), is regarded by Hasse as the abstract substitute of the classical method of *uniformization* in the case $K = \mathbb{C}$. More precisely, the abelian variety Γ is the abstract equivalent to the universal covering space $\mathbb{C}$ modulo the lattice of periods. It is true that by definition the isomorphism (3) depends on the choice of the base point P_0. But it turns out that different choices of the base point lead to essentially the same result – as it does in the classical case, where P_0 corresponds to the origin of the universal covering space.

Accordingly one of the main tasks was to clarify the group structure of Γ, or at least of the torsion part of Γ.

We can fairly well observe the process in which Hasse gradually obtained his abstract algebraic viewpoint for his new proof. In those years Hasse had an extensive correspondence with his friend Davenport, and Hasse informed him frequently about the progress of his work. In a letter to Davenport of October 6, 1933 Hasse writes, referring to an elliptic function field $F|K$ where

K is the algebraic closure of a finite field of characteristic p:[20]

> *I have proved that the automorphism group given by the addition theorem is of "dimension 2". For the "infinite finite field" (composite of all finite fields to p) it is isomorphic to the additive group of all pairs (r_1, r_2) of rational numbers, with denominator prime to p, considered mod. 1. This is entirely in accordance with what I proved analytically ... and I hope the proofs will also allow a purely algebraic treatment. I am not far enough to tell you more at present. I have, however, got the knack of it now, in particular of where complex multiplication and imaginary quadratic fields come in.*

Davenport replied a week later:

> *It will be splendid if you obtain a purely algebraic treatment of the elliptic case. What is the starting-point for your proof ... ?*

The "*automorphism group given by the addition theorem*" which Hasse mentioned is the group of translation automorphisms. Today it seems trivial that for any abelian variety, the translations are given by automorphisms of the function field. But let us repeat: At that time there was no algebraic theory of abelian or elliptic function fields of characteristic p. Earlier that year, Davenport in a letter of February 21, 1933 had asked Hasse:

> *Are you going to get new automorphisms or birational transformations from your method, or what ?*

We see that Hasse had to *discover* those automorphisms; he could not wave his hands and refer to general principles of abstract algebraic geometry. But how did he discover the translation automorphisms?

Let P be any point of $F|K$. The translation automorphism τ_P for P (or, in Hasse's words, the "*automorphism given by the addition theorem*") is defined by the property that $\tau_P X = X + P$ for all points X. In the classicial situation, when $K = \mathbb{C}$ is the complex number field, these automorphisms are obtained from uniformization, i.e., generating $F|K$ by the doubly periodic Weierstrass function $\wp(u)$ and its derivative $\wp'(u)$, and then aplying a variable substitution $u \mapsto u+t$. In the algebraic setting, without the analytically based uniformization available, Hasse constructs the translation as follows:

Consider the divisor $P_0 \cdot P$, the product of the point P_0 of reference with the given point P. Since $g = 1$, there exists a non-constant element $z \in F$ which admits $P_0 \cdot P$ as its pole divisor. The rational function field $K(z)$ depends on P but not on the choice of the element z according to the specification above. We have $[F : K(z)] = 2$. The non-trivial automorphism σ_P of $F|K(z)$ has the property that $\sigma_P X = -X + P$ for all X. Taking P_0 for P we obtain another involution σ_{P_0} with the property: $\sigma_{P_0} X = -X$. Hence the translation τ_P can be constructed as $\tau_P = \sigma_P \cdot \sigma_{P_0}$, a product of two involutions.

We see that this construction does not refer to explicit formulas like (5), (6).

[20] Hasse's letters to Davenport were usually written in English; no translation is necessary.

The map $P \mapsto \tau_P$ gives an isomorphism of the additive group Γ to the group of all translation automorphisms of $F|K$. Hasse's statement, in his letter above, about the structure of the group of translation automorphisms is in fact a statement about the structure of the group Γ, (or of the group of divisor classes of degree 0 of F which is isomorphic to Γ). In Hasse's case (in his letter to Davenport) when K is the algebraic closure of a finite field, every divisor class is of finite order. In the general case, when K is arbitrary algebraically closed (as Hasse assumes in his publications), Hasse's description holds for the torsion subgroup of Γ.

Actually, Hasse's result as stated in his above mentioned letter to Davenport, is not complete because the p-power torsion group of Γ is not covered. Hasse sent the correct statement (including proofs) one month later to Davenport, in a letter dated November 11, 1933. This correct statement is also found in the Hamburg 1934 notes. The p-power torsion group is, in Hasse's terminology, "one-dimensional" in as much as it is isomorphic to the rational numbers modulo 1 whose denominators are p-powers (not to pairs of such numbers) – except in some cases in which the p-power torsion group vanishes. Hasse was able to describe those exceptional cases explicitly by the vanishing of what today is called the "Hasse invariant" A of an elliptic curve, defined as a certain coefficient in the power series expansion of the holomorphic differential. We shall describe this result later, as well as its role in connection with the Riemann hypothesis. See section 4.

2.2 Meromorphisms and endomorphisms

As above, F denotes an elliptic function field with algebraically closed base field K. Hasse defines a "meromorphism" as a K-isomorphism μ of F into itself. Hasse writes the application of μ as a right operator; thus $F\mu$ denotes the image of F. We have $F\mu \subset F$. Such an isomorphism defines naturally a rational map $\mu : \Gamma \to \Gamma$. Hasse's terminology of "meromorphism" has not survived; today one would just talk about "a rational map of Γ into itself", more precisely: "a rational map of finite degree".

The map $\mu : \Gamma \to \Gamma$ is in some sense dual to $\mu : F \to F$ and hence it is written as left operator; thus μP denotes the image of P. In his Göttingen report Hasse says that this notation had been suggested to him by Ernst Witt (who at that time was one of his assistants in Göttingen). If the point P of Γ is regarded as a prime divisor of F and its residue map is denoted by $z \mapsto zP$ then Witt's notation implies

$$z \cdot \mu P = z\mu \cdot P \qquad \text{for} \qquad z \in F\,. \tag{7}$$

Indeed, this notation looks rather elegant, in Witt's style which we know from his other papers.

The meromorphism $\mu : F \to F$ is uniquely determined by the rational map $\mu : \Gamma \to \Gamma$. More generally: If $\mu P = \nu P$ for infinitely many points P then $\mu = \nu$ as meromorphisms of F.

Using the definition (3) we obtain

$$\mu(P + Q) + \mu P_0 = \mu P + \mu Q\,. \tag{8}$$

μ is called "normalized" if $\mu P_0 = P_0$ and thus

$$\mu(P+Q) = \mu P + \mu Q\,. \tag{9}$$

Every meromorphism of F can be normalized by multiplication with a translation automorphism. The normalized meromorphisms yield homomorphisms of the group Γ into itself. Hasse introduced the name "multiplier". Today's terminology is "endomorphism" instead of "multiplier". This makes sense as long as it is understood that the discussion is done in the category of algebraic geometry in which only those group endomorphisms are considered which are maps within this category. Hasse had chosen the name "multiplier", following the established terminology in the classical case, but this terminology has not survived.

Here we mostly prefer to use today's terminology; the reader who looks through Hasse's papers will have no difficulty to understand that a "multiplier" in his sense is what today is called "endomorphism" of an abelian variety. However, we will denote the ring of all endomorphisms of Γ by M, as Hasse does (and not by E as the name "endomorphism" would suggest).

Meromorphisms can be multiplied. The product $\mu\nu : F \to F\mu\nu$ means first applying μ and then ν as right operators on F. If μ and ν are normalized then so is $\mu\nu$. From (7) we see that the corresponding endomorphism $\mu\nu : \Gamma \to \Gamma$ means first applying ν and then μ as left operators on Γ. Thus the order of application is changed, as it should by general functional principles.

Hasse defines the "norm" of a meromorphism (or endomorphism) μ as the field degree

$$\mathcal{N}(\mu) = [F : F\mu]\,. \tag{10}$$

Today this is called the "degree" of the meromorphism, i.e., of the corresponding rational map of Γ to itself. It will turn out that $\mathcal{N}$ is the norm function on M in an imaginary quadratic field. Thus let us keep Hasse's terminology and continue to say "norm". The reader will have no difficulty to recall that this norm is the degree in the sense of algebraic geometry.

We have the product formula for the norm:

$$\mathcal{N}(\mu\nu) = \mathcal{N}(\mu)\mathcal{N}(\nu)\,. \tag{11}$$

If $F|F\mu$ is separable then, since both fields are of genus 1, it is unramified. It is an abelian extension, the Galois group being the group of translation automorphisms τ_Q belonging to those $Q \in \Gamma$ for which $\mu Q = 0$, i.e., Q is in the kernel Γ_μ of the endomorphism μ. Thus $\mathcal{N}(\mu)$ equals the order of this kernel. For brevity, μ is said to be separable if the field extension $F|F\mu$ is.

If μ is not separable then the order of Γ_μ equals the separable part $\mathcal{N}_s(\mu) = [F : F\mu]_s$ of the norm. The product formula (11) holds also for the separable part $\mathcal{N}_s$ of the norm, and also for its inseparable part $\mathcal{N}_i$.

2.3 The addition of meromorphisms

As operators on the additive group Γ, endomorphisms can also be added. However, it is not clear *a priori* that the sum $\mu_1 + \mu_2$ of two such endomorphisms come again from some meromorphism, i.e., from an isomorphism of F into itself. Hasse showed that this is indeed the case. Today we would wave this problem with the comment that by definition, the meromorphisms are algebraic maps of an algebraic group in the sense of algebraic geometry. But at the time of Hasse such an argument could not be used because the abstract algebraic geometry was not yet developed. Instead, he had to verify the above fact in the framework of the theory of function fields he was working in.

Before proceeding let us insert a remark which perhaps we should have given earlier, namely: It is convenient to consider every place $P : F \to K$ as some kind of "improper" meromorphism of F. The corresponding operator on Γ is the constant map $\Gamma \to P$. If $P = P_0$ is the place of reference then we obtain the zero map of the group Γ. (Recall that P_0 is by definition the zero element of Γ.) The inclusion of the zero map among the endomorphisms of Γ is necessary in order to consider them as a ring. In the following discussion this improper meromorphism and its corresponding zero endomorphism is included although we do not always stop to insert extra considerations even when they would be necessary formally. In every such case those extra considerations are classical, straightforward and left to the reader.

In his Hamburg 1934 notes Hasse did not give a detailed proof of the fact that meromorphisms can be added; he referred vaguely to the explicit addition formulas (5), (6). However, he said, one should look for a more elegant solution which is susceptible to generalization. He sketches such a method but adds:

> "Ich habe diesen Gedankengang aber noch nicht im einzelnen durchgeführt."
>
> "*But I have not yet followed this thread in detail.*"

In the Göttingen 1935 report Hasse gives a more detailed description of this, and full details follow in his Crelle paper (II). Let us explain the main idea:

Write $F = K(X)$ where X is a generic point of Γ over K. In addition to X, consider all F-rational points M of Γ, with the specification that M should not be K-rational, hence generic over K. Then $K(M) \subset F$ and the specialization $X \to M$ defines an isomorphism

$$F = K(X) \to F\mu = K(M) \subset F$$

i.e., a meromorphism μ. In this way the meromorphisms $\mu \neq 0$ of F are in bijective correspondence with the F-rational points M of Γ which are not K-rational. (The improper endomorphism $\mu = 0$ will correspond to the point P_0 which, however, is K-rational.)

If P is any K-rational point of Γ then the image μP can be described in terms of M as follows: Consider P as a prime divisor of F with residue map $z \to zP$ from F to K. The curve Γ, originally defined over K, is also defined over F and, as such, admits *good reduction* modulo P. Accordingly, every F-rational point M of Γ is reduced modulo P to a K-rational point $M \cdot P$ of Γ. We have

$$M \cdot P = \mu P$$

by comparing the definitions of both sides. Moreover, any F-rational divisor A of Γ admits a reduction $A \cdot P$; under this reduction map the degree of divisors is preserved and also divisor equivalence. Points which are K-rational are fixed under the reduction. Therefore, in view of (3), any relation of the form

$$M_1 + M_2 = M_3$$

yields after reduction modulo P the relation

$$M_1 \cdot P + M_2 \cdot P = M_3 \cdot P$$

which gives

$$\mu_1 P + \mu_2 P = \mu_3 P\,.$$

This is the essence of Hasse's proof[21] of the

> **Addition theorem:** *If μ_1, μ_2 are endomorphisms of the elliptic function field F then their sum $\mu_1 + \mu_2$ is also an endomorphism.*

To be sure, Hasse did not talk of "good reduction", and he did not talk about an elliptic curve and generic points etc. Instead of considering F-rational points M of the given curve Γ, Hasse considered the independent field compositum FF' of F with an K-isomorphic copy F'. Regarding FF' as an elliptic function field over F he considered prime divisors M of $FF'|F$ of degree 1. Our presentation is nothing but a "translation" of Hasse's arguments into the language of algebraic geometry.

We have to keep in mind that a theory of "good reduction" of curves was not yet in existence at that time. A systematic theory was developed by Deuring and published in 1942 only; see [Deu42]. In 1935, Hasse had to develop the necessary facts directly, in the special case under consideration.[22]

2.3.1 Abel's theorem

In a function field $F|K$ of genus g the holomorphic differentials form a K-vector space Ω of dimension g. Here, "holomorphic" means "without poles". If $F|K$ is elliptic then $g = 1$ and so Ω is of dimension 1. The meromorphisms μ of F act naturally on Ω as follows: Let $\omega \in \Omega$ and write $\omega = y\mathrm{d}x$ where $x, y \in F$ and x is a separating variable. Then $x\mu, y\mu \in F\mu \subset F$ and accordingly $\omega\mu = y\mu\,\mathrm{d}(x\mu)$ is regarded as a differential in F. It is verified that $\omega\mu$ is well defined in this way, and it is holomorphic. Hence $\omega\mu = c_\mu\omega$ with $c_\mu \in K$.

It is easy to verify that $c_{\mu\nu} = c_\mu c_\nu$. It is not so easy to show that[23]

$$c_{\mu+\nu} = c_\mu + c_\nu \tag{12}$$

[21] If $\mu_1 = 0$ or $\mu_2 = 0$ or $\mu_1 + \mu_2 = 0$ then the corresponding M_i has to be replaced by the point P_0 of reference.

[22] Note that in the first version of his proof which we had discussed in Part 2, Hasse had already to deal with a situation of good reduction, even in the more subtle case where the characteristic of the base field differs from the residue characteristic. Compare [Roq04], p.68.

[23] For the improper endomorphism one has to put formally $c_o = 0$.

which can be regarded as the algebraic analogue of *Abel's theorem* in the elliptic case. Hasse's proof in his Crelle paper (II) runs similarly as the proof of the addition theorem for meromorphisms discussed in section 2.3.

Thus $\mu \mapsto c_\mu$ yields a representation of the endomorphism ring M in the base field K. By definition, $c_\mu = 0$ if and only if μ is inseparable (or $\mu = 0$). Since K is of characteristic p it follows $c_p = 0$. Here, p stands for the endomorphism $p \cdot \mathbf{1}$, which means "multiplication with p" (in accordance with the identification $\mathbb{Z} \subset \mathsf{M}$.) From this one deduces that p as a meromorphism of F is inseparable – a fact which becomes important later when it comes to determine the p-torsion of Γ. (See section 3.4.3.)

2.4 First structure theorems

Since endomorphisms μ can be multiplied and added, they form a ring M. Hasse proceeds to investigate the structure of M. In the Hamburg 1934 notes we find the following first structure theorems.

(i) M *has no zero divisors.*
Follows from the product formula for the norms (11).

(ii) M *admits an identity* $\mathbf{1}$.
It belongs to the identity meromorphism.

(iii) M *contains only finitely many units.*
For, there are only finitely many automorphisms of F leaving P_0 fixed.

(iv) M has characteristic 0.

Theorems (i)–(iii) are immediate consequences of the definitions[24] whereas in Hasse's setup, Theorem (iv) is lying deeper. In the Hamburg notes he stated the stronger assertion about the norm

(v) $\mathcal{N}(n \cdot \mathbf{1}) = n^2 \neq 0$ for $n \in \mathbb{N}$,

and he indicated a somewhat complicated induction procedure for this purpose. Earlier, in a letter to Davenport of November 11, 1933 he had said that this procedure was "*following approximately Weber, Algebra* III, §58". Checking this citation [Web08] we found that Weber in §58 discussed recursive formulas for the multiplication of the Weierstrass $\wp$-function, i.e., for computing $\wp(nu)$ as rational functions of $\wp(u)$ and $\wp'(u)$. The formulas which Hasse developed in characteristic p were somewhat more delicate since in the induction process he had to jump over the numbers n which are divisible by p. Later he was able to avoid this whole induction procedure. In his 1936 Crelle paper (I) Hasse presented another, simplified proof, and Deuring in his 1940 correspondences paper contributed further simplifications. Nevertheless we have mentioned here Hasse's first approach of November 1933 because on this occasion we have his explicit statement that for inspiration he heavily drew on H. Weber's book on elliptic functions – and we know this not only for this particular problem but

[24] For (iii) at least in characteristic $p > 3$ where the classical Weierstrass normal form could be used. In characteristics $p \leq 3$ and in particular if $p = 2$ Hasse had to prove a new theorem which had no analogy in the characteristic 0 case. He did so in his Crelle paper (II), §1.

quite generally, in the process of building the theory of elliptic function fields for arbitrary characteristic p.

But it turns out that it is not really necessary at this point to know the precise value of the norm $\mathcal{N}(n \cdot \mathbf{1})$. As Deuring [Deu40] observed: To prove (iv) it suffices to show that for a given $n \in \mathbb{N}$ the kernel Γ_n of the multiplication $n : \Gamma \to \Gamma$ is finite. According to (3) this means that there are only finitely many P for which $\dfrac{P^n}{P_0^n}$ is a principal divisor. In his 1935 Göttingen report Hasse announces that he will prove this

> …mit Schlüssen, die aus der Theorie der Weierstraßpunkte geläufig sind, nämlich durch Betrachtung von Differentialdeterminanten …
>
> *…using methods which are well known from the theory of Weierstrass points, namely by considering differential determinants …*

And in the 1936 Crelle paper (I) Hasse presented the details. He used the theory of higher derivatives in characteristic p which he had developed for this purpose in an earlier paper in the same volume of Crelle's Journal [Has36a]. Since this is of general interest, apart from its application to the Riemann hypothesis, let us briefly report on it.

2.4.1 Higher derivatives and differential determinants

In this section we present the theory of higher derivatives in the systematic and generalized form as it had been developed by Hasse and F. K. Schmidt in their later 1937 paper [Has37a]. See also Teichmüller [Tei36].

Given a field extension $F|K$ of arbitrary characteristic, a "higher derivation" of $F|K$ is defined to be a sequence of K-linear functions $y \mapsto D^{(\nu)}(y)$ $(\nu = 0, 1, 2, \ldots)$ such that $D^{(0)}(y) = y$ and the following rules are satisfied:

$$D^{(\nu)}(yz) = \sum_{i+j=\nu} D^{(i)}(y) D^{(j)}(z) \qquad \text{(product formula)}$$

$$D^{(\mu)} D^{(\nu)}(y) = \binom{\mu+\nu}{\mu} D^{(\mu+\nu)}(y) \qquad \text{(iteration formula)}$$

Here, y, z range over the elements of the given field F, and the values $D^{(\nu)}(y)$, $D^{(\nu)}(z)$ should be contained in F.

In the iteration formula the binomial coefficient $\binom{\mu+\nu}{\mu}$ occurs whereas in the classical case of characteristic 0 the $D^{(\nu)}$ are defined by recurrence and there is no extra coefficient (and then binomial coefficients occur in the product formula). This seemingly minor point makes all the difference and admits the application also in characteristic p.

If $F|K$ is an algebraic function field and $x \in F$ a separating element then there is one and only one higher derivation $D_x^{(\nu)}$ of $F|K$ such that $D_x^{(1)}(x) = 1$ and $D_x^{(\nu)}(x) = 0$ for $\nu > 1$. This is called the derivation "with respect to x".

If $\mathcal{L} \subset F$ is any finite K-module and $y_0, y_1, \dots y_{n-1}$ a basis of $\mathcal{L}$ then the determinant

$$D_x(\mathcal{L}) = \det D_x^{(\nu)}(y_i) \qquad (i, \nu = 0, 1 \dots, n-1)\,,$$

if non-zero, does not depend on the choice of the basis (up to a constant factor). If (dx) denotes the divisor of the differential dx then the divisor

$$\mathfrak{d}(\mathcal{L}) = D_x(\mathcal{L})(dx)^{1+2+\cdots+n-1} \tag{13}$$

is independent also of the choice of the separating element x. This divisor is contained in the $(1+2+\cdots+n-1)$-th power of the differential class of $F|K$. If $F|K$ is elliptic then the differential class coincides with the principal class, hence $\mathfrak{d}(\mathcal{L})$ is a principal divisor, i.e., a non-zero element in F, uniquely determined by $\mathcal{L}$ up to a constant factor.

These $\mathfrak{d}(\mathcal{L})$ are the differential determinants which Hasse had mentioned in his letter to Davenport.

Now, assume $F|K$ to be elliptic and P_0 its point of reference. Let $n \in \mathbb{N}$. Consider the K-module $\mathcal{L}_n = \mathcal{L}(P_0^n)$ of those $z \in F$ which have P_0 as its only pole, and of order $\leq n$. It is of dimension n (since the genus $g = 1$). In formula (13) take $\mathcal{L} = \mathcal{L}_n$. In his first 1936 Crelle paper (I) Hasse shows that $D_x(\mathcal{L}_n) \neq 0$ and

$$\mathfrak{d}(\mathcal{L}_n) = \frac{A_n}{P_0^{n^2}} \tag{14}$$

where A_n is an integral divisor whose prime components P are precisely those for which $\dfrac{P^n}{P_0^n} \sim 1$, i.e., $nP = 0$.

This then proves that the kernel Γ_n of $n : \Gamma \to \Gamma$ is finite, hence theorem (iv) above. In order to prove theorem (v), Hasse discusses carefully the numerator A_n of $\mathfrak{d}(\mathcal{L}_n)$ and finds that every prime P dividing A_n has multiplicity $\mathcal{N}_i(n)$, which is the inseparable factor of the norm $\mathcal{N}(n)$. But, as said above already, this was later superseded by Deuring's observation.

The verification of (14) is done, as Hasse had announced, with methods which are used in the theory of Weierstrass points. Of course, there are no Weierstrass points in the elliptic function field $F|K$. Hasse meant that the *methods* used in the theory of Weierstrass points are the same, or similar, to what he used here.

Hasse was familiar not only with Weber's book [Web08] but also with the book by Hensel-Landsberg on the theory of algebraic functions [HL02] where the classical theory of Weierstrass points is presented. There, on page 454 we indeed find the differential determinants which appear in Hasse's setup – but with the difference that now he had to modify the notion of higher derivatives in the way explained above, so that it can be applied also in characteristic p. Although the final outcome looks rather natural and straightforward, Hasse had to work quite a lot to put these things into shape. We can follow this development in his frequent letters to his friend Davenport where Hasse reports on his progress. On October 16, 1935 Hasse writes after explaining to Davenport his modified notion of higher derivatives:

> *Do not think all this is trivial and contained in elementary books. For it is not. Let alone that I could not find a book that contained the explicit formulae ... Even if such a book existed, it would have been of no use whatsoever. For it surely will be using the recurrent definitions* [of the higher derivatives] *which are senseless for fields of prime characteristic p .*

By the way, the proper theory of Weierstrass points in characteristic p was developed some years later by F. K. Schmidt in [Sch39]. It seems evident that he was inspired by Hasse's modified theory of differential determinants, which F. K. Schmidt calls "Wronskian determinants".

As to formula (14) see also our comments to H. L. Schmid's paper [Sch41] at the end of section 3.2.

2.5 The Frobenius operator and the R.H.

Due to the theorem (iv) above, it is possible to identify $\mathbb{Z}$ with a subring of the endomorphism ring M. Hence for every $\mu \in \mathsf{M}$ the ring $\mathbb{Z}[\mu] \subset \mathsf{M}$ is an integral domain.

In his Hamburg lectures, Hasse did not yet know whether every $\mu \in \mathsf{M}$ is algebraic; he settled this question later only (in the affirmative sense). Also, the question whether M is always commutative was not yet settled. (It turned out that this is not always the case, but this can happen only when the so-called Hasse invariant $A = 0$.)

But the above mentioned first structure properties (i)-(iv) are sufficient to prove the Riemann hypothesis for F, *provided* some basic facts about the Frobenius operator are granted. The discovery of the Frobenius operator and its role in the arithmetic of function fields over finite base fields, is to be considered as the essential point of Hasse's second proof.

Suppose that the base field K is the algebraic closure of a finite field $\mathbb{F}_q$ with q elements. Let $F_q|\mathbb{F}_q$ be an elliptic function field and consider $F = F_qK$, the base field extension of $F_q|\mathbb{F}_q$. Geometrically speaking, $F = K(\Gamma)$ should be the function field of a smooth complete curve Γ which is defined over $\mathbb{F}_q$ already.

The exponentiation $z \mapsto z^q$ in F_q leaves the elements of the base field $\mathbb{F}_q$ fixed. It extends uniquely to an isomorphism π of F into itself leaving the elements of K fixed. In this way π becomes a meromorphism of $F|K$. The point of reference P_0 is to be chosen rational over $\mathbb{F}_q$; then π is normalized and hence defines an endomorphism of Γ. The $\mathbb{F}_q$-rational points are precisely those which are kept fixed by π. Today π is called the *q-th Frobenius operator* of F with respect to q.

As to the terminology we note that, in the context of function fields, Hasse does *not* use the name "Frobenius operator" – although the defining property, namely "raising into the q-th power", is the same as in the number field case where Hasse had introduced the name "Frobenius symbol" (see [Has30]).[25] Here

[25] Actually, the direct analogue of Hasse's "Frobenius symbol" in function fields means

Hasse just says "operation π". We do not know who had introduced the name "Frobenius operator" in the present context.

Since the image field is $F\pi = (F_q)^q K = F^q$ we have $\mathcal{N}(\pi) = q$. Since π is purely inseparable by definition, it is verified that $\pi - 1$ is separable. Hence $\mathcal{N}(\pi - 1)$ equals the number of points P for which $(\pi - 1)P = 0$, i.e., $\pi P = P$, i.e., P rational in $\mathbb{F}_q$. As usual in this context, the number of these primes is denoted by N. Thus we have:

$$\mathcal{N}(\pi) = q \qquad \text{and} \qquad \mathcal{N}(\pi - 1) = N\,. \tag{15}$$

As said above, in the 1934 Hamburg notes Hasse does not yet know that every endomorphism in M is algebraic. But for the Riemann hypothesis it is necessary to know that π is algebraic. Hasse writes to Davenport on January 29, 1934:

> *I am very troubled at present because I found a gap in my proofs about the elliptic case while drawing up my lectures for Hamburg. The whole thing seems too sensible for being wrong. But it may be that the proof of the actual result lies a bit deeper than my argument went so far. The possibility I have to exclude is that the operation π is transcendental. I can prove that if it is algebraical it must be imaginary quadratic, because a unit operation cannot exist.*

When Hasse writes that "*a unit operation cannot exist*" then he has in mind theorem (iii) of section 2.4. Thus he means that there are only finitely many units. This implies by the Dirichlet unit theorem that $\mathbb{Z}[\pi]$ is an order in an imaginary quadratic number field (or $\pi \in \mathbb{Z}$), and hence the only units in $\mathbb{Z}[\pi]$ are ± 1 except in the cases when $\mathbb{Z}[\pi]$ is the ring of 3-rd or of 4-th roots of unity in which case there are 6 or 4 units respectively.

Fortunately Hasse had been able to straighten this up, for on February 12, 1934, after his visit to Hamburg, he reported to Davenport as follows:

> "*... I was able to fill up the gap in my proof shortly after I wrote you how depressed I was. The new proof is, as Artin meant, even more adequate than the old would have been, were it consistent ...*"

And then he reports to Davenport about this proof, the same which we find in the Hamburg notes. Since this is somewhat involved, and since it was later superseded by Hasse's more complete structure results for M, we will not go into much detail here. Let us be content to say that Hasse defines the "conjugate" $\overline{\pi} \in \mathsf{M}$ and proves by comparing degrees that

$$\pi\overline{\pi} = \mathcal{N}(\pi) = q\,, \qquad \pi + \overline{\pi} = q + 1 - N\,. \tag{16}$$

This shows that π and $\overline{\pi}$ are the roots of the quadratic polynomial $L^\star(t)$ of (1) over $\mathbb{Z}$. Thus π is algebraic indeed and, as said above already, $\mathbb{Z}[\pi]$ is an order

something different: given a Galois field extension $E|F$ of function fields with finite base field and an unramified prime P of F with extension Q to E, the "'Frobenius symbol" $\left(\frac{E|F}{Q}\right)$ denotes an automorphism of the Galois group of $E|F$, with the property that it induces *in the residue field* the exponentiation with q^f, the order of the residue field modulo P.

in an *imaginary quadratic* field. Thus the discriminant of the polynomial $L^\star(t)$ is negative, i.e.,

$$|q+1-N| \leq \sqrt{q}.$$

This is the Riemann hypothesis for $F_q|\mathbb{F}_q$. (The case $\pi \in \mathbb{Z}$ needs some extra care. It can only happen when $\pi = \overline{\pi}$ and q is a square.)

We see here that for the Riemann hypothesis, it is not necessary to know the precise structure of the whole endomorphism ring M. It suffices to know the behavior of π and $\pi - 1$ only.[26] But Hasse did not stop here. He wished to go beyond and to clear up the precise structure of the whole endomorphism ring, even if this would not be absolutely necessary for the Riemann hypothesis itself.

In any case, it seems noteworthy that at this point already Hasse was able to define the conjugate $\overline{\pi}$, and even $\overline{\mu}$ for an arbitrary endomorphism μ; this was identical to the Rosati anti-automorphism which Deuring introduced later. But Hasse seemed not to know yet that $\mu \mapsto \overline{\mu}$ is an anti-automorphism. It is almost trivial that $\overline{\mu \cdot \nu} = \overline{\nu} \cdot \overline{\mu}$ but the additive property $\overline{\mu + \nu} = \overline{\mu} + \overline{\nu}$ is more subtle. If Hasse had known this, the proof of algebraicity could have been much shortened. (See section 3.3.)

2.6 Summary

The first task for Hasse was to find a substitute in characteristic p for the analytically based uniformization of a given elliptic curve. Hasse found at least a partial substitute by algebraically constructing the Jacobian and its isomorphism to the given curve. Today's construction, based on abstract algebraic geometry, was not yet available at that time and so he worked in the framework of algebraic function fields. The endomorphisms of the Jacobian (as an abelian variety) are given, in Hasse's setup, by what he called "meromorphisms", which he defined as isomorphisms of the function field into itself. The endomorphism ring of the Jacobian turns out to be without zero divisors and of characteristic 0. At the time of his Hamburg lecture Hasse did not know yet that every endomorphism is algebraic. But if an endomorphism μ is known to be algebraic then Hasse showed that the ring $\mathbb{Z}[\mu]$ contains only finitely many units and so, by Dirichlet's unit theorem, it is an order in an imaginary quadratic field (or $\mu \in \mathbb{Z}$).

In case of a finite base field Hasse discovered what today is called the "Frobenius endomorphism" π. He could show that π is algebraic, and that its quadratic equation over $\mathbb{Z}$ coincides with the L-polynomial which governs the zeta function of the curve. The fact that $\mathbb{Z}[\pi]$ is imaginary yields the validity of the Riemann hypothesis.

[26] In fact, this idea was taken up by Manin again many years later [Man60]. Manin says explicitly that his proof is based on Hasse's ideas. But, he adds, his proof is completely elementary. Since he worked with the Weierstrass normal form, he has to assume $p > 3$.

3 More structure theorems

As said in the foregoing section, in Hamburg 1934 Hasse did not yet know whether every endomorphism $\mu \in \mathsf{M}$ is algebraic. But he knew that *if* some $\mu \in \mathsf{M}$ is algebraic then μ is an imaginary quadratic integer (or $\mu \in \mathbb{Z}$). As said above, this follows from the Dirichlet unit theorem since $\mathbb{Z}[\mu] \subset \mathsf{M}$ contains only finitely many units. Hence μ is the root of a quadratic polynomial

$$X^2 - aX + b \qquad \text{with} \quad a, b \in \mathbb{Z} \quad \text{and} \quad |a| \leq 2\sqrt{b}\,. \tag{17}$$

It can be shown, and Hasse does it, that $b = \mathcal{N}(\mu)$; this implies that $a = \mathcal{N}(\mu) + 1 - \mathcal{N}(\mu - 1)$. This is a consequence of Hasse's norm addition formula, discussed below.

3.1 The norm addition formula

Hasse's norm addition formula reads as follows::

$$\mathcal{N}(\mu + \nu) + \mathcal{N}(\mu - \nu) = 2\,\mathcal{N}(\mu) + 2\,\mathcal{N}(\nu), \tag{18}$$

valid for arbitrary endomorphisms $\mu, \nu \in \mathsf{M}$. Given this formula together with the statements:

(a) $\mathcal{N}(\mu) \in \mathbb{Z}$
(b) $\mu \neq 0 \Rightarrow \mathcal{N}(\mu) > 0$
(c) $\mathcal{N}(\mu\nu) = \mathcal{N}(\mu)\mathcal{N}(\nu)$

it is easy to deduce that $\mu \mapsto \mathcal{N}(\mu)$ defines a quadratic form on M and that every $\mu \in \mathsf{M}$ satisfies a quadratic equation

$$\mu^2 - a\mu + b = 0 \tag{19}$$

with

$$a = \mathcal{N}(\mu) + 1 - \mathcal{N}(\mu - 1) \tag{20}$$

$$b = \mathcal{N}(\mu)\,. \tag{21}$$

Since the quadratic form $\mu \to \mathcal{N}(\mu)$ is positive definite it follows

$$a^2 - 4b \leq 0 \tag{22}$$

which means that $\mu \in \mathsf{M}$ is *imaginary quadratic* (or $\mu \in \mathbb{Z}$). In case $\mu = \pi$ (Frobenius operator) we have noted already in section 2.5 that this implies the Riemann hypothesis. Hasse noted in particular that in this setup he did not have to use Dirichlet's unit theorem any more; recall that in his earlier proof this had been necessary, as mentioned in Hasse's letter to Davenport of January 29, 1934, cited in section 2.5.

Moreover, the above information implies the following

Theorem: *The endomorphism ring* M *of an elliptic function field* $F|K$ *is of one of the following types:*

I. $\mathsf{M} = \mathbb{Z}$.
If for all $\mu \in \mathsf{M}$ equality holds in (22).

II. M *is an order in an imaginary quadratic number field.*
If there exists $\mu \in \mathsf{M}$ for which (22) is a strict inequality, and μ commutes with all elements in M.

III. M *is an order in a quaternion division algebra over* $\mathbb{Q}$.
Otherwise.[27]

Hasse had presented this structure theorem in his Göttingen seminar.[28] Or maybe it was in the workshop (*Arbeitsgemeinschaft*) which had been established in Göttingen, organized by Ernst Witt.[29] As a consequence, several members of the seminar, or workshop, contributed to the attempt to simplify the derivation of the theorem from the norm addition formula.

One of those members was *Behrbohm* whose name is mentioned in Hasse's 1935 Göttingen report.[30] Hasse had published Behrbohm's simplified proof [Beh35] in the *Göttinger Nachrichten* right after Hasse's report. In the 1936 Crelle paper (III) Hasse mentioned that he followed Behrbohm's exposition together with certain further simplifications provided by *Teichmüller*, another member of the workshop. Finally, *Witt* in his *Zentralblatt* review of Behrbohm's note [Wit36] presented a short proof using not more than half a page deriving the theorem from the norm addition formula (18).

As to the norm addition formula itself, Hasse discovered it while trying to adapt a result of Davenport. Several times already we have had occasion to cite from the Hasse-Davenport letters; this reflects the fact that during those years there was a lively exchange of letters between the two. Among other topics, Hasse reported about the progress of his work and tried to interest Davenport in his problems on elliptic curves and beyond. On October 9, 1935 Hasse wrote:

> *I am very glad you are spending some further energy on the subject of our common interest. Your communication about the nature of the meromorphisms in the elliptic case seems to me extremely important and interesting. I should very much* [*like*] *to have a more detailed account of your proofs.*

[27] In this context the terminology "order" of a number field or a division algebra Σ over $\mathbb{Q}$ is meant in the sense of classical number theory. It is defined as a finite $\mathbb{Z}$-algebra $\mathsf{M} \subset \Sigma$ such that $\mathbb{Q}\mathsf{M} = \Sigma$.

[28] Note that in the summer of 1934 Hasse had moved from Marburg university to Göttingen.

[29] It is known that Hasse participated in the meetings of this workshop and, to a large degree, determined the topics to be studied.

[30] Hermann Behrbohm is mentioned in the list of Hasse's doctoral students, a list that was written down by Hasse himself. But it seems that Behrbohm did his Ph.D. thesis not with Hasse. Besides Behrbohm's above mentioned publication in the *Göttinger Nachrichten* he published only one paper which was on number theory, namely on the euclidean algorithm in quadratic fields [BR36], jointly with the Hungarian mathematician L. Redei who in 1934/35 was visiting Hasse in Göttingen as a Humboldt fellow. After that Behrbohm published only papers on applied mathematics; it seems that he had switched to aircraft industry. Behrbohm is mentioned in the list of German Ph.D.'s taking their examination in 1944. (This list is available in the internet on the homepage of the DMV (*Deutsche Mathematiker Vereinigung*)). His dissertation on supersonic flows is available in the Göttingen university archive. There he mentions Dozent Dr. Graeser and Prof. Kaluza as his referees.

The "subject of our common interest" was, of course, the structure of the endomorphism ring M and its relevance for the Riemann hypothesis.

We do not know the precise content of Davenport's communication. However we can guess from what he later published in the Cambridge Proceedings [Dav36]. Namely, the main result of Davenport in that paper is the theorem that every endomorphism in M is algebraic and, moreover, that M is commutative if $\pi \notin \mathbb{Z}$[31] (note that $\pi \in \mathbb{Z}$ can only happen if q is a square). For this purpose Davenport developed some kind of euclidean algorithm for endomorphisms. In addition he had to use and to prove the following norm inequality

$$\mathcal{N}(\mu + \nu) \leq 2\mathcal{N}(\mu) + 2\mathcal{N}(\nu), \tag{23}$$

which is a weaker form of (18).

It was Davenport's proof of this formula which Hasse was not satisfied with, and which he therefore wished to adapt to fit in his own framework. For, Davenport worked with Weierstrass normal form (4) (and hence he could deal with the case $p > 3$ only), and then he used the explicit formulae for the addition theorem (5), (6). For the proof of (23) it was necessary to estimate the degrees of the rational functions appearing in those formulas.

But as we have pointed out above already, Hasse wished to avoid, if possible at all, the use of normal forms in this context. On October 21, 1935 he told Davenport that he had obtained another proof and added:

> *What I have achieved with it is the total elimination of any normal form. This seems to me of high importance. For I have no hope of mastering the case $g > 1$ by discussing the degrees in the rational functions of the addition formulae.*

And several weeks later, on November 21, 1935, Hasse reported:[32]

> Zu meiner eigenen grössten Überraschung fand ich nämlich gestern den in meinen Augen "wahren" Beweis für die fraglichen Sätze über Meromorphismen ...
>
> *To my greatest surprise I found yesterday what in my eyes is the "genuine" proof for the meromorphism theorems in question ...*

And he proceeds to explain his "genuine" proof of the norm addition formla (18) in detail. Here, "genuine" in Hasse's opinion implies that there is no reference to normal forms and explicit addition formulas. Moreover, Hasse's norm addition formula (18) is a precise equality whereas Davenport's (23) is just an estimate.

It seems that Davenport, after having seen Hasse's norm addition formula and its proof, was hesitating to submit his own manuscript for publication, since it was to a large part superseded by Hasse's. But Hasse disagreed resolutely. On November 27, 1935 he wrote:

[31] This is not quite true; see our remark at the end of section 4.4.

[32] This letter was written in German; the translation is ours.

> *My dear Harold! Thanks very much for your kind letter. Of course you must publish your proof ! I have mentioned the fact, that you first had the idea of considering $N(\mu)$ as a sort of absolute value and proved the algebraicity and commutativity of normalized meromorphisms on this basis, in both my preliminary paper for the Göttinger Nachrichten and my detailed account for Crelle's Journal. . .*

Upon this, Davenport published his version in the Cambridge Proceedings [Dav36].

3.2 Hasse's proof

Perhaps it is not without interest to exhibit Hasse's main idea although, as we shall see, the Deuring shortcut 1940 in [Deu40] has rendered this proof obsolete.

We know that any normalized meromorphism $\mu : F \to F$ leads to an endomorphism $\mu : \Gamma \to \Gamma$. This is obtained by assigining to every point (prime divisor) P of F its induced point in the subfield $F\mu$, i.e., its norm, and then mapping this back to F by the isomorphism $\mu^{-1} : F\mu \to F$. By linearity this map extends to arbitrary divisors D of F. Thus we obtain an endomomorphism μ of the divisor group of F, defined by the formula

$$\mu D = \mathrm{Norm}_{F|F\mu}(D)\mu^{-1}.$$

This map preserves the degree of the divisor D.

By duality μ leads also to an endomorphism $\overline{\mu}$ of the divisor group of F. This is obtained in the following way: Any divisor D of F is transported to a divisor $D\mu$ of $F\mu$ by the isomorphism $F \to F\mu$, and in view of the inclusion $F\mu \subset F$ lifted to F by the conorm:

$$\overline{\mu}\,D = \mathrm{Conorm}_{F|F\mu}(D\mu)\,. \tag{24}$$

Under this map the degree of D will be multiplied by the field degree $[F : F\mu] = \mathcal{N}(\mu)$. If $D = P_0$ is taken as the prime of reference, of degree 1, then

$$\deg \overline{\mu}\,P_0 = \mathcal{N}(\mu)\,. \tag{25}$$

Now Hasse does this for the 4 meromorphisms $\mu, \nu, \mu + \nu, \mu - \nu$. He obtains 4 divisors of F, of degrees $\mathcal{N}(\mu)$, $\mathcal{N}(\nu)$, $\mathcal{N}(\mu + \nu)$ and $\mathcal{N}(\mu - \nu)$ respectively. Hasse in [Has36d] shows that the divisor

$$\frac{\overline{(\mu+\nu)}\,P_0 \cdot \overline{(\mu-\nu)}\,P_0}{\overline{\mu}\,P_0^2 \cdot \overline{\nu}\,P_0^2} \tag{26}$$

is a principal divisor of F, hence of degree 0. This gives (18). Well, this works only under the assumption that neither of those 4 endomorphisms is zero; the other cases require extra care which however one is used to in the theory of complex multiplication and can deal with in the standard manner. Under the said assumption Hasse could explicitly exhibit an element in F whose principal divisor is given by (26): Take $x \in F$ which has P_0^2 as its pole divisor; then we have

$$\frac{\overline{(\mu+\nu)}\,P_0 \cdot \overline{(\mu-\nu)}\,P_0}{\overline{\mu}\,P_0^2 \cdot \overline{\nu}\,P_0^2} \cong x\mu - x\nu \tag{27}$$

where $\cong$ means equality of divisors. Thus the norm addition formula (18), which is a relation between degrees, is interpreted as a relation between divisors – which fits well into Hasse's intentions.

Hasse explains in [Has37b] that he had found the above proof in analogy to the classical case:

> Die Normenadditionsformel erhält man, wenn man das aus der klassischen komplexen Multiplikation geläufige Verfahren der Nullstellen- und Polbestimmung der Funktion $\wp(\mu u) - \wp(\nu u)$ algebraisiert, d.h. die Zähler- und Nennerprimdivisoren von $x\mu - x\nu$ bestimmt und ihre Anzahlen gleichsetzt, wo x irgendein Element mit dem genauen Nenner P_0^2 aus F ist.
>
> *The norm addition formula is obtained by algebraizing the familiar procedure from the classical complex multiplication, to determine the zeros and poles of the function $\wp(\mu u) - \wp(\nu u)$; this means to determine the prime divisors of the numerator and those of the denominator of $x\mu - x\nu$ and to compare their numbers, where x is any element in F with the exact denominator P_0^2.*

The "familiar procedure" which Hasse is referring to, is represented by the formula

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} = \wp(u) - \wp(v) \tag{28}$$

known from the classical theory of elliptic functions. Here, $\wp(u)$ and $\sigma(u)$ denote the Weietrstrass $\wp$-function and σ-function. The formal coincidence of this classical formula with (27) is apparent. It is a good example of the translation process from the analytic to the algebraic language. The role of analytic functions is taken over, in the algebraic framework, by divisors.

In later years, H. L. Schmid (an assistent to Hasse in Göttingen until 1938) took up the challenge, and he found algebraic equivalents for several other analytically based formulas. In his 1941 paper [Sch41] he says:

> Das Ziel der Arbeit ist zu zeigen, daß der gesamte Bestand der Formeln, welche die (in ihrer transzendenten Uniformisierung durch $\wp$ und $\wp'$ ausdrückbaren) elliptischen Funktionen als Produkt von σ-Funktionen darstellen, abstrakt darstellbar ist... Die Gleichheiten werden zu Divisorrelationen, die das Wesentliche, nämlich Nullstellen und Pole, in Evidenz setzen.
>
> *The aim of this paper is to show that the entire stock of formulas which represent elliptic functions (given in their transcendental uniformisation by $\wp$ and $\wp'$) as products of σ-functions, are representable in abtract form... Equalities become divisor relations which make evident the essential features, namely zeros and poles.*

H. L. Schmid's paper discusses not only Hasse's (27) but also quite a number of other relations. Particularly noteworthy is the analytic origin of Hasse's determinant formula (14) which H. L. Schmid identifies as:

$$\begin{vmatrix} \wp'(u) & \wp''(u) & \dots & \wp^{(n-1)}(u) \\ \wp''(u) & \wp'''(u) & \dots & \wp^{(n)}(u) \\ \dots & \dots & \dots & \dots \\ \wp^{(n-1)}(u) & \wp^{(n)}(u) & \cdots & \wp^{(2n-3)}(u) \end{vmatrix} = \varepsilon \frac{\sigma(nu)}{\sigma(u)^{n^2}} \qquad (\varepsilon \text{ constant}) \qquad (29)$$

If we consider that at Hasse's time there was no algebraic theory of endomorphisms of abelian varieties, and that Hasse had set out not only to find the facts but also to develop the proper framework to understand the facts, then we appreciate his proof of (14) which consists of the algebraization of those analytic formulas. But as said earlier already, that proof was soon superseded by Deuring's shortcut.

3.3 Deuring's shortcut

In a letter of May 9, 1936 Deuring, who held a position as assistant to van der Waerden in Leipzig at that time, sent a letter to Hasse announcing that he had developed a concept which would probably allow one to generalize Hasse's results to function fields of higher genus. Deuring wrote:

> In den letzten Wochen habe ich versucht, Ihre Ergebnisse für elliptische Funktionenkörper auf Körper höheren Geschlechts zu verallgemeinern. Das ist mir bis zur Aufstellung des Multiplikatorenringes und den Beweis seiner Algebraizität gelungen. . . . ich schicke Ihnen die Einleitung einer geplanten Arbeit. Die Beweise sind zwar vollständig durchgeführt, aber noch in einem monströsen Zustand.
>
> *In recent weeks I have tried to generalize your results from elliptic function fields to fields of higher genus. I have succeeded in setting up the ring of multipliers*[33] *and proved its algebraicity. . . I am sending you the introduction of a paper in preparation. The proofs are already complete but still in bad shape.*

In fact, Deuring's concept marked a decisive turn on the way towards the proof of the Riemann hypothesis for higher genus. His results appeared finally in two papers on correspondences: one in 1937 and the second in 1940: [Deu37], [Deu40]. We shall discuss this in detail in Part 5. Here we only wish to remark that even for genus $g = 1$, Deuring's results led to substantial progress.

In his second paper he showed that (for arbitrary genus) the endomorphism ring M admits an *involutoric anti-automorphism* $\mu \mapsto \overline{\mu}$ which he called "Rosati anti-automorphism". It seems that a letter of Lefschetz to Hasse, dated July 20, 1936 caused Deuring to study Rosati's work. This letter was written in Oslo right after the conference of the International Mathematical Union. Hasse had been invited to give an 1-hour talk at Oslo, and had reported about his work on the Riemann hypothesis for elliptic function fields [Has37b]. In the last part of his talk he reported briefly about Deuring's new approach for higher genus

[33] To say it again, Deuring means the ring of "endomorphisms" in today's terminology.

– which in fact was quite new since he had received Deuring's letter only a couple of weeks earlier. It seems that after Hasse's talk he had a discussion with Lefschetz. In his letter Lefschetz referred to this discussion and mentioned some literature regarding the work of Italian geometers, in particular that of Rosati. Hasse had shown Lefschetz' letter to Deuring.[34]

In the elliptic case Deuring proved the relation

$$\mu\overline{\mu} = \mathcal{N}(\mu) \tag{30}$$

as an almost immediate consequence from his definition. Combined with the fact that $\mu \mapsto \overline{\mu}$ is an anti-automorphism, Hasse's norm addition formula (18) follows easily. However, in view of (30) it is not necessary any more to consider the norm addition formula. For we compute

$$\mathcal{N}(\mu - 1) = (\mu - 1)(\overline{\mu - 1}) = (\mu - 1)(\overline{\mu} - 1) = \mathcal{N}(\mu) - (\mu + \overline{\mu}) + 1 \tag{31}$$

and hence μ is the root of the quadratic polynomial

$$\begin{aligned}(X - \mu)(X - \overline{\mu}) &= X^2 - \big(\mathcal{N}(\mu) + 1 - \mathcal{N}(\mu - 1)\big)X + \mathcal{N}(\mu) \\ &= X^2 - aX + b\end{aligned} \tag{32}$$

whose coefficients a, b are integers in $\mathbb{Z}$. (Compare with (20), (21).) This shows, firstly, that every $\mu \in \mathsf{M}$ is a quadratic integer. Moreover, since $\mathcal{N}(\mu) > 0$ for all $\mu \neq 0$ it follows

$$|a| \leq 2\sqrt{b}$$

which, in case $\mu = \pi$ is the Frobenius operator, yields the Riemann hypothesis (2) in view of (15).

We may assume that Hasse, who in his letter to Davenport of November 21, 1935 had expressed his satisfaction to have found his "genuine proof" of algebraicity, will have changed his mind after having seen Deuring's arguments, and perhaps he will have considered that as the true "genuine" proof.

Remark: It is not without purpose that in (24) we have used the notation $\overline{\mu}$. (Hasse in [Has36d] did not use it.) This is the same notation which we have used for the Rosati anti-automorphism as defined by Deuring. Note that the conorm map in (24) induces a homomorphism of divisor classes of degree 0. But the group of divisor classes of degree 0 is the Jacobian of the given elliptic curve Γ, and hence it is isomorphic to Γ by means of (3). Thus the conorm map in (24) defines a homomorphic map of Γ into itself and, as Deuring [Deu37] has observed, this map can indeed be represented by a meromorphism in the sense of Hasse. It follows from Deuring's theory that this is the Rosati anti-automorphism of M.

We see that in reality Hasse's formula (24) refers to Rosati's anti-automorphism, without Hasse having been aware of this fact.

3.4 Consequences

In [Deu40] Deuring presents more results concerning the structure of M, as consequences of his shortcut arguments involving the Rosati anti-automorphism:

[34] This letter, as well as other correspondence of Hasse concerning the R.H. for higher genus, including the letters exchanged with A. Weil, will be discussed in more detail in Part 5.

3.4.1 The norm

If $\mu \notin \mathbb{Z}$ then it follows from (30) and (32) that $\mu \mapsto \overline{\mu}$ is the Galois action of $\mathbb{Z}[\mu]$, and $\mathcal{N}$ is the ordinary norm function from the quadratic field $\mathbb{Q}(\mu)$ to $\mathbb{Q}$ – which in the first place was the reason for Hasse to call $\mathcal{N}$ the "norm" and not just "degree".

If $\mu = n \in \mathbb{Z}$ then $\overline{n} = n$ and hence from (30)

$$\mathcal{N}(n) = n^2. \tag{33}$$

This is the formula which Hasse had obtained when he proved theorem (iv), section 2.4. But here the formula (33) appears quite naturally from (30), without cumbersome comparison of divisor degrees – once the above theorem (iv) is established which says that M is of characteristic 0. The latter is necessary to ensure that the endomorphism $n \cdot \mathbf{1} \neq 0$. For, on the left hand side of (33), the symbol n stands for the n-th fold identity endomorphism $n \cdot \mathbf{1}$ which thereafter is identified with $n \in \mathbb{Z}$ because of characteristic 0. For the proof of theorem (iv) Deuring still refers to Hasse's formula (14), although in retrospective we observe that this would not have been necessary; it is easy to verify that not all $P \in \Gamma$ are annihilated by a single prime number.

If $n \not\equiv 0 \bmod p$ then it follows from (33) that n as a meromorphism of F is separable, and hence $\mathcal{N}(n) = n^2$ equals the order of the n-torsion group Γ_n of Γ. This gives immediately Hasse's structure theorem for the whole torsion group of Γ, as long as only torsion $\not\equiv 0 \bmod p$ is considered, namely: this group is isomorphic to the pairs (r_1, r_2) of rational numbers modulo 1 with the specification that the denominators of the r_i are not divisible by p. We have reported on that theorem in section 2.1 already.

3.4.2 ℓ-adic representation

Let ℓ be a prime number different from the characteristic p. The group of ℓ-power torsion of Γ is isomorphic to the pairs (r_1, r_2) of rational numbers modulo 1 whose denominators are powers of ℓ. The group theoretic endomorphisms of this group can be represented by 2×2 matrices with coefficients in the ℓ-adic integers $\mathbb{Z}_\ell$. This yields a faithful representation of M by 2×2 matrices over Z_ℓ.

It seems that Deuring was the first who in a publication had defined these ℓ-adic representations and used it to investigate elliptic function fields. (But we find them already earlier in a letter of Hasse to Davenport dated October 21, 1935.)

In his second correspondence paper (1940) Deuring considered the case when M is non-commutative and hence an order in a quaternion division algebra Σ. The ℓ-adic representation of M extends uniquely to a representation of Σ by 2×2-matrices over the ℓ-adic rationals $\mathbb{Q}_\ell$. The existence of such a representation implies that Σ splits over $\mathbb{Q}_\ell$. This holds for all prime numbers $\ell \neq p$. But every quaternion division algebra over $\mathbb{Q}$ is ramified at 2 primes at least (where "primes" include ∞ in this context). It follows that Σ is necessarily the unique quaternion division algebra $\mathbb{H}_{\infty,p}$ which is ramified at ∞ and at p only.[35]

[35] Deuring writes $Q_{\infty,p}$.

This is the first structure theorem on M which goes beyond Hasse's results. At the end of his paper Deuring announces more precise structure theorems. These appeared one year later in the *Hamburger Abhandlungen*, through a more detailed investigation of the ℓ-adic representation. See section 6.

Note: It was well known in 1935 that quaternion algebras over $\mathbb{Q}$ are in 1-1 correspondence with the finite subsets S of primes p in $\mathbb{Q}$ (including $p = \infty$) – with the specification that the cardinality of S is even. This is a consequence of Hasse's theory of what today are called "Hasse invariants" of finite dimensional simple algebras over number fields. The set S is the set of prime numbers which are ramified in the quaternion algebra. See [Has33b]. Certainly Deuring was well acquainted with the theory of algebras and in particular with their Hasse invariants, for this was covered in his book [Deu35] on algebras.

If $p = 2$ then $\mathbb{H}_{\infty,2}$ is just the ordinary quaternion algebra over $\mathbb{Q}$, generated by i and j with the relations $ij = -ji$ and $i^2 = -1$, $j^2 = -1$. If the last relation is replaced by $j^2 = -p$ then we obtain generators of $\mathbb{H}_{\infty,p}$ for $p > 2$, provided $p \equiv -1 \bmod 4$. In the case $p \equiv 1 \bmod 4$ one has to change the first relation too, namely $i^2 = -r$ where $r \equiv -1 \bmod 4$ is a positive prime number which is a quadratic non-residue modulo p.[36]

3.4.3 p-torsion

As to the group of p-power torsion of Γ, it suffices to determine the group Γ_p of those endomorphisms which are annihilated by p. Note that the order of Γ_p equals the separability degree $\mathcal{N}_s(p)$, hence from (33) it is either 1, p, or p^2. But the last alternative does not appear. This follows from the representation of M on the K-module Ω of holomorphic differentials of F. That representation yields a homomorphic mapping of M into the field K of characteristic p, and consequently $p \in \mathsf{M}$ is mapped onto zero. This signifies that p as a meromorphism of F is inseparable. See our section 2.3.1 on Abel's theorem.

It follows that *either* Γ_p is of order p , *or* $\Gamma_p = 0$. In the first case the full p-power torsion of Γ is isomorphic to the group of rational numbers r modulo 1 whose denominator is a power of p, and in the second case the p-power torsion of Γ is 0. However, this argument gives no clue whether any of those possibilities can occur, and under what circumstances. This will be discussed below with the help of Hasse's invariant A which vanishes if and only if $\Gamma_p = 0$.

If $\Gamma_p \neq 0$ then, similarly as above for ℓ, we obtain a faithful p-adic representation of M, but this time by 1×1 matrices, which is to say in the p-adic integers. In particular it follows that M is commutative in this case. It follows that in the non-commutative case one has necessarily $\Gamma_p = 0$.

[36] I am indebted to Patrick Morton for reminding me that those relations are stated by Hasse in his Italian paper [Has43], p.346. (Note that Hasse forgot to say that r should be a *prime number* with the stated properties.) That paper will be discussed in detail in Part 5.

3.5 Summary

In Hasse's Hamburg lecture notes the proofs were often given as a sketch only. During the next years he worked out the details. His final version was published 1936 in three parts in Crelle's Journal. There he had to rely on a number of general properties of function fields which were not known before, and which therefore he had to establish first in separate papers. This preparatory work includes: the theory of differentials and the theorem of the residues; the theory of higher derivations and differentials; the arithmetic of cyclic extensions of function fields including the Artin-Schreier extensions, in particular their ramification structure; the construction of unramified cyclic extensions of degree p . Some of this work was done in collaboration with others: F. K. Schmidt, Teichmüller, Behrbohm, Witt and Deuring.

One of the main theorems which Hasse presented in his Crelle papers is what he called the "norm addition formula". He found it after he had learned from Davenport a somewhat weaker result, when he tried to fit Davenport's proofs into his framework of abstract function fields. Once the norm addition formula was established, the structure of the endomorphism ring could be immediately obtained. It turned out that the endomorphism ring is either $\mathbb{Z}$*, or an order in an imaginary quadratic number field, or else an order in a quaternion division algebra over* $\mathbb{Q}$*. Hasse showed by an example that also the third type does occur in characteristic p. The discovery of non-commutative endomorphism rings came as a surprise to the people working in this area.*

Starting in 1936 Deuring developed the algebraic theory of correspondences of curves (or function fields) which turned out to provide the basis for the proof of the Riemann hypothesis for higher genus. But Deuring's theory was also useful for the elliptic case and provided a shortcut for some essential parts of Hasse's proofs. This was due to the discovery of the Rosati anti-automorphism of the endomorphism ring which probably was obtained following a hint in a letter of Lefschetz to Hasse. But Deuring did not only simplify and streamline Hasse's proofs; by using the ℓ*-adic representations of the endomorphism ring he showed that in the non-commutative case the quaternion division algebra which appears was the one which is uniquely determined by the fact that only* ∞ *and p (the characteristic) are ramified.*

4 The Hasse invariant A

4.1 p-torsion

Even before Deuring's shortcut, Hasse was well aware about the two alternatives for the p-torsion Γ_p. In fact, as early as November 1933 Hasse had communicated this to Davenport; we have mentioned this letter already in section 2.1, last paragraph. Hasse was able to define an invariant of the elliptic field which he called A, which vanishes if and only if the p-torsion $\Gamma_p = 0$; if $A \neq 0$ then Γ_p is cyclic of order p. As above, Γ_p denotes the group of those points $P \in \Gamma$ which are annihilated by p.

This result was really new. The structure of Γ_p is quite different from what was known from the analytic theory in characteristic 0. So it was not just a question of transferring known classical results to prime characteristic. Hasse was the first to develop an idea how to approach this problem in characteristic p. Let us discuss the way how he arrived at this and similar results.

The structure problem for Γ_p is equivalent to the problem of unramified cyclic extensions of F. To see this, consider the meromorphism μ_p which induces the multiplication with p, i.e., $\mu_p X = pX$ for all X. Consider the subfield $F\mu_p \subset F$. The field extension $F|F\mu_p$ is not separable; let $F'|F\mu_p$ be the separable part while $F|F'$ is purely inseparable. Then $F'|F\mu_p$ is unramified and abelian, and its Galois group is the group of translations τ_P for $P \in \Gamma_p$; this group is isomorphic to Γ_p. Hence Hasse's theorem about Γ_p is equivalent to a statement about the Galois group of unramified abelian extensions of $F\mu_p$. Since $F\mu_p$ is isomorphic to F we see that Hasse's theorem can also be formulated in the following way:

Theorem: *Let $F|K$ be elliptic with algebraically closed base field K of characteristic $p > 0$. Either there exists precisely one cyclic unramified extension of degree p, or there is none. This alternative is given by the Hasse invariant A being $\neq 0$ or $A = 0$.*

Let us first discuss Hasse's definition of A. Actually, Hasse in [Has34d] assumed that $p > 2$. But his idea works also for $p = 2$, and so we will present his theory without any restriction on the characteristic; this certainly would get his approval.

4.2 Motivation and definition

In the elliptic function field $F|K$ there exists a unique holomorphic differential $\omega \neq 0$ (up to a constant factor). In this connection, "holomorphic" is to be understood in the algebraic sense; it means "without poles". The differential divisor (ω) is trivial, i.e., ω has no zeros either. Let t be a uniformizing variable at the point P_0 of reference, and consider the power series expansion at P_0:

$$\omega = (c_0 + c_1 t + c_2 t^2 + \cdots)\,\mathrm{d}t\,. \tag{34}$$

Here, $c_0 \neq 0$ since ω has no zeros. Then Hasse defines the invariant

$$A = \frac{c_{p-1}}{c_0^p}\,. \tag{35}$$

If ω is replaced by a multiple $c\omega$ with $0 \neq c \in K$ then A has to be replaced by $c^{-(p-1)}A$ which is immediate from the definition (35). Thus the element A itself is not really an invariant of the field, but the fact that $A \neq 0$ or $A = 0$ is invariant.[37]

In his letter of November 5, 1933 to Davenport, Hasse explains how he discovered this invariant A. He refers to the classical case where the base field

[37] Recall that we assume here that the base field K is algebraically closed. If K is arbitrary perfect then the residue class of A modulo $(p-1)$-th powers of K is an invariant.

$K = \mathbb{C}$ is the field of complex numbers. In this case the "integral of the first kind" $u = \int \omega$ has the expansion

$$u = c_0 t + \frac{c_1}{2} t^2 + \frac{c_2}{3} t^3 + \cdots \tag{36}$$

in view of (34). Explicitly, if the field F is generated in Weierstrass normal form:

$$F = K(x, y) \quad \text{with} \quad y^2 = 4x^3 - g_2 x - g_3, \quad \Delta = g_2^3 - 27 g_3^2 \neq 0 \tag{37}$$

one usually takes the following normalization of the holomorphic differential and a uniformizing variable at the point at infinity:

$$\omega = \frac{\mathrm{d}x}{y} \qquad \text{and} \qquad t = \frac{-2x}{y} \tag{38}$$

(This normalization implies that in the expansion (34) one has $c_0 = 1$.) Then u satisfies the differential equation $\mathrm{d}u = \frac{\mathrm{d}x}{y}$ or, equivalently, $y = \frac{\mathrm{d}x}{\mathrm{d}u}$. In other words: If x and y are regarded as analytic functions of the local parameter u then y appears as the derivative of x.[38]

Having pointed out this classical procedure of uniformization, Hasse writes to Davenport:

> *This is not possible for characteristic* p*, on account of the well-known denominators in the development of* $x = \wp(u)$, $y = \wp'(u)$ *in power series in* u *or of the reciprocal series of* u *in* $t = \frac{-2x}{y} = -\frac{2\wp(u)}{\wp'(u)}$ *. But one can get an approximation, by taking*

$$u \ = c_0 t + \frac{c_1}{2} t^2 + \frac{c_2}{3} t^3 + \cdots + \frac{c_{p-2}}{p-1} t^{p-1} \tag{39}$$

instead of (36). Then, Hasse continues,

$$\begin{aligned} \omega &= \mathrm{d}u + c_{p-1} t^{p-1} \mathrm{d}t + \cdots & (40) \\ &= \mathrm{d}u + c_{p-1} \frac{u^{p-1}}{c_0^{p-1}} \frac{\mathrm{d}u}{c_0} + \cdots & (41) \\ &= (1 + A u^{p-1}) \mathrm{d}u + \cdots & (42) \end{aligned}$$

where the dots represent terms of higher order. We see:

The Hasse invariant A *defined in characteristic* p *by formula* (35) *represents the first obstacle to integrating the holomorphic differential* ω*, and it leads to an approximate integral* u *of the form* (39)*, satisfying a differential equation of the form* (42)*.*

A does not depend on the choice of the point P_0 of reference since the group of translation automorphisms acts transitively on the points.

[38] One usually writes $x = \wp(u)$, $y = \wp'(u)$; this is the classical Weierstrass notation. But Hasse in his papers on the Riemann hypothesis mostly avoids this notation, presumably because he wishes to use the symbol $\wp$ for the Artin-Schreier operator $\wp(x) = x^p - x$. See the next section 4.3. But in his letter to Davenport cited below he uses the function symbol $\wp(u)$ in the Weierstrass meaning.

4.3 Unramified cyclic extensions

Having explained the definition of A, Hasse now proceeds to prove his theorem about unramified cyclic extensions and the alternative $A \neq 0$ or $A = 0$ (see section 4.1).

Today this theorem is well known, and it is the starting point of all investigations involving p-extensions of elliptic fields. In Hasse's time, the necessary tools for its proof were not yet available, and so Hasse had to provide them himself. In particular Hasse had to use the results of his paper [Has34d] concerning Artin-Schreier extensions of function fields.

In 1927 Artin and Schreier [AS27] had shown that in characteristic $p > 0$ every cyclic field extension $E|F$ of degree p can be generated in the form $E = F(y)$ where y satisfies an equation of the form

$$y^p - y = z \qquad \text{with} \qquad z \in F\,. \tag{43}$$

Today such extensions are called "Artin-Schreier extensions", and an equation of the above form is called "Artin-Schreier equation". Introducing the Artin-Schreier operator $\wp(y) = y^p - y$, such an equation can also be written in the form $\wp(y) = z$. The element z is called an "Artin-Schreier radicand" of E. It is uniquely determined modulo $\wp F$. (More precisely, the additive subgroup of $F/\wp F$ of order p generated by z is determined by the cyclic extension E.)

By 1934 the Artin-Schreier theory was well known but, for application in function fields F, it had still to be amended by valuation theoretic considerations, in particular with respect to ramification properties. This was done by Hasse in his 1934 paper on cyclic fields. Before Hasse, little was known about a cyclic p-extension of function fields. In a letter of July 7, 1933 Hasse wrote to Davenport:

> *My dear Harold, I have succeeded in proving my presumption on the exponentials. For $y^p - y = f_3(x)$ the genus is really $p - 1$ ...*

And one day later:

> *I have got much more general results on $y^p - y \;= C$ than I first thought ...*

Here, Hasse studied Artin-Schreier extensions over a rational function field. And finally, in his 1934 paper on cyclic fields Hasse was able to compute the genus of an Artin-Schreier extension over an arbitrary function field of characteristic p – he obtained the formulas which today are given in any textbook on function fields. (See e.g., Stichtenoth [Sti93].)

Let P be any point of F and denote by v_P the corresponding valuation, normalized such that $v_P(F^\times) = \mathbb{Z}$. Suppose the cyclic p-extension $E|F$ is given by the Artin-Schreier radicand $z \in F$ as explained above. Hasse showed: There exists $z_P \in F$ such that $z \equiv z_P \bmod \wp F$ and that the following alternative holds: *either* $v_P(z_P) \geq 0$, *or* $v_P(z_P) < 0$ and $v_P(z_P) \not\equiv 0 \bmod p$. In the first case $E|F$ is unramified at P, and in the second case the ramification degree is p.

Moreover, if in the second case $v_P(z_P) = -m_P < 0$ then the contribution of P to the different of $E|K$ equals $(p-1)(m_P+1)$. Hence, if g_F denotes the genus of $F|K$ and similarly g_E then by the Riemann-Hurwitz genus formula one has

$$2g_E - 2 = 2g_F - 2 + \sum_{P \text{ ramified}} (p-1)(m_P+1)\,. \tag{44}$$

For elliptic fields the genus is 1 and it follows:

Suppose F is elliptic and $E|F$ a cyclic extension of degree p. Then $E|F$ is unramified if and only if E is elliptic too.

Now, if F is elliptic: Which radicands $z \in F$ lead to unramified cyclic extensions $E|F$? To every $P \in \Gamma$ there has to exist $z_P \equiv z \bmod \wp F$ such that $v_P(z_P) \geq 0$. Now, Hasse proceeds to normalize z in a suitable way so that he could classify those z. This means to replace z by a suitable representative $\equiv z \bmod \wp F$.

Let P_0 be the point of reference. Hasse's first normalization process replaces z by an element which has P_0 as its only pole; this can be achieved by the so-called "strong approximation theorem". The second process replaces z by an element whose pole order at P_0 is p (while still there is no pole of z other than P_0). This can be done because the genus of F is 1 and therefore, for every $r > 1$ there exist elements which have P_0 as their only pole, and of order r.

This being done, there is still the condition that for P_0 there exists $z_{P_0} = z - \wp(w)$ such that $v_{P_0}(z_{P_0}) \geq 0$. Since the pole order of z at P_0 is p, it follows that the pole order of w at P_0 is 1 (of course w has other poles as well). Hence, if u is any uniformizing variable at P_0 we may write $w = \frac{c}{u}$ with some $0 \neq c \in K$ and we obtain

$$z = \frac{c^p}{u^p} - \frac{c}{u} + \cdots \tag{45}$$

as the Laurent series expansion of z at the point P_0, where the dots represent terms of higher order. We see:

Every unramified extension $E|F$ of degree p can be generated by an Artin-Schreier equation $\wp(y) = z$ where the radicand z has P_0 as its only pole, and a Laurent expansion of the form (45) *with $0 \neq c \in K$.*

The above construction shows that z is unique up to a substitution $z \mapsto az+b$ with $a, b \in K$ and $a^p = a$, i.e. $a \in \mathbb{F}_p$; hence $E|F$ is unique.

In the following let us take the uniformizing variable u as in the definition of the Hasse invariant A in (42). Now consider the differential $z\omega$. This has P_0 as its only pole, and has the Laurent expansion:

$$z\omega = \left(\frac{c^p}{u^p} - \frac{c}{u} + \cdots\right)\left(1 + Au^{p-1} + \cdots\right)\mathrm{d}u \tag{46}$$

$$= \left(\frac{c^p}{u^p} + \frac{c^pA - c}{u} + \cdots\right)\mathrm{d}u \tag{47}$$

Accordingly the residue of $z\omega$ at the pole P_0 is $c^pA - c$. But P_0 is the only pole of $z\omega$. Since the sum of all its residues vanishes it follows

$$c^pA - c = 0\,, \qquad \text{i.e.,} \qquad A = c^{-(p-1)} \neq 0\,. \tag{48}$$

Conversely, if $A \neq 0$ then choose c according to (48); define a differential by the expansion (47) with the specification that P_0 is the only pole of this differential; writing it in the form (46) as $z\omega$, this element z is the Artin-Schreier radicand of a cyclic unramified extension $E|F$. This proves the theorem formulated in section 4.1.

Remark: In the above argument Hasse had to use the "Theorem of the residues" which says that the sum of the residues of a differential of F vanishes. At the time of Hasse this theorem had not yet been established in the algebraic framework. Hence Hasse had to develop this himself; he did it in his 1934 paper on differentials. In particular he had to prove that the residue of a differential at a point P is independent of the choice of the local parameter. This of course was well known in characteristic 0 but in characteristic p there arose difficulties. Today we are used to the proof by specializing the assertion from characteristic 0 to characteristic p. This is an idea which Artin used to present in his lectures; however this was much later.[39] Hasse's proof was somewhat lengthy in characteristic p.

4.3.1 The Hasse-Witt matrix

Actually it is possible to avoid differentials and hence the theorem of the residues altogether, by defining the Hasse invariant A through the following property which is obtained in the way as explained above leading to the expansion (45):

Let u be any uniformizing variable at P_0. There exists an element $z \in F$ having P_0 as its only pole, with the Laurent expansion

$$z = \frac{1}{u^p} - \frac{A}{u} + \cdots \ . \tag{49}$$

z is uniquely determined up to an additive constant from K.

If $A \neq 0$ write $A = c^{1-p}$ with $c \in K$, then $c^p z$ is an Artin-Schreier radicand for an unramified cyclic extension of degree p.

In this form the invariant A can be defined quite generally for an arbitrary function field $F|K$ of genus $g > 0$, not as an element in F but as a $g \times g$ matrix. Thus is done in the joint paper of Hasse and Witt [HW36]. The paper appeared in 1936 but was submitted already on October 22, 1935. This was the time when Hasse was in the process of completing his Crelle papers (I)-(III) where, in the elliptic case, his above mentioned theorem on unramified cyclic extensions was used. We can imagine that he showed the manuscripts of his Crelle papers to his assistent Witt and asked him for proofreading and for his comments. And Witt, with his known gift for immediately seeing the essentials, pointed out the possibility of generalization. The new joint paper Hasse-Witt solved the same problem for function fields of arbitrary genus g. The rank $\gamma \leq g$ of the matrix $AA^p \cdots A^{p^{g-1}}$ equals the rank of the Galois group of the maximal abelian unramified extension $E|F$ of exponent p. This Galois group is isomorphic to the p-torsion of the Jacobian of F.

To prove this one has to develop a kind of semi-linear algebra for operators T which satisfy $T\alpha = \alpha^p T$. Today this is standard, and it is contained in the

[39] We do not know where in the literature this idea was first used.

calculus of the so-called Cartier operator. But in 1935 this was quite unusual. If we are not mistaken then we can allot this idea to Witt as his contribution.

4.4 The extreme cases

Consider the situation of the Riemann hypothesis. Thus there is given an elliptic function field F_q over the finite field $\mathbb{F}_q$ with q elements, and $F = F_q K$ is its constant field extension with the algebraic closure K of $\mathbb{F}_q$. And $\pi \in \mathsf{M}$ is the corresponding Frobenius meromorphism, which induces in F_q the exponentiation with q.

The "extreme cases" (*Grenzfälle*) of Hasse are those for which $\overline{\pi} = \pm\pi$; this means $\pi^2 = \pm q$. According to (1) and (2) this is equivalent to

$$N = \begin{cases} q+1 & \text{or} \\ q+1-2\sqrt{q} \end{cases} \tag{50}$$

where in the second case $q = p^{2r}$ has to be a square. Already in November 1933 Hasse had written to Davenport that these extreme cases can occur only when $A = 0$. In his Crelle paper (III) he gives a proof:

An extreme case occurs if and only if the Hasse invariant $A = 0$. *If* $A \neq 0$ *then* $0 < |N - q - 1| < 2\sqrt{q}$.

In fact, let μ_p denote the meromorphism which induces the multiplication with p. The relation $A = 0$ signifies that the field extension $F|F\mu_p$ is purely inseparable. Since this is of degree $\mathcal{N}(p) = p^2$ it follows $F\mu_p = F^{p^2}$. Repeating this for powers of p instead of p we obtain by induction: $F\mu_q = F^{q^2}$. On the other hand, $F|F\pi$ is purely inseparable of degree q, hence $F\pi = F^q$ and therefore $F\pi^2 = F^{q^2}$. Thus the two normalized meromorphisms π^2 and μ_q have the same image field. Hence they differ by a factor ε which is an automorphism of F. In the endomorphism ring M (where we have identified $\mu_q = q$) we obtain the relation $\pi^2 = \varepsilon q$, where $\varepsilon \in \mathsf{M}$ is a unit. If $\varepsilon \neq \pm 1$ then $\pi = \sqrt{\varepsilon q} \in \mathsf{M}$ would be of degree > 2 which is not the case. Thus $\pi^2 = \pm q$.

Remark: In [Has36d] Hasse says:

> Ist ... $\overline{\pi} \neq \pi$, so ist der Meromorphismenring M eine Ordnung eines imaginär quadratischen Zahlkörpers...
>
> *If ...* $\overline{\pi} \neq \pi$ *then the endomorphism ring* M *is an order in an imaginary quadratic number field ...*

And he uses the argument that every meromorphism μ commutes with π.

This, however, is not true in the extreme case if $\overline{\pi} = -\pi$. For, as we shall see below, Deuring has proved that whenever $A = 0$ then M is an order in a quaternion algebra. Hasse's argument is valid for those meromorphisms μ only, which are defined over $\mathbb{F}_q$ already, i.e., which map F_q into itself. For, the Frobenius operation π acts on F_q as the exponentiation with q. The meromorphisms which are defined over $\mathbb{F}_q$ form a subring of M, and it is obviously this subring which Hasse tacitly had in mind when he formulated his theorem above.

4.5 Summary

Given an elliptic curve in characteristic p, its p-torsion group is either cyclic of order p or it vanishes. This is equivalent to whether the function field admits precisely one cylic unramified extension of degree p, or no such extension. Already in November 1933 Hasse was aware of this dichotomy; he mentioned it in a letter to Davenport. The so-called Hasse invariant A of the curve regulates this behavior; A vanishes if and only if there is no cyclic unramified extension of degree p. Hasse published this theorem in 1934. By definition, A can be viewed as the first obstruction for the integration of the holomorphic differential on the curve. In the third 1936 Crelle paper Hasse showed that the vanishing of A signifies the presence of an "extreme case", which means that the conjugate $\overline{\pi}$ of the Frobenius endomorphism satisfies $\overline{\pi} = \pm\pi$.

If the endomorphism ring is non-commutative then $A = 0$, but Hasse did not know yet whether the converse also holds. This was verified later by Deuring (see section 6).

5 Some general comments

Hasse's work on elliptic function fields culminated in his three Crelle papers (I)–(III). He had started this work in December 1932 after his conversation with Artin in Hamburg; see Part 2. Since then (from 1933 to 1936) Hasse published 15 papers on the theory of function fields, mostly for the elliptic case but some of them in more generality paving the way for the investigation of function fields of higher genus. The guiding line was to establish the necessary tools for the proof of the Riemann hypothesis, first for the elliptic case, and with the hope to obtain a proof also for higher genus. But the final aim of Hasse was not only the Riemann hypothesis; in addition he wanted to provide a coherent framework in which to consider various other problems of "diophantine geometry"[40]. He had expressed this very clearly in his Oslo talk at the Conference of the International Mathematical Union 1936.[41]

In this spirit Hasse wished to clarify the complete structure of the endomorphism rings of elliptic function fields in characteristic p, even if this would not all be necessary for the proof of the Riemann hypothesis. We have said this before already. But now we observe that he did not complete his program. It is true that in his last Crelle paper (III) he had already some results, namely the theorem mentioned in section 3.1 with the list of the three possible types for the structure of an endomorphism ring. Hasse noted that all of those three types do occur. But a more detailed investigation about which of these types

[40] This is today's terminology; in the 1930s this terminology did not yet exist. Hasse envisaged the theory of function fields, or curves, over base fields which carry an arithmetic structure, e.g., number fields, p-adic fields or finite fields.

[41] See [Has37b]. In his talk Hasse mentioned, among other things, the recent paper of Elisabeth Lutz on the structure of the group of rational points on an elliptic curve over a $\mathfrak{p}$-adic field. Lutz was a student of André Weil in Strasbourg. When Weil had informed him about her result (an announcement of which appeared in [Lut36]), Hasse was so delighted that he immediately offered publication in Crelle's Journal [Lut37]. Weil, in his letter of April 26, 1936 to Hasse, considered this as a sign of continued cooperation ("*ein Zeichen der fortgesetzten Zusammenarbeit*").

occur in given characteristic p and under which circumstances, was still missing. Hasse himself in his later publications never returned to these questions about the elliptic case.

Why not? We do not know. But one of the reasons, it seems to us, was his wish to concentrate his efforts towards the Riemann hypothesis for function fields of higher genus.

We conclude this from several remarks of Hasse in his letters. For instance, in a letter to Siegel dated December 19, 1935 Hasse wrote:

> Leider bin ich bei den abstrakten Funktionenkörpern vom Geschlechte $g > 1$ noch immer in Anfängen. Ich musste ja meine wissenschaftliche Tätigkeit von Mai 1934 an zunächst einmal gründlich unterbrechen und konnte erst in diesem Oktober wieder damit anfangen, meine Forschungen aufzunehmen.
>
> *Unfortunately I am still at the very beginnings with the abstract function fields of genus $g > 1$. For I had to interrupt my scientific activities since May 1934 and was able to start in October only to resume my research work.*

The reason for the interruption of his scientific activities was, of course, the chaotic and almost bizarre situation which Hasse had to face when he moved from Marburg to Göttingen in the summer of 1934. Due to the antisemitic policy of the German Nazi government the Mathematical Institute in Göttingen had lost many of its members, and with them its role and reputation as one of the flourishing mathematical centers in the world. The situation has been described in several articles: [Fre77], [Seg80], [Sch87], [Seg03].

One of the many obstacles which were put into Hasse's way in Göttingen was connected with Deuring's *habilitation.*

Emmy Noether had warmly recommended Deuring (e.g., in a letter from Bryn Mawr dated March 6, 1934; see [LR06]). Accordingly, Deuring was scheduled to have his *Habilitation* in Göttingen in December 1935. However, a position of *Dozent* for him was finally rejected by the Göttingen university faculty; this was due mainly to the dealings of Hasse's colleague Tornier in Göttingen who posed as a fervent Nazi and tried, for political reasons, whatever he could to counteract Hasse's plans if these were not in line with his Nazi ideology.[42] It seems that also Teichmüller was involved in this rejection (he had been a representative of the *Fachschaft*, the student organization which in those times was completely dominated by Nazi followers). We conclude this from a letter of Hasse to Deuring of June 11, 1936, when Hasse discussed the possibility of repeating the application for *Dozent* position in Göttingen. Hasse wrote that

[42] In the files of the German ministry (*Ministerium für Wissenschaft, Volksbildung und Erziehung*) we have found a 3-page opinion (*Gutachten*) on Hasse, signed by Tornier and dated May 2, 1935, in which he writes that Hasse is not able to fill the position of Director of the Mathematics Institute. For, Tornier writes, Hasse cannot understand the New Time ("*...hindert ihn sein Charakter und sein jüdischer Einschlag, die heutige Zeit zu verstehen*"). Tornier also criticized that Hasse had kept close contact to jewish mathematicians, in particular to Emmy Noether – and that Hasse had ordered a wreath to be placed on her coffin in the name of her Göttingen colleagues. (Emmy Noether had died on April 14, 1935.)

this would be possible, but that certain obstructions should be out of the way. He wrote:

> Es wäre insbesondere wünschenswert, daß dann von vornherein sicher steht, daß von der hiesigen Fachschaft kein Widerstand mehr ausgeht. Solange aber Herr Teichmüller noch hier ist, kann ich dafür keine Garantie übernehmen.
>
> *In particular it would be desirable that from the "Fachschaft" there will be no more objection. But as long as Mr. Teichmüller is still here, I cannot guarantee this.*

Deuring did not fit into the political picture which those "Fachschaft" people wished to establish among the *Dozenten* in Göttingen. Hasse was much disappointed ("*aufs Tiefste enttäuscht*") by these dealings which, for political reasons, did not allow him to get the best people to Göttingen. He wrote to van der Waerden on December 16, 1935: "*We have lost a battle.*"[43]

The rejection to promote Deuring had not been an isolated affair in Göttingen. We conclude this from a letter to Toeplitz dated already April 18, 1935 where Hasse had said:

> Was mich vielmehr bedrückt, ist die Tatsache, dass ich einerseits der mathematischen Welt gegenüber die Verantwortung für den Wiederaufbau Göttingens zu einem mathematischen Platz von Rang trage, mir aber andrerseits durch die bestehenden hochschulpolitischen Regelungen fast jeder entscheidende Einfluss auf die personelle Gestaltung hier genommen ist. Dies betrifft nicht nur die Besetzung der Ordinariate, sondern gilt in gleicher Weise für die Lehraufträge, Assistenten- und Hilfsassistentenstellen.
>
> *I am more downhearted by the fact that, on the one hand, I am carrying the responsibility toward the mathematical world for the reconstruction of Göttingen to a mathematical place of high ranking, but on the other hand I have got almost no decisive influence on whom to offer a position here, due to the present political regulations. This concerns not only the professors but also the lecturers, the assistents and postdocs.*

When Hasse mentions his "responsibility toward the mathematical world" then this can be seen as his reaction to the encouragement which he got from several quarters. Among the Hasse papers there are a number of letters expressing the hope that Hasse might answer the challenge and restore Göttingen to a leading mathematical place; let us mention only the names of some of the

[43] At that time Deuring held a position as assistant professor in Leipzig with van der Waerden. There had developed some external difficulties, from the political side, for Deuring to have his *Habilitation* in Leipzig, and so Hasse, in agreement with van der Waerden, had planned to follow Emmy Noether's recommendation to get Deuring to Göttingen. This explains why Hasse wrote the above cited letter on Deuring to van der Waerden. Actually, in the same letter Hasse proposed to van der Waerden a meeting so that they could talk about the situation and how to secure Deuring's future as a mathematician; it appears that Hasse did not wish to put his ideas in writing. That meeting took place on January 4, 1936.

senders: Hermann Weyl, Emmy Noether, Abraham Fraenkel, H. Rademacher and F. K. Schmidt. And there were more. All this caused Hasse to try and to put his energy towards the task to restore Göttingen as a mathematical center.

But from the beginning he (and his colleagues) had to realize that there existed a strong opposition and that this deprived Hasse of much time and energy. This had not remained unknown to the mathematical community, and it had led Toeplitz to inquire whether Hasse might perhaps consider a change from Göttingen to the University of Bonn. In answer to this Hasse wrote the letter from which we have cited above. In principle, Hasse wrote, he was willing to consider a change, in view of the reasons which he had stated in his above cited letter. Accordingly, Bonn tried hard to get Hasse but the ministry in Berlin did not agree.

We have mentioned all this in order to explain, to some extent, the reason why Hasse in 1936 had decided to quit his work on elliptic curves. After all he had been able to complete his proof of the Riemann hypothesis in the elliptic case, notwithstanding all those annoyances and hostilities which he had to cope with in Göttingen. He now wished to concentrate on his long standing project about the Riemann hypothesis for higher genus.

But the ball was taken up by Deuring. He published in the next years (1940-1943) four papers in which more detailed questions on elliptic function fields in characteristic p were treated, with complete and important results about the structure of their endomorphism rings. We do not know whether Hasse had directly proposed to Deuring to follow up on the theory of elliptic function fields which he (Hasse) had started. The correspondence file Hasse-Deuring as preserved in the Göttingen *Handschriftenabteilung* does not give any clue to this question. And so we rather tend to believe that this was not the case. After Deuring had found out that his general theory of correspondences was suitable to provide essential simplifications of Hasse's proofs in the elliptic case (see section 3.3), it seems to us quite natural that he tried to go ahead and settle the questions which were left open in Hasse's papers. And that is precisely what he did.

6 Deuring's contributions

6.1 Deuring

Let us briefly insert some biographic information about Deuring:

Max Deuring (1907–1984) had been a student of Emmy Noether who had called him "one of the best students" (in a letter to Hasse of November 13, 1929; see [LR06]). His book "*Algebren*" [Deu35], written under the guidance of Emmy Noether, appeared 1935 and became a classic. At that time he had already a number of other significant papers on algebraic numbers and on algebraic functions. He was considered to be one of the most promising young mathematicians in Germany at the time. Deuring had studied one year in Rome (1929/1930) and another year as a Rockefeller fellow in Yale with Ore (1932/1933). In 1935 he held a position at the University of Leipzig as assistant to van der Waerden.

In the foregoing section we have already reported that Hasse wished to get Deuring as *Dozent* to Göttingen but that this was unsuccessful. Nevertheless Hasse continued his contact with Deuring and supported him whenever he was able to. In 1938 Deuring got a position as *Dozent* at the University in Jena (where F. K. Schmidt held a professorship). His two papers on the algebraic theory of correspondences (1937/40) gave rise to a decisive turn in the direction towards the proof of the Riemann hypothesis for curves of arbitrary genus. But also for elliptic curves he provided essential contributions. Here we shall discuss those of his papers which we have mentioned in section 1.2. Later in his life, from 1950 on, he published more on elliptic curves: First an algebraic treatment of classical complex multiplication [Deu49], [Deu52], and then in several papers a comprehensive study of zeta functions of elliptic curves over number fields. We shall report on those papers elsewhere.

For more biographic information on Deuring see [Kne87], [Roq89].

6.2 The supersingular case

As above, $F|K$ denotes an elliptic function field with base field K algebraically closed of characteristic p.

It was Hasse who had discovered that for $p > 0$ the endomorphism ring M may be non-commutative. In his third Crelle paper 1936 he had given three possible structure types for M (see section 3.1). The third type III is when M is non-commutative, namely an order in a quaternion division algebra over $\mathbb{Q}$. Hasse comments on this as follows:

> Das Beispiel $p = 3$, $y^2 = x^3 - 2x - 1$ lehrt jedenfalls, dass der Typ III wirklich vorkommt.
>
> *The example* $p = 3$, $y^2 = x^3 - 2x - 1$ *shows that type* III *does in fact occur.*

But Hasse did not say more. The available evidence points to the conclusion that Hasse did not know much more about type III, besides this example and maybe some others.

Deuring, in his 1941 paper on endomorphism rings, gives a complete description of the elliptic fields whose endomorphism ring is non-commutative. Deuring calls these fields "*super-singular*". The motivation for this terminology is as follows:

In the classical case, when the base field is the complex numbers, any elliptic function field $F|K$ can be generated by an equation of Weierstrass form (37). The element

$$j = 12^3 \, \frac{g_2^3}{\Delta} \tag{51}$$

is called the *absolute invariant* of $F|K$. It is well known that $F|K$ is uniquely determined (up to isomorphisms) by j, and that every $j \in K$ is the invariant of some elliptic field $F|K$.

Now, in the classical case the invariant j was called "*singular*" if the endomorphism ring of the corresponding elliptic field F is an order in an imaginary quadratic field. From classical complex multiplication it was known that those singular invariants j are algebraic numbers, and they are abelian over the corresponding imaginary quadratic field. Thus they are very special complex numbers. Classically the terminology "singular" expresses the fact that these numbers are quite special, in contrast to the "general" case in which the endomorphism ring is $\mathbb{Z}$.

For characteristic $p > 0$, Deuring used essentially the classical terminology. He called an elliptic field $F|K$ (or its invariant j) "singular" if the endomorphism ring is an order in an imaginary quadratic field. But as pointed out above, in characteristic $p > 0$ the endomorphism ring may be even larger, namely non-commutative. These fields, or their invariants, are then somewhat more singular than the others, and so Deuring called them "supersingular".

This was the motivation for Deuring to introduce the word "supersingular".

As to the absolute invariant j of an elliptic function field of prime characteristic p, it is defined for $p > 3$ by the same formula (51) as above. Note that for $p > 3$ every elliptic function field $F|K$ admits a Weierstrass normal form (37). The definition of the invariant in characteristics $p = 3$ and $p = 2$ will be discussed below.

Now, in his second paper on correspondences 1940, Deuring had shown that if j is supersingular then the p-torsion Γ_p vanishes; see section 3.4.3. This in turn is equivalent to the vanishing of the Hasse invariant A; see section 4.1. But it was not yet clear whether, conversely, $A = 0$ would imply j to be supersingular. This is indeed the case, and it is one of various results which Deuring proved in his long 1941 paper on endomorphism rings.

Let us recall the definition (35) of the Hasse invariant A. Hasse was well aware of the fact that his abstract definition would be of no use if one could not compute his invariant A directly. In principle, of course, this can be done by computing the coefficients of the expansion (34). For this purpose, one has to start with an explicit expression of the holomorphic differential ω. Suppose for the moment that $p > 3$ so that F can be generated in the form $F = K(x, y)$ with x, y related by an equation in Weierstrass normal form (37). Then the holomorphic differential ω can be chosen in the form (38). Expanding this at the point at infinity with respect to the uniformizing variable $t = \frac{-2x}{y}$ we get the coefficients c_i in (34) as functions of the coefficients g_2, g_3 in (37). Now, Hasse in his 1934 paper on unramified cyclic extensions had stated that A can be put into the following form, where Δ denotes the discriminant and j the absolute invariant (51):

The Hasse invariant A defined by (35) *is of the form:*

$$A = \begin{cases} \Delta^{\frac{p-1}{12}} P(j) & \text{for} \quad p \equiv 1 \mod 12 \\ g_2\, \Delta^{\frac{p-5}{12}} P(j) & \text{for} \quad p \equiv 5 \mod 12 \\ g_3\, \Delta^{\frac{p-7}{12}} P(j) & \text{for} \quad p \equiv 7 \mod 12 \\ g_2 g_3\, \Delta^{\frac{p-11}{12}} P(j) & \text{for} \quad p \equiv 11 \mod 12 \end{cases} \tag{52}$$

where $P(X)$ is a polynomial, depending on p only, with coefficients in the prime *field $\mathbb{F}_p$, of degree at most equal to the exponent of Δ in the formula.*

But Hasse adds:

> Ich vermute, daß $P(X)$ immer genau von diesem Grade ist. Die vorstehenden Ausführungen lassen aber noch nicht einmal erkennen, ob $P(X)$ nie identisch Null ist.
>
> *I suspect that $P(X)$ is always of this degree. But the preceding arguments do not even show whether $P(X)$ is never identical zero.*

It is with this question that Deuring begins in his 1941 paper on endomorphism rings. In this paper he proves the following

Theorem:

1. *The relation $A = 0$ is not only necessary but also sufficient for j to be supersingular.*
2. *As conjectured by Hasse, the polynomial $P(X)$ in (52) has precisely the degree which is given by the exponent of Δ in the formulas (52), and its roots are different. Consequently, the number of supersingular invariants j equals that degree, plus one additional invariant in the cases $p \equiv 5, 7 \bmod 12$ and two additional invariants if $p \equiv 11 \bmod 12$ – these additional invariants corresponding to the cases $g_2 = 0$ (hence $j = 0$) and $g_3 = 0$ (hence $j = 12^3$) respectively.*
3. *Supersingular invariants j satisfy $j^{p^2} = j$, hence they are contained in $\mathbb{F}_{p^2}$, the quadratic extension of the prime field $\mathbb{F}_p$.*[44]
4. *If j is supersingular then the corresponding endomorphism ring M is isomorphic to a <u>maximal</u> order in $\mathbb{H}_{\infty,p}$, the quaternion division algebra which is ramified at ∞ and p only. Conversely, every maximal order in $\mathbb{H}_{\infty,p}$ appears as the endomorphism ring M for some supersingular invariant. If the prime divisor of p in M is principal then there is exactly one supersingular invariant j belonging to M, and j is contained in the prime field $\mathbb{F}_p$. If not, then there are exactly two such supersingular invariants j, they are contained in $\mathbb{F}_{p^2}$ and they are conjugate to each other.*
5. *The number of supersingular invariants equals the class number of $\mathbb{H}_{\infty,p}$.*

In addition, Deuring writes down an explicit formula for the polynomial $P(j)$ which, he says, is useful to compute the values of the supersingular invariants for small p.[45] In fact, his paper contains a list of all supersingular invariants for primes $p < 100$.[46]

These results on the supersingular case are very precise and complete. Although in our discussion we had assumed $p > 3$, it turns out that the theorem

[44] Ogg has proved that there are precisely 15 primes for which all supersingular invariants are contained in $\mathbb{F}_p$ already: $2 \leq p \leq 31$ and $p \in \{41, 47, 59, 71\}$. See [Ogg75] and also [Mor07].

[45] The investigation of those polynomials for the supersingular invariants has produced a number of highly interesting papers, some of them connecting to the theory of modular forms. See, e.g., the list of references in [Mor06]. I would like to thank Patrick Morton for pointing out to me that those papers arose from the interest generated by Deuring's paper. In particular the question of determining directly the number of roots of $P(j)$ was solved, which Deuring could solve only indirectly by means of Eichler's class number formula for quaternions [Eic37].

[46] In the paper [BM04] the authors state that they have checked the entries in Deuring's table and found only two errors, for $p = 73$ and 97.

holds also in characteristic $p = 3$ and $p = 2$, except of course its second section which refers to the Weierstrass normal form (37). The definition of the invariant j for $p = 2$ and $p = 3$ is as follows:

Classically, besides the Weierstrass normal form there is another normal form, called Legendre's, which is as follows:

$$y^2 = x(x-1)(x-\lambda) \qquad \text{with} \qquad \lambda \neq 0, 1\,. \tag{53}$$

Then

$$j = 2^8 \frac{(1-\lambda(1-\lambda))^3}{\lambda^2(1-\lambda)^2} \tag{54}$$

This works also in all prime characteristics $p \geq 3$.

Referring to the Legendre normal form, Deuring gives a formula for the computation of the Hasse invariant A by means of the parameter λ, namely:

$$A = (-1)^{\frac{p-1}{2}} \sum_{0 \leq i \leq \frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \lambda^i\,. \tag{55}$$

For $p = 3$ this reduces to $A = -(1+\lambda)$ and we see that this vanishes for $\lambda = -1$ only which gives $j = 0$ in characteristic 3. And so in characteristic 3 there is only one supersingular invariant, $j = 0$. This belongs to the example which Hasse had found in characteristic 3; we have mentioned this above already.

In characteristic 2 the situation is quite different. Before Deuring there did not exist a definition of an absolute invariant j of an elliptic function field F of characteristic 2. The difference to characteristic $\neq 2$ can be explained as follows:

Since $F|K$ is elliptic, i.e., of genus 1, there exists $x \in F$ whose pole divisor is P_0^2. Recall that P_0 denotes the point of reference, which however can be arbitrarily chosen. x is unique up to a linear transformation $x \rightarrow ax + b$ with $a, b \in K$ and $a \neq 0$. We have $[F : K(x)] = 2$. If the characteristic is $\neq 2$ then F is generated over $K(x)$ by an element y with $y^2 \in K(x)$. After suitable normalization we have $y^2 = f(x)$ where $f(x) \in K[x]$ is a polynomial. Since F is of genus 1 it is seen that $f(x)$ is of degree 3 with three distinct roots. After a linear transformation of x this leads either to the Weierstrass normal form in characteristic $\neq 3$ (where the coefficient of x^2 in $f(x)$ vanishes), or to the Legendre normal form (where two of the roots of $f(x)$ are 0 and 1.) However, if the characteristic is $p = 2$ then F cannot be generated as above; instead we have to use an Artin-Schreier equation $y^2 - y = f(x)$.

Accordingly, for characteristic 2 Deuring in [Deu41b] obtains the normal form

$$y^2 - y = jx^2 + \frac{1}{jx}\,, \tag{56}$$

and he defines the coefficient j which appears in this formula as the invariant; it is verified that $F|K$ is uniquely determined by j and vice versa. There is one exception, though, namely if $F|K$ is generated by the equation

$$y^2 - y = x^3 \tag{57}$$

in which case Deuring assigns to it the invariant $j = 0$.

Deuring also states a normal form which he first [Deu41b] claims to be valid for all characteristics but later [Deu47] has to admit that in characteristic 3 the case $j = 0$ has to be excepted:[47]

$$y^2 - y + \alpha\, xy = x^3 \qquad \text{with} \qquad \alpha^3 \neq -27\,. \tag{58}$$

For this he gives the expression

$$j = -\frac{\alpha^3(\alpha^3 + 24)^3}{\alpha^3 + 27}\,. \tag{59}$$

From this one can compute the Hasse invariant A and one finds $A = \alpha$ in characteristic 2, therefore $A = 0$ if and only if $\alpha = 0$, i.e., $j = 0$. Thus the only supersingular invariant in characteristic 2 is $j = 0$, which corresponds to the exceptional case (57) above.

6.3 Singular invariants

In his 1941 paper Deuring also treats *singular invariants* in characteristic p, i.e., those invariants whose endomorphism ring is an order in an imaginary quadratic field. Perhaps, from a systematic point of view, we should have reported about the singular case first before discussing the supersingular case. But we have decided to start with the supersingular case because those results are particularly interesting in view of the fact that non-commutative endomorphism rings do not appear in the classical case and hence represent new discoveries.

Deuring's results on singular invariants are as follows. Recall that $F|K$ is assumed to be an elliptic function field of characteristic $p > 0$ with the base field K algebraically closed. j denotes the absolute invariant of $F|K$ and M its endomorphism ring.

Theorem:

1. *j is singular if and only if $A \neq 0$ and j is absolutely algebraic (i.e., algebraic over the prime field $\mathbb{F}_p$).*
2. *If j is singular then the corresponding endomorphism ring M is isomorphic to an order in an imaginary quadratic field Σ with the following specifications: p splits in Σ into two different prime ideal factors, and the conductor of M is prime to p. Conversely, every order M of an imaginary quadratic field Σ with these properties appears as the endomorphism ring belonging to some singular invariant j in characteristic p. If h is the class number of M then there are precisely h singular invariants belonging to M.*
3. *Let $\mathfrak{p}$ denote one of the two prime ideal factors of p in M. If f is the order of $\mathfrak{p}$ in the class group of M (i.e., f is the first exponent such that $\mathfrak{p}^f$ is a principal ideal) then j is of degree f over the prime field, i.e., $\mathbb{F}_p(j) = \mathbb{F}_{p^f}$. The f conjugates of j are also singular invariants belonging to the same endomorphism ring M.*

[47] Silverman [Sil86] calls this the "Deuring normal form", whereas Husemöller [Hus04] speaks of the "Hessian family" of elliptic curves.

Recall that the conductor of M is defined to be the smallest positive number $m \in \mathbb{Z}$ such that every integer $\alpha \in \Sigma$ with $\alpha \equiv 1 \bmod m$ is contained in M. It is well known that M is uniquely determined by m, and consists of all integers $\alpha \in \Sigma$ which are congruent modulo m to some $a \in \mathbb{Z}$. The (fractional) ideals of M which are prime to the conductor form a group. The class group (modulo principal ideals) is finite, and its order is the *class number h*.

Whereas in characteristic 0 *every* order in an imaginary quadratic field is the endomorphism ring of some elliptic function field, Deuring had discovered that in characteristic $p > 0$ this is not so. The restriction concerns the behavior of the characteristic p in M, and it is the result of Deuring's detailed study of the ℓ-adic representation of M, including $\ell = p$ when the representation is 1-dimensional.

The only remaining invariants in characteristic $p > 0$, i.e., those which are neither singular nor supersingular, are the transcendental ones. They are precisely those whose endomorphism ring $\mathsf{M} = \mathbb{Z}$.

6.4 Elliptic subfields

It is not possible here to give a detailed report on Deuring's proofs of the above cited two theorems. These proofs, although not particularly difficult, are somewhat roundabout and not straightforward. But we wish to present the main ideas of Deuring because they are quite remarkable, and also because they are essential tools for Deuring's further investigations concerning the algebraic foundation of of classical complex multiplication (starting 1949 in the *Hamburger Abhandlungen* [Deu49]).

One of those main ideas is to study the elliptic subfields of the given elliptic field F. (It is assumed that the subfields have the same base field K as does F.)

Recall that for $0 \neq \mu \in \mathsf{M}$ we have denoted by $F\mu$ the image of F under the normalized meromorphism μ. (See section 2.2.) Now, if $0 \neq \mathfrak{a} \subset \mathsf{M}$ denotes any left ideal, let $F\mathfrak{a}$ denote the field theoretic compositum of all $F\mu$ with $\mu \in \mathsf{M}$. This is an elliptic subfield of F. Deuring showed:

> *We have $[F : F\mathfrak{a}] = \mathcal{N}(\mathfrak{a})$. The Galois group of $F|F\mathfrak{a}$ consists of all translation automorphisms τ_P with P in the kernel $\Gamma_{\mathfrak{a}} \subset \Gamma$ of the ideal $\mathfrak{a}$. The endomorphism ring of $F\mathfrak{a}$ is the right order of $\mathfrak{a}$.*

Here $\mathcal{N}(\mathfrak{a}) \in \mathbb{Z}$ denotes the norm of the ideal $\mathfrak{a} \subset \mathsf{M}$. Since F may be inseparable over $F\mathfrak{a}$, the Galois group is to be interpreted as the Galois group of the maximal separable subextension. The right order of $\mathfrak{a}$ consists of all elements ρ in the quotient field of M for which $\mathfrak{a}\rho \subset \mathfrak{a}$.

These theorems exhibit a close relationship between the subfield structure of F and the ideal structure of its endomorphism ring M. Moreover:

> *If F is supersingular then* every *elliptic subfield of F is of the form $F\mathfrak{a}$ for some left ideal $\mathfrak{a} \subset \mathsf{M}$.*

This turns out to be the main reason for the validity of the theorem in section 6.2 in the supersingular case.

In the singular case there are more elliptic subfields. Note that every elliptic subfield $F' \subset F$ defines an *isogeny* from the curve Γ generating F to the curve Γ' for F'. The field F' is uniquely determined by the kernel Γ_0 of this isogeny, together with the degree of inseparability of $F|F'$. Γ_0 is a finite subgroup of Γ, and the translation automorphisms τ_P with $P \in \Gamma_0$ constitute the Galois group of $F|F'$. Conversely, given any finite subgroup $\Gamma_0 \subset \Gamma$, the translation automorphisms belonging to Γ_0 determine a subfield F' of F consisting of the elements fixed by those isomorphisms; this is an elliptic subfield of F, as well as any purely inseparable subfield of F'.

Based on these facts, combined with a detailed study of the ℓ-adic representations of M (including the p-adic representation for the characteristic p), Deuring shows:

> *Suppose F is singular, i.e., M is an order in an imaginary quadratic field Σ. If $F' \subset F$ then the endomorphism ring M' of F' is an order in the same field Σ. Conversely, any order M' of Σ is the endomorphism ring of some elliptic subfield $F' \subset F$ – provided that M' satisfies the condition set forth in the theorem of section* 6.3*, i.e., the conductor of M' is prime to the characteristic p.*

The above result is used by Deuring for the existence proof of singular elliptic fields F in characteristic p with prescribed endomorphism rings in a given imaginary quadratic field Σ. For, by the above result he needs only to construct an elliptic field F whose endomorphism ring is *some* order in Σ; then among its elliptic subfields there will appear one with the prescribed order. Of course, Σ has to satify the condition set forth in the theorem of section 6.3, namely that p splits in Σ in two different prime ideals. And the prescribed order has to have conductor prime to p.

6.5 Good reduction

In characteristic 0 it is well known from analytic uniformization that every order M in an imaginary quadratic field is the endomorphism ring of some suitable elliptic function field. One has to view M as a 2-dimensional lattice in $\mathbb{C}$ and then take F to be generated by that Weierstrass function $\wp(u)$ which has period lattice M, and its derivative $\wp'(u)$.

In characteristic p one has to assume that M satisfies the specifications set forth in the theorem stated in section 6.3. But there is no direct way of proving the existence of an elliptic field F with a given such M as its endomorphism ring – except to construct F as a reduction of a suitable function field in characteristic 0. In order to be able to do this, Deuring had to establish the necessary tools from the theory of good reduction.

More precisely, he had to *develop* the theory of good reduction since until that time no systematic way of reducing curves was known. It is true that Hasse in his first proof used the idea of lifting an elliptic curve in characteristic p

suitably to characteristic 0 and then studying the behavior of the lifted curve by reducing it again. But he had no general theory of reduction at his disposal; therefore he had to check directly every detail in the reduction process. Since he relied on explicit computations with generating equations, this resulted in several restrictions which he had to impose, e.g., the characteristic should be $p > 3$, and the invariant j of the elliptic curve should have odd degree over $\mathbb{F}_p$. (See Part 2, section 5.3.) But also in Hasse's second proof which works solely in characteristic p, he had to use several constructions which today we would subsume under the theory of good reduction. (See section 2.2.) The same holds for Deuring's proofs in his general theory of correspondences [Deu37].

Now, Deuring wished to systematize those arguments through a general theory of good reductions; he did it in his 1942 paper [Deu42]. Although that paper appeared one year later than his 1941 paper on endomorphism rings, it was completed at the same time, and Deuring relies on it in his 1941 paper. What are the main results which Deuring had achieved?

Deuring's theory of good reduction refers to the following situation: Given an algebraic function field $F|K$ (or curve) whose base field K is equipped with a prime $\mathfrak{p}$, i.e., valuation, or place. Deuring assumed that the valuation is discrete but a straightforward check shows that this assumption is not really necessary. $\mathfrak{p}$ can be any valuation, or place, in the general sense of Krull. Accordingly we may keep our general assumption that the base field K is algebraically closed whereas Deuring, working with discrete valuations only, often has to perform a finite extension of the base field in order to ensure the validity of his argument. The residue map (place) of K belonging to $\mathfrak{p}$ is denoted by $z \mapsto z\mathfrak{p}$. We also write $\overline{z}$ instead of $z\mathfrak{p}$.

Suppose that $\mathfrak{p}$ can be extended to a place $\mathfrak{P}$ of F with the following properties:

1. The residue field $\overline{F} = F\mathfrak{P}$ is an algebraic function field with base field $\overline{K} = K\mathfrak{p}$.
2. There exists a separating element $x \in F$ such that $\overline{x} = x\mathfrak{P}$ is transcendental over $\overline{K}$ and $[\overline{F} : \overline{K}(\overline{x})] = [F : K(x)]$.
3. The genus of $\overline{F}$ equals the genus of F.[48]

In this situation $\overline{F}|\overline{K}$ is called a "good reduction" of $F|K$ at $\mathfrak{p}$. Actually, Deuring did not use the terminology of "good reduction" which was introduced later. Deuring spoke of a "regular reduction", and $\mathfrak{P}$ was called a "regular extension" of $\mathfrak{p}$ to F. For a given $F|K$, almost all primes of K (i.e., all but the poles of finitely many elements) admit a regular extension to F. Deuring in [Deu42] did not yet know that the regular extension $\mathfrak{P}$ of $\mathfrak{p}$, if it exists, is unique (if the genus $g > 0$). For genus $g = 1$ he proved it later in [Deu55], and for arbitrary $g > 0$ this was shown by Lamprecht [Lam57].

If $\overline{F}$ is a good reduction of F in the above sense then this leads, according to Deuring [Deu42], to a "reduction map" of the divisor group $\mathcal{D}(F)$ to the divisor

[48] Recall that we have assumed K and hence $\overline{K}$ to be algebraically closed. Much of Deuring's theory remains true without this assumption; then one has to add the condition that $F|K$ and $\overline{F}|\overline{K}$ are conservative, i.e., their genus should be preserved under extensions of the base field.

group $\mathcal{D}(\overline{F})$ such that the relations between divisors, elements and divisor classes are preserved. In particular this means that integral divisors are mapped to integral divisors, the image of a divisor has the same degree as the divisor itself, principal divisors are mapped to principal divisors, etc. More precisely, if D is a principal divisor in $\mathcal{D}(F)$, say $D = (z)$ with $0 \neq z \in F$ then z can be normalized by a constant factor from K such that its residue $\overline{z} = z\mathfrak{P} \neq 0, \infty$, and then the image $\overline{D}$ of D equals the principal divisor $(\overline{z})$.[49]

This being said, Deuring in his 1941 paper on endomorphism rings shows in addition:

> *Suppose $F|K$ to be elliptic. Then:*
>
> (1) *$F|K$ admits good reduction at $\mathfrak{p}$ if and only if its absolute invariant j is $\mathfrak{p}$-integral, i.e., $j\mathfrak{p} \neq \infty$. If this is the case then the absolute invariant of $\overline{F}|\overline{K}$ is the image $\overline{j} = j\mathfrak{p} \in \overline{K}$.*
>
> (2) *If $F|K$ admits good reduction at $\mathfrak{p}$ then there is a natural isomorphism $\mu \mapsto \overline{\mu}$ of the endomorphism ring M of F into the endomorphism ring $\overline{\mathsf{M}}$ of $\overline{F}$ such that $\overline{\mu P} = \overline{\mu}\overline{P}$ for any point P of F and its reduction $\overline{P}$ of $\overline{F}$.*

M may be identified with its image in $\overline{\mathsf{M}}$ so that

$$\mathsf{M} \subset \overline{\mathsf{M}}$$

and the formula in (2) appears as

$$\overline{\mu P} = \mu\overline{P}\,.$$

$\overline{\mathsf{M}}$ may be larger than M. If F is singular then $\overline{F}$ is either singular or supersingular. If both F and $\overline{F}$ are singular then M and $\overline{\mathsf{M}}$ have the same quotient field Σ. If in addition M is a *maximal* order of Σ, then $\overline{\mathsf{M}} = \mathsf{M}$.

The following theorem can be used to lift an elliptic function field from characteristic p to characteristic 0.

Theorem:

> *As above, suppose K equipped with a place $\mathfrak{p}$ and residue field $\overline{K} = K\mathfrak{p}$. Let $\overline{F}|\overline{K}$ be a given elliptic field, and μ one of its endomorphisms. Then there exists an elliptic field $F|K$ admitting $\overline{F}|\overline{K}$ as a good reduction modulo $\mathfrak{p}$ such that its endomorphism ring M contains μ.*

In other words: The elliptic field $\overline{F}$, equipped with a given endomorphism μ, can be lifted from the residue field $\overline{K}$ to K.

This is an important result. It explains and systematizes Hasse's procedure in his first proof of the Riemann hypothesis (see Part 2). Consider the situation of the Riemann hypothesis, i.e., an elliptic curve defined over a finite field of

[49] Deuring's theory of good reduction was later generalized by Shimura [Shi55], in the framework of algebraic geometry to varieties of arbitrary dimension.

characteristic p. (see section 2.5). Hasse, in his first proof not yet being aware of the notion of Frobenius operator, succeeded somehow to lift the elliptic function field to characteristic 0 such that after lifting (and after suitable base field extension) p splits in the endomorphism ring $p = \pi\overline{\pi}$. Using class field theory and reduction modulo a prime divisor of p Hasse verified that this π has the properties which we now use to define the Frobenius operator.

The method of Hasse worked in the framework of the analytically based classical complex multiplication. In particular he used the so-called "invariant-equations" (meaning the algebraic equations between the invariants of different elliptic fields) which used to be a common tool in classical complex multiplication. Deuring also uses invariant-equations but he is able, by means of the above reduction theorems, to derive the relevant facts by purely algebraic means. This includes the so-called u-expansions of the roots of the invariant-equations, u being a suitable uniformizing variable at ∞. Deuring says in [Deu41a]:

> Die solchermassen aufgestellten u-Entwicklungen für die Wurzeln der Invariantenpolynome leisten für die Theorie der komplexen Multiplikation das gleiche wie die q-Entwicklungen (nach $q = e^{2\pi iw}$) in der analytischen Theorie. Es kommt also auf die Konvergenz der q-Entwicklungen gar nicht an. Die Galoissche Theorie der Invariantengleichungen kann mit Hilfe der u-Entwicklungen genau so behandelt werden wie mittels der q-Entwicklungen ...
>
> *The u-expansions as given above for the roots of the invariant-polynomials are useful in the theory of complex multiplication in the same way as the q-expansions (with respect to $q = e^{2\pi iw}$) in the analytic theory. Thus the convergence of the q-expansions is completely irrelevant. The Galois theory of the invariant-equations can be treated with the help of u-expansions in the same way as with the q-expansions ...*

And Deuring cites the third algebra volume by Weber [Web08] for the q-expansions. When he mentions "Galois theory" of the q-expansions then this is in fact the class field theory of complex multiplication.

Here we do not wish to go into more details of Deuring's work. We have included the above citation for two reasons: *First*, we want to point out again that for Hasse, Deuring and contemporaries, the algebra book by Weber had been a valuable and inspiring source. Through his book[50] Weber has exerted a decisive influence on the making of today's algebraic number theory. *Secondly*, we would like to recall that Hasse in his treatment of classical complex multiplication [Has26], [Has31] has based the whole theory on q-expansions, which in his setup remained the only analytically based tool. Now, Deuring had algebraized this too, and so the road was open to completely algebraize the classical theory of complex multiplication.

In fact, Deuring did this in two papers designed to match Hasse's two above cited papers. In the first paper [Deu49] in the *Hamburger Abhandlungen* he used the general class field theory, whereas in the second [Deu52] in *Mathematische*

[50] and, of course, through his many articles

Annalen he was able to *deduce* the class field theory of imaginary quadratic fields from the algebraic results of his paper [Deu41a].

By the way, Hasse himself had foreseen that through his algebraic treatment of complex multiplication it would eventually be possible to algebraize the whole classical body of analytically based complex multiplication. In his 1934 Hamburg lecture Hasse had said:

> Von der analytischen Theorie der elliptischen Funktionen ausgehend habe ich bereits vor einem Jahr ... einen Beweis der Riemannschen Vermutung in elliptischen Funktionenkörpern mit endlichem Konstantenkörper skizziert. Kurz gesagt, wurde dort die Riemannsche Vermutung aus dem Klassenkörperzerlegungsgesetz der durch die Teilwerte der elliptischen Funktionen gelieferten Relativkörper über einem imaginär-quadratischen Zahlkörper gefolgert. Hiernach ist es verständlich, dass ein Beweis dieser Riemannschen Vermutung auf algebraischer Grundlage umgekehrt auch zu einem Beweis jenes Klassenkörperzerlegungsgesetzes führt ... Überdies erscheint diese Schlussrichtung viel naturgemäßer.
>
> *Starting from the analytic theory of elliptic functions I have already last year ... sketched a proof of the Riemann hypothesis based on the class field decomposition law of extension fields of imaginary quadratic number fields, namely those extensions which are generated by the division values of the elliptic functions. From this viewpoint it is understandable that an algebraically based proof of the Riemann hypothesis leads, in the other direction, to a proof of the said class field decomposition law ... Moreover, this kind of reasoning appears much more natural.*

This seems just a vision, for at the time of writing this Hasse had not yet worked out all details, as we have seen above. Finally it was Deuring who completed this project of Hasse's.

Later, Deuring's work was reformulated in the context of Chevalley's class field theory using "idèles". See [Bo66].

6.6 Summary

Originally, Hasse had wished to prove the Riemann hypothesis for curves over finite fields, of arbitrary genus. The motivation for this came from a discussion with Artin in December 1932; we have reported on this in Part 2. Hasse considered the elliptic case as the first step towards this goal; he was able to solve the problem in the elliptic case because of his detailed knowledge of classical complex multiplication. While writing down the proof he discovered that complex multiplication for elliptic curves can be developed in a purely algebraic manner, and that the Riemann hypothesis is immediate if enough is known about the structure of the endomorphism ring of the elliptic curve.

However, gradually there arose the wider project of a complete description of the structure of endomorphism ring – even if not all those details are necessary for the proof of the Riemann hypothesis. For some reason which we can *only guess, Hasse did not complete this project but stopped this line of investigation after the Riemann hypothesis was established in the elliptic case. But Deuring continued Hasse's project and gave a full classification of all possible endomorphism rings in characteristic p, and more. These results paved the way for the complete algebraization of classical complex multiplication and its class field theory. Hasse had already foreseen this possibility in his Hamburg lectures, but it was Deuring who had executed these ideas in full detail.*

References

[Art24a] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen I. (Arithmetischer Teil.). *Math. Zeitschr.*, 19:153–206, 1924. 13

[Art24b] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen II. (Analytischer Teil.). *Math. Z.*, 19:207–246, 1924. 13

[AS27] E. Artin and O. Schreier. Algebraische Konstruktion reeller Körper. *Abh. Math. Semin. Univ. Hamb.*, 5:85–99, 1927. 41

[AW45] E. Artin and G. Whaples. Axiomatic characterization of fields by the product formula for valuations. *Bull. Am. Math. Soc.*, 51:469–492, 1945. 13

[Beh35] H. Behrbohm. Über die Algebraizität der Meromorphismen eines elliptischen Funktionenkörpers. *Nachr. Ges. Wiss. Göttingen (2)*, 1:131–134, 1935. 10, 30

[BM04] J. Brillhart and P. Morton. Class number of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial. *J. Number Theory*, 106:79–111, 2004. 51

[Bo66] A. Borel and others. *Seminar on complex multiplication. Seminar held at the Institute for Advanced Study, Princeton, N.J., 1957-58.*, volume 21 of *Lecture Notes in Mathematics.* Springer, 1966. IV, 102 pp. 59

[BR36] H. Behrbohm and L. Redei. Der Euklidische Algorithmus in quadratischen Körpern. *J. Reine Angew. Math.*, 174:192–205, 1936. 30

[Cea96] S. S. Chern et al. Wei-Liang Chow 1911–1995. *Notices Am. Math. Soc.*, 43(10):1117–1124, 1996. 5, 8

[CN35] C. Chevalley and H. Nehrkorn. Sur les démonstrations arithmétiques dans la théorie du corps de classes. *Math. Ann.*, 111:364–371, 1935. 5

[CW34] C. Chevalley and A. Weil. Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers. *Abh. Math. Semin. Univ. Hamb.*, 10:358–361, 1934. 5

[Dav36] H. Davenport. The meromorphisms of an elliptic function field. *Proc. Cambridge philos. Soc.*, 32:212–215, 1936. 10, 31, 32

[Deu35] M. Deuring. *Algebren.* Erg. d. Math. u. ihrer Grenzgebiete. Julius Springer, Berlin, 1935. 143 pp. 37, 48

[Deu37] M. Deuring. Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper. I. *J. Reine Angew. Math.*, 177:161–191, 1937. 11, 34, 35, 56

[Deu40] M. Deuring. Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper. II. *J. Reine Angew. Math.*, 183:25–36, 1940. 11, 24, 32, 34, 35

[Deu41a] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Semin. Univ. Hamb.*, 14:197–272, 1941. 11, 58, 59

[Deu41b] M. Deuring. Invarianten und Normalformen elliptischer Funktionenkörper. *Math. Z.*, 47:47–56, 1941. 11, 52, 53

[Deu42] M. Deuring. Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers. *Math. Z.*, 47:643–654, 1942. 11, 22, 56

[Deu47] M. Deuring. Zur Theorie der elliptischen Funktionenkörper. *Abh. Math. Semin. Univ. Hamb.*, 15:211–261, 1947. 11, 53

[Deu49] M. Deuring. Algebraische Begründung der komplexen Multiplikation. *Abh. Math. Semin. Univ. Hamb.*, 16(1/2):32–47, 1949. 49, 54, 58

[Deu52] M. Deuring. Die Struktur der elliptischen Funktionenkörper und die Klassenkörper der imaginären quadratischen Zahlkörper. *Math. Ann.*, 124:393–426, 1952. 49, 58

[Deu55] M. Deuring. Die Zetafunktion einer algebraischen Kurve vom Geschlechte eins. II. *Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl.*, 1955:13–42, 1955. 56

[DH34] H. Davenport and H. Hasse. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *J. Reine Angew. Math.*, 172:151–182, 1934. 7

[DW82] R. Dedekind and H. Weber. Theorie der algebraischen Funktionen einer Veränderlichen. *J. Reine Angew. Math.*, 92:181–290, 1882. 13

[Eic37] M. Eichler. Über die Idealklassenzahl total definiter Quaternionenalgebren. *Math. Z.*, 43:102–109, 1937. 51

[Fre77] G. Frei. *Leben und Werk von Helmut Hasse 1. Teil: Der Lebensgang.*, volume 37 of *Collection Mathématique, Série: Mathématiques pures et appliquées.* Université Laval, Québec, 1977. 59 pp. 46

[Fre06] G. Frei. *Gauss' unpublished Section Eight of the Disquisitiones arithmeticæ: The Beginning of the Theory of Function Fields over a Finite Field.* Nachrichten der Akademie der Wissenschaften zu Göttingen, II. Mathematisch-Physikalische Klasse. Vandenhoeck & Ruprecht, Göttingen, 2006. 71 pp. 14

[FS92] G. Frei and U. Stammbach. *Hermann Weyl und die Mathematik an der ETH Zürich, 1913-1930.* Birkhäuser, 1992. 181 pp. 8

[Has26] H. Hasse. Neue Begründung der komplexen Multiplikation I: Einordnung in die allgemeine Klassenkörpertheorie. *J. Reine Angew. Math.*, 157:115–139, 1926. 58

[Has30] H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. II: Reziprozitätsgesetz. *Jahresber. Dtsch. Math.-Ver.*, 6(Ergänzungsband), 1930. IV + 204 pp. 26

[Has31] H. Hasse. Neue Begründung der komplexen Multiplikation. II. Aufbau ohne Benutzung der allgemeinen Klassenkörpertheorie. *J. Reine Angew. Math.*, 165:64–88, 1931. 58

[Has32] H. Hasse. Zu Hilberts algebraisch–zahlentheoretischen Arbeiten. In *D. Hilbert, Gesammelte Abhandlungen.*, volume 1, pages 528–535. J. Springer, Berlin, 1932. 6

[Has33a] H. Hasse. Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Vorläufige Mitteilung. *Nachr. Ges. Wiss. Göttingen, Math.–Phys. Kl. I*, 1933(42):253–262, 1933. 7

[Has33b] 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. 37

[Has34a] H. Hasse. Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern. *Abh. Math. Semin. Univ. Hamb.*, 10:325–348, 1934. 6, 8, 9

[Has34b] H. Hasse. Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrad p über elliptischen Funktionenkörpern der Charakteristik p. *J. Reine Angew. Math.*, 172:77–85, 1934. 10

[Has34c] H. Hasse. Theorie der Differentiale in algebraischen Funktionenkörpern mit vollkommenem Konstantenkörper. *J. Reine Angew. Math.*, 172:55–64, 1934. 10

[Has34d] H. Hasse. Theorie der relativ–zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper. *J. Reine Angew. Math.*, 172:37–54, 1934. 10, 39, 41

[Has35] H. Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper. *Nachr. Ges. Wiss. Göttingen I. N.F.*, 1:119–129, 1935. 10, 17

[Has36a] H. Hasse. Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper der Charakteristik p. *J. Reine Angew. Math.*, 175:50–54, 1936. 10, 24

[Has36b] H. Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper. I. die Struktur der Divisorenklassen endlicher Ordnung. *J. Reine Angew. Math.*, 175:55–62, 1936. 10

[Has36c] H. Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper. II. Automorphismen und Meromorphismen. Das Additionstheorem. *J. Reine Angew. Math.*, 175:69–88, 1936. 10

[Has36d] H. Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper. III. die Struktur des Meromorphismenrings. *J. Reine Angew. Math.*, 175:193–207, 1936. 10, 32, 35, 44

[Has37a] H. Hasse. Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten. Nach einer brieflichen Mitteilung von F. K. Schmidt. *J. Reine Angew. Math.*, 177:215–237, 1937. 10, 24

[Has37b] H. Hasse. Über die Riemannsche Vermutung in Funktionenkörpern. In *C. R. du Congrès Internat. Math. Oslo 1936.*, volume 1, pages 189–206. 1937. 10, 33, 34, 45

[Has43] H. Hasse. Punti razionali sopra curve algebriche a congruenze. *Reale Accademia d'Italia, Fondazione Alessandro Volta. Atti dei Convegno.*, 9:85–140, 1943. 37

[Hey29] K. Hey. *Analytische Zahlentheorie in Systemen hyperkomplexer Zahlen.* Dissertation, Hamburg, 1929. 49 p. 4

[Hil99] D. Hilbert. Über die Theorie des relativquadratischen Zahlkörpers. *Math. Ann.*, 51:1–127, 1899. 6

[Hil02] D. Hilbert. Über die Theorie der relativ-Abelschen Zahlkörper. *Acta Math.*, 26:99–132, 1902. Mit geringen Änderungen abgedruckt aus den Göttinger Nachrichten 1898. 6

[HL02] K. Hensel and G. Landsberg. *Theorie der algebraischen Funktionen einer Variablen und ihre Anwendungen auf algebraische Kurven und abelsche Integrale.* Teubner, Leipzig, 1902. XVI 707 pp. 7, 25

[Hur86] A. Hurwitz. Über algebraische Korrespondenzen und das verallgemeinerte Korrespondenzprinzip. *Berichte v.d. sächsischen Gesellsch. d. Wissenschaften, mathematisch-physikalische Klasse.*, 1886:10–38, 1886. Wiederabdruck in Math. Ann. Bd.28 (1887) 561-585. 9

[Hus04] D. Husemöller. *Elliptic curves. With appendices by O. Forster, R. Lawrence, S. Theisen.*, volume 111 of *Graduate texts in Mathematics.* Springer, Berlin, 2 edition, 2004. XII + 400 pp. 53

[HW36] H. Hasse and E. Witt. Zyklische unverzweigte Erweiterungskörper vom Primzahlgrad p über einem algebraischen Funktionenkörper der Charakteristik p. *Monatsh. Math. Phys.*, 43:477–492, 1936. 10, 43

[Kne87] M. Kneser. Max Deuring 9.12.1907 - 20.12.1984. *Jahresber. Dtsch. Math.-Ver.*, 89:135–143, 1987. 49

[Lam57] E. Lamprecht. Zur Eindeutigkeit von Funktionalprimdivisoren. *Arch. Math.*, 8:30–38, 1957. 56

[Lan35] W. Landherr. Über einfache Liesche Ringe. *Abh. Math. Semin. Univ. Hamb.*, 11:41–64, 1935. 5

[LR06] F. Lemmermeyer and P. Roquette, editors. *Helmut Hasse and Emmy Noether. Their correspondence 1925-1935. With an introduction in English.* Universitäts–Verlag, Göttingen, 2006. 303 pp. 14, 46, 48

[Lut36] E. Lutz. Les solutions d'equation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques. *C. R. Acad. Sci., Paris*, 203:20–22, 1936. 45

[Lut37] E. Lutz. Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques. *J. Reine Angew. Math.*, 177:238–247, 1937. 45

[Man60] Yu. Manin. On cubic congruences to a prime modulus. *Am. Math. Soc., Transl., II. Ser.*, 13:1–7, 1960. Russian original 1950. 28

[Mor06] P. Morton. Explicit identities for invariants of elliptic curves. *J. Number Theory*, 120:234–271, 2006. 51

[Mor07] P. Morton. Ogg's theorem via explicit congruences for class equations. 2007. preprint. 51

[Neh33] H. Nehrkorn. Über absolute Idealklassengruppen und Einheiten in algebraischen Zahlkörpern. *Abh. Math. Semin. Univ. Hamb.*, 9:318–334, 1933. 5

[Ogg75] A. P. Ogg. Automorphisms de courbes modulaires. *Sèminaire Delange-Pisot-Poitou (Théorie des nombres).*, 1975(7), 1975. 51

[Roq89] P. Roquette. Über die algebraisch-zahlentheoretischen Arbeiten von Max Deuring. *Jahresber. Dtsch. Math.-Ver.*, 91:109–125, 1989. 49

[Roq02] P. Roquette. The Riemann hypothesis in characteristic p, its origin and development. Part 1. The formation of the zeta-functions of Artin and F. K. Schmidt. *Mitt. Math. Ges. Hamburg*, 21/2:79–157, 2002. 3

[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. 3, 22

[Sch31] F. K. Schmidt. Analytische Zahlentheorie in Körpern der Charakteristik p. *Math. Z.*, 33:1–32, 1931. 7, 12, 14

[Sch39] F. K. Schmidt. Zur arithmetischen Theorie der algebraischen Funktionen. II: Allgemeine Theorie der Weierstraßpunkte. *Math. Z.*, 45:75–92, 1939. 26

[Sch41] H. L. Schmid. Zur Meromorphismentheorie der elliptischen Funktionenkörper. *Math. Z.*, 47:399–421, 1941. 26, 33

[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. 46

[Seg80] S. Segal. Helmut Hasse in 1934. *His. Math.*, 7:46–56, 1980. 46

[Seg03] S. L. Segal. *Mathematicians under the Nazis.* Princeton University Press, Princeton, NJ, 2003. xxii, 530 pp. 46

[Sha57] I. Shafarevic. Exponents of elliptic curves. *Dokl. Akad. Nauk SSSR, n.S.*, 114:714–716, 1957. Russisch. 12

[Shi55] G. Shimura. Reduction of algebraic varieties with respect to a discrete valuation of the basic field. *American J. Math.*, 77:134–176, 1955. 57

[Sil86] J.H. Silverman. *The arithmetic of elliptic curves.*, volume 106 of *Graduate texts in Mathematics.* Springer, Berlin, 1986. XII + 400 pp. 53

[Söh35] H. Söhngen. Zur komplexen Multiplikation. *Math. Ann.*, 111:302–328, 1935. 5

[Sti93] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer, Berlin etc., 1993. X+260 pp. 41

[Tei36] O. Teichmüller. Differentialrechnung in Charakteristik *p*. *J. Reine Angew. Math.*, 175:89–99, 1936. 10, 24

[Web08] H. Weber. *Lehrbuch der Algebra. Dritter Band: Elliptische Funktionen und algebraische Zahlen.*, volume 3. Friedr. Vieweg u. Sohn, Braunschweig, 1908. XVI, 733 pp. 23, 25, 58

[Wit36] E. Witt. Referat über Behrbohms Artikel: Über die Algebraizität der Meromorphismen eines elliptischen Funktionenkörpers. *Zentralblatt für Mathematik*, 13(19801), 1936. 30

[Zas34] H. Zassenhaus. Zum Satz von Jordan-Hölder-Schreier. *Abh. Math. Semin. Univ. Hamb.*, 10:106–108, 1934. 6

[Zas37] H. Zassenhaus. *Lehrbuch der Gruppentheorie. Bd. 1.*, volume 21 of *Hamburg. Math. Einzelschriften.* B. G. Teubner, Leipzig, Berlin, 1937. VI, 152 pp. 6

[Zor33] M. Zorn. Note zur analytischen hyperkomplexen Zahlentheorie. *Abh. Math. Semin. Univ. Hamb.*, 9:197–201, 1933. 4