COMPUTABILITY IN PRINCIPLE AND IN PRACTICE IN ALGEBRAIC NUMBER THEORY: HENSEL TO ZASSENHAUS

by

Steven Andrew Kieffer

M.Sc., Carnegie Mellon University, 2007

B.Sc., State University of New York at Buffalo, 2003

A Thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Science

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Spring 2012

APPROVAL

Name:	Steven Andrew Kieffer
Degree:	Master of Science
Title of Thesis:	Computability in principle and in practice in algebraic number theory: Hensel to Zassenhaus
Examining Committee:	Dr. Jason Bell Chair
	Dr. Michael Monagan Senior Supervisor Professor
	Dr. Nils Bruin Supervisor Professor
	Dr. Tom Archibald Supervisor Professor
	Dr. J. Lennart Berggren Internal Examiner Professor
Date Approved:	16 April 2012

Partial Copyright Licence

Abstract

In the early years of algebraic number theory, different mathematicians built the theory in terms of different objects, and according to different rules, some seeking always to demonstrate that the objects were computable in principle. Later, prominently in the era in which electronic computers were becoming available for academic research, efforts were initiated by some to compute the objects of the theory in practice. By examining writings, research, and correspondence of mathematicians spanning these early and late computational periods, we seek to demonstrate ways in which ideas from the old tradition influenced the new. Among the connections we seek are personal influence on problem selection, and borrowing of computational methods. In particular, we examine such links among the works of Kurt Hensel, Helmut Hasse, Olga Taussky, and Hans Zassenhaus.

For Mom and Dad

"Wie man sich in der Musik nach der in heroischen und dämonischen Werken und in kühnsten Phantasien schwelgenden romantischen und nachromantischen Epoche heute bei aller Freude an diesem Schaffen doch auch wieder stärker auf den Urquell reiner und schlichter Musikalität der alten Meister besinnt, so scheint mir auch in der Zahlentheorie, die ja wie kaum eine andere mathematische Disziplin von dem Gesetz der Harmonie beherrscht wird, eine Rückbesinnung auf das geboten, was den großen Meistern, die sie begründet haben, als ihr wahres Gesicht vorgeschwebt hat."

— Helmut Hasse, 1945

Acknowledgments

I am grateful to my advisors Michael Monagan and Nils Bruin for sharing their expertise and enjoyment of computer algebra and number theory, for their careful comments and revisions, for the assignment to study Hensel's lemma, which has proved a more interesting topic than I ever expected, and for the gift of time in which to think about mathematics. I also thank my parents and friends for their support. Len Berggren generously gave his time to participate on the examining committee, and he and others in the department helped to make the history seminars interesting. Ideas from my former advisor Jeremy Avigad were surely at the back of my mind as I searched for interesting questions to ask about the methodology of mathematics. And finally, I would like to give very special thanks to Tom Archibald: for long discussions of historiographic questions, for a great deal of thoughtful feedback, for running the history seminars, and for his generous guidance and continual encouragement in the study and telling of history.

Contents

List of Tables

List of Figures

Preface

This thesis originated from the idea of studying Zassenhaus's use of Hensel's lemma for a polynomial factorization algorithm. If this seems a far cry from the resulting study, consider that polynomial factorization over the p-adics is central to Hensel's version of algebraic number theory, in its role in the definition of *prime divisors*. Consider furthermore that Hensel's factorization algorithm demonstrated computability mainly in principle, whereas Zassenhaus was concerned with practical factorization. From this starting point, the history examined here presented itself.

Chapter 1

Introduction

The subject of algebraic number theory, taught today with algebraic number fields $\mathbb{Q}(\alpha)$ as the central objects, and with unique factorization recovered through the theory of *ideals*, has been built and rebuilt since the early nineteenth century in terms of different objects, and according to different methodologies. We review the nature of these alternative approaches here, and in the process will encounter the major questions that we will be concerned with in this thesis.

In early work, such as P.G.L. Dirichlet's (1805 - 1859) studies on what we today call units in the rings of integers of number fields, [1] the notion was not that one was studying a collection called a "number field" but that one was simply studying the rational functions in a given algebraic number, i.e. expressions of the form

$$\frac{c_m\alpha^m + c_{m-1}\alpha^{m-1} + \cdots + c_0}{d_n\alpha^n + d_{n-1}\alpha^{n-1} + \cdots + d_0}$$

where the coefficients c_i and d_j were rational numbers, and where α was some fixed algebraic number, i.e. the root of a polynomial

$$a_k z^k + a_{k-1}z^{k-1} + \cdots + a_0$$

with rational coefficients.

Even after R. Dedekind (1831 - 1916) introduced the term *"Zahlkörper"* ("number field" in English) in 1871 [2], some, for example K. Hensel (1861 - 1941), persisted for at least a

[1] What is still today known as the Dirichlet Unit Theorem, though since Hilbert's *Zahlbericht* it has almost always been proved by the methods of Minkowski (1864 - 1909), was handled by Dirichlet in three papers, (Lejeune Dirichlet 1840, 1841, 1842).

[2] See (Dedekind 1930-1932a, p. 224) for Dedekind's introduction of the term *Körper* ("field"), in 1871.

little while longer in thinking in the way that Dirichlet had, i.e. simply in terms of rational functions of an algebraic number. [3] In this, Hensel was probably influenced by his teacher L. Kronecker (1823 - 1891), who did not believe that mathematics could legitimately deal with infinite completed totalities like *Zahlkörper*. For a time, Hensel teetered between the less popular framework of his doctoral advisor Kronecker, and the more popular Dedekindian viewpoint, for example opening a paper of 1894 with,

> Let x be a root of an arbitrary irreducible equation of nth degree with integral coefficients. All rational functions
>
> $$\xi = \varphi(x)$$
>
> of x with integral coefficients then form a closed domain ($\mathfrak{G}$) of algebraic numbers, a *Gattungsbereich* [4] in Kroneckerian, a field in Dedekindian nomenclature. [5]

Hensel eventually came to use Dedekind's notion of *Zahlkörper* himself (e.g. (Hensel 1904a, p. 66)), perhaps because it was expedient to use the same language that a majority of his intended audience wanted to use, or perhaps because he was not so philosophically strict as Kronecker. [6] Among Hensel's published papers, only seven mention the terms *Gattung* or *Gattungsbereich* in the title; the first of these was published in 1889, and the last in 1897, while overall, Hensel's publications run from 1884 to 1937. (See Figure 3.4 on page 73.) At least Kronecker's terminology, if not his conception of things, was still

[3] See for example (Hensel 1897c), in which Hensel retains this image of things. At the top of page 84, where x is a root of the polynomial $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n$, Hensel considers the arbitrary rational function $X = \varphi(x)$ in x, and notes that it satisfies an equation $F(X) = 0$ of the same degree n. The rational function X stands in place of an element in the number field $\mathbb{Q}(x)$, which we would today speak of instead, following Dedekind.

[4] The term *Gattung*, as used by Kronecker, has been translated as "species", in keeping with the Linnaean taxonomic terms like "class" and "order" which number theorists had been appropriating since Gauss. A *Bereich* in general is a "domain", so that e.g. an *Integritätsbereich* is an integral domain. By the term *Gattungsberich*, Kronecker meant a number field.

[5] (Hensel 1894, p. 61): *Es sei x eine Wurzel einer beliebigen irreductiblen Gleichung des n-ten Grades mit ganzzahligen Coefficienten. Alle rationalen Functionen*

$$\xi = \varphi(x)$$

von x mit ganzzahligen Coefficienten bilden dann einen in sich abgeschlossenen Bereich ($\mathfrak{G}$) *von algebraischen Zahlen, einen* Gattungsbereich *in* Kronecker*scher, einen Körper in* Dedekind*scher Bezeichnungsweise.*

[6] Petri writes (Petri 2011, p. 5) that after Kronecker's death Hensel relaxed his own claims regarding constructivity.

recalled by E. Hecke (1887-1947) [7] as late as 1923, but gradually awareness of Kronecker's framework seems to have faded from popular discourse.

As for the means by which to recover unique factorization, there is a great deal more variation. For a basic pedigree of nineteenth century methods, we can begin by naming those of Dedekind, Kronecker, Hensel, and E.E. Kummer (1810-1893), and we will say later how these methods relate to one another. There was also the approach of E.I. Zolotarev (1847 - 1878), who achieved a complete generalization of Kummer's theory to general number fields, using ideas almost identical with those Hensel would later publish. His treatise (Zolotarev 1880) was published posthumously and through an unfortunate reception never became widely known. [8] There is a method by E. Selling, [9] and there may be more still.

The basic problem, in today's language, is that in a number field such as $E = \mathbb{Q}(\sqrt{-5})$, the ring of integers may fail to have unique factorization. Following Dedekind, we define the ring of integers $\mathcal{O}_E$ in E to be the ring of all numbers $\alpha \in E$ whose minimal polynomial (defined to be monic) over $\mathbb{Q}$ has all integral coefficients. [10] For this particular field $\mathbb{Q}(\sqrt{-5})$ it is equal to the set of all $\mathbb{Z}$-linear combinations over the basis $\left\{1, \sqrt{-5}\right\}$. Irreducibility of a nonunit $\alpha \in E$ means that in any factorization $\alpha = \beta\gamma$ of α, at least one of the factors β, γ must be a unit. Each of the numbers 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ is integral in E (since their minimal polynomials are $x - 2$, $x - 3$, and $x^2 - 2x + 6$), and it can be shown easily (by considering norms) that each is irreducible in $\mathcal{O}_E$, so that in

$$6 = 2 \cdot 3$$
$$6 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right)$$

we have a failure of unique factorization: the number 6 can be factored into irreducibles in $\mathcal{O}_E$ in two distinct ways.

Starting not with a quadratic field such as we have considered in this example, but with cyclotomic fields $\mathbb{Q}(\alpha)$, α a primitive λ^{th} root of unity, λ a positive rational prime, Kummer invented a way to "save" unique factorization, which he presented in detail in a

[7] "Following Kronecker the term *domain of rationality* is also used in place of the term field." (Hecke 1981, p. 54), English translation of original (Hecke 1923).

[8] Piazza (Piazza 2007) explains the reasons for Zolotarev's obscurity – including unfavourable (and unjust) assessments by Dedekind and Kronecker – and also gives a summary of his methods.

[9] Selling is noted in (ibid., p. 455), and in (Bachmann 1905, p. 153).

[10] See (Edwards 1980, p. 332) on the origin of this definition.

paper of 1847. [11] The language of "saving" unique factorization is taken from a letter of 28 April 1847 from Kummer to Liouville, [12] and it is figurative; we must take a moment to understand properly what was actually done by each of Kummer, Dedekind, Kronecker, and Hensel.

What each of these mathematicians did, in his own way, was to provide a *correlate*, of some kind, for each integer in a number field, (i.e. to define a mapping from the integers of a number field to some other domain of objects) in such a way that for the entire system of these correlated objects there was indeed a kind of unique factorization, and such that an algebraic integer α would divide another, β, if and only if the correlate of α "divided" the correlate of β. In this way all questions of divisibility in the ring of integers of a number field could be decided on the grounds of divisibility in a separate domain of correlated objects, where unique factorization did hold. Kummer initially called these correlated objects "ideal complex numbers", and later "ideal divisors". In subsequent work of Dedekind, Kronecker, and Hensel, this name curiously would be split in half, Dedekind referring to his objects as "ideals", while Kronecker and Hensel would call their objects "divisors". [13]

In general, the correlated domain contained many more objects than just those that corresponded to algebraic integers. For one thing, in general the correspondence would be extended so that not just algebraic *integers* but all algebraic *numbers* (quotients of integers) would have a correlate; namely, an algebraic number α would be written as a quotient β/γ of two algebraic integers, and then the correlate assigned to α would be the quotient of those assigned to β and to γ. Beyond this, however, there could be still more elements in the correlated domain, which corresponded to no algebraic number whatsoever, and this "surplus" represented the failure of unique factorization in a very precise sense: there would be a surplus in the domain correlated to a number field E if and only if unique factorization failed in E. I stress that this language of correlation is mine, and that individual writers

[11] The detailed investigation was given in the paper (Kummer 1847b), which Kummer submitted to Crelle's journal in September 1846. He had already communicated a summary of his results to the Berlin Academy on 26 March 1846, according to Weil (Kummer 1975). The summary was reprinted as (Kummer 1847c), with the incorrect submission date of March 1845.

[12] Reprinted in (Kummer 1847a). Kummer wrote of the law of unique factorization for complex numbers built out of roots of unity that, "one can save it by introducing a new kind of complex numbers which I have named *ideal complex numbers*" (*on peut la sauver en introduisant un nouveau genre de nombres complexes que j'ai appelé* nombres complexe ideal). See (Edwards 1977, pp. 76-80) for discussion of the events surrounding the writing of this letter.

[13] Kummer's approach is examined by Edwards in (ibid.), and Kronecker's in (Edwards 1990).

held varying conceptions of what they were doing.

As for the pedigree of the methods of these four mathematicians, we receive different advice from different corners. H. Hasse (1898 - 1979), for one, would always speak of "the Kronecker-Hensel method of divisors". [14] H. Weyl (1885 - 1955), on the other hand, in his book (Weyl 1940) depicts Hensel's method as the natural extension of Kummer's method, not Kronecker's. To the present author, Weyl's picture seems to be the more accurate, although time has not permitted a proper study of Kronecker's basic work on number fields (Kronecker 1882), commonly referred to as "the *Grundzüge*." To be fair, Hensel's work does involve Kronecker's *forms*, to some extent, [15] but its defining characteristic, the use of p-adic numbers, seems to have its roots in Kummer. For the present discussion we will not try to settle this question, but will be satisfied to simply give a brief idea of the nature of each of the four methods. In Appendix A we demonstrate in depth how Hensel's theory can be viewed as a direct generalization of Kummer's.

Dedekind's method seems to be the one that has remained the most well-known to this day, probably because it is the one taught in most graduate courses in algebraic number theory. This at least seems the proximate cause, whereas the distal cause must be "Hilbert's reigning influence" (as Hasse would put it [16]) and his use of Dedekind's theory of *ideals* in his *Zahlbericht* (Hilbert 1897), which, according to Lemmermeyer and Schappacher, [17] "was the principal textbook on algebraic number theory for a period of at least thirty years after its appearance," and "has served as a model for many standard textbooks on algebraic number theory through the present day". Or consider Corry, who writes that,

> Since Hilbert basically adopted Dedekind's approach as the leading one, and since the *Zahlbericht* became the standard reference text for mathematicians working in algebraic number theory, the publication of this survey turned out to be a decisive factor for the consequent dominance of Dedekind's perspective over that of Kronecker within the discipline. (Corry 1996, p. 148)

Weyl too expressed similar sentiments in 1944 (ibid., p. 148), as have many others. [18] Considering this eventual outcome, it is surprising to learn that Dedekind complained in

[14] Cf. for example page 218.

[15] See for example (Hensel 1908) Chapter 10.

[16] See the foreword to (Hasse 1952).

[17] See their introduction to the English edition (Hilbert 1998) of Hilbert's *Zahlbericht*, p. XXIII.

[18] Ewald suggests that even some of the folklore surrounding number theory may have had its origin in

an 1876 letter to R. Lipschitz (1832-1903) that he had given up hope that his theoretical framework would in his time interest anyone but himself (Edwards, Neumann, and Purkert 1982, p. 52).

The *ideal*, at any rate, correlated to an algebraic number α is denoted (α) and is simply the set of all multiples of α with algebraic integers in the field in question. In general, ideals may be generated as the set of all linear combinations over any finite set of algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$, with the coefficients again being algebraic integers, and with such an ideal denoted $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Only those ideals that can be generated by a single number are called *principal*. These principal ideals are the ones correlated to actual algebraic numbers; the others are the "surplus" which represent the failure of unique factorization.

Dedekind defines the product of two ideals I and J to be the set of all finite sums $\sum \alpha_i \beta_i$ with the α_i in I and the β_i in J. With respect to this notion of multiplication, Dedekind defines prime ideals to be those that are divisible only by themselves and by the ideal (1), i.e. the entire ring of integers. He shows that ideals have unique factorization into prime ideals.

Meanwhile, from the sketchy image of Kronecker's theory that can be gleaned from a cursory inspection of his *Grundzüge*, together with hints from Weyl 1940, and especially Edwards's study (Edwards 1990), we may say a few things about Kronecker's theory of *divisors*.

Kronecker's approach is perhaps best understood by putting the failure of unique factorization in rings of algebraic integers into a different light. It can be expressed instead as the existence of pairs of integers $\alpha, \beta \in \mathcal{O}_E$ for which there is no greatest common divisor (GCD) in $\mathcal{O}_E$. This is equivalent to the failure of unique factorization, and it is in fact on the subject of greatest common divisors that Kronecker opens the second part of the *Grundzüge* (Kronecker 1882, p. 45), in the section immediately before the one in which he introduces *divisors* (ibid., p. 48).

Given algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$, whereas Dedekind would form the ideal $I = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ generated by these numbers, Kronecker instead forms a polynomial, or

---

the *Zahlbericht*. He notes the occurrence in the book's introduction of Kronecker's famous saying, "God created the integers while all else is the work of man" (*Die ganze Zahl schuf der liebe Gott, alles übrige ist Menschenwerk*) adding that, from here, "it would certainly have passed into general currency." (Ewald 2005, p. 942)

form, having the α_i as its coefficients, namely, the linear form

$$f(u_1, u_2, \ldots, u_n) = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$

where $u_1, u_2, \ldots, u_n$ are indeterminates. Immediately, the form f does appear to be in a certain sense equivalent to Dedekind's ideal I; if you allowed the indeterminates u_i to run over the ring of integers $\mathcal{O}_E$ then the set of values that the form f would take on would be precisely I. This already sounds like just the sort of alternative approach which we would expect Kronecker to prefer: instead of speaking of a completed infinite totality like I, we simply speak of a finite, symbolically representable form which in some way contains the same data.

The crux of Kronecker's approach is the result sometimes known as "Gauss's lemma". The *content* of a polynomial is defined to be the GCD of its coefficients, and Gauss's lemma states that the content of a product of two polynomials is equal to the product of their contents, taken individually. It is because of this that a form $\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$ can in a sense *stand in for* the GCD of $\alpha_1, \alpha_2, \ldots, \alpha_n$, even if there is not any actual number that is the GCD of these numbers. The multiplicativity of contents guaranteed by Gauss's lemma means that instead of multiplying GCDs we can multiply the forms that stand in for them. Out of this, an adequate theory of divisibility can be developed by working with such forms.

It is, moreover, a *computational* theory, in the following sense. If you are given two forms

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$

$$\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_m v_m$$

you can compute their product by hand, simply by multiplying the two forms together as you would multiply any polynomials, distributing and collecting terms. While it is true that you can do similarly with two ideals provided they are given by generating bases, Dedekind was not himself concerned with the fact; at least, this conclusion emerges from an appreciation of Dedekind's overall outlook. One can point to examples of objects in his theory for which Dedekind gave no way to compute a representation. One example is the intersection of two ideals, which serves as their least common multiple in his theory. He is satisfied to define it as the set-theoretic intersection, and leave it at that. He does not tell us how, given a basis

representation of each ideal, we can compute a basis representation of their intersection. [19] Another example is the *integral basis*, which we will review in detail in Chapter 2.

To Kronecker, on the other hand, it was of the essence of mathematics that we must be able to compute any object involved in the theory. In our group of authors, Dedekind was the odd man out in this respect, since Kummer and Hensel were also very computational. In Hensel we see the direct influence of his teacher Kronecker, for example when he begins his paper (Hensel 1904a) with the statement that only the positive whole numbers are given by nature, while zero, negative, fractional, irrational, and imaginary numbers are mere symbols, [20] or more significantly in that throughout his 349-page book (Hensel 1908) (*Theorie der algebraischen Zahlen*, henceforth TAZ) he consistently gives algorithms with which to compute the objects on whose existence his proofs depend. As for Kummer, his attitude seems to show through in an analogy he makes toward the end of the main paper (Kummer 1847b) in which he first introduced ideal divisors, where he compares number theory to chemistry, and prime factorizations to chemical formulae. In defining ideal divisors, he gives us a way to test for their presence, which he compares to the way in which chemical reagents are used to test for the presence of hypothetical radicals that cannot otherwise be isolated. Thus, for Kummer, number theory was to be like a natural science, where, for any postulated entity, there was a repeatable experiment you could run that would demonstrate its presence.

We may also consider Hasse's statement that,

> The sense that the explicit control of the subject in all its details should keep step with the general development of the theory was made known by Gauss, and later above all by Kummer in very pronounced terms. [21]

---

[19] This observation is made by Avigad, in (Avigad 2006, p. 173), who examines Dedekind's attitudes towards computability in depth. Dedekind defines the least common multiple of two modules in (Dedekind and Lejeune Dirichlet 1894) on page 498. Since ideals are modules, this is the definition that applies to them.

[20] (Hensel 1904a, p. 51): *In der Arithmetik sind die positiven ganzen Zahlen und nur sie durch die Natur gegeben; die Null, die negativen, die gebrochenen, die irrationalen und die imaginären Zahlen sind Symbole, welche man hinzugenommen hat, um in dem erweiterten Gebiete alle Rechnungsoperationen ausführen zu können.*

[21] (Hasse 1952, p. VII) *Der Sinn dafür, daß die explizite Beherrschung des Gegenstandes bis in alle Einzelheiten mit der allgemeinen Fortentwicklung der Theorie Schritt halten sollte, war bei Gauß und später vor allem noch bei Kummer in ganz ausgeprägter Weise vorhanden.*

and his reference to "Kummer's methods of proof, which were more computational, constructive, and hence easy to be carried out explicitly". [22] Here Hasse was comparing Kummer's methods to those of Hilbert (1862 - 1943), who would adopt Dedekind's ideal-theoretic approach with its lack of concern for computability, and would launch it into great popularity in his *Zahlbericht*.

It is about this difference in attitudes toward the importance of computability that we will be primarily concerned in this thesis.

When we set out to compare Kummer's methods with those of Dedekind, Kronecker, and Hensel, we must remember that there is a certain mismatch, in that he did not handle general number fields. In the seminal 1847 paper (Kummer 1847b), he introduced ideal divisors only for cyclotomic fields. His methods were nevertheless entirely computational, and contained in primitive form several key ideas of Hensel's method. We will now give a brief indication of the way in which the ideal prime divisors in Kummer's and Hensel's theories were defined with computability in mind. The concepts and notations that we use here are defined in Appendix A.

Kummer refers to algebraic numbers as "complex numbers". He starts with a complex root α of the equation $\alpha^\lambda = 1$, where λ is a fixed positive rational prime, and he considers all "complex numbers" of the form

$$\varphi(\alpha) = a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \cdots + a_{\lambda-1}\alpha^{\lambda-1}$$

where the a_i are rational *integers*. Thus, he really does not work in what we today know as the field $\mathbb{Q}(\alpha)$, but rather in what we know as its ring of integers [23] $\mathbb{Z}[\alpha]$. Questions of divisibility then are simply questions of the existence of a quotient in this ring.

Next Kummer fixes a primitive root γ mod λ, and a factorization $\lambda - 1 = e \cdot f$, and [24] he partitions all the imaginary roots of the equation $z^\lambda = 1$ into sums η_i which he calls *periods*,

[22] *...die mehr rechnerischen, konstruktiven und daher der expliziten Durchführung leicht zugänglichen Beweismethoden Kummers...* (Hasse 1952)

[23] It is *not* true for arbitrary algebraic numbers θ that the ring of integers of the field $\mathbb{Q}(\theta)$ is equal to $\mathbb{Z}[\theta]$, but this does hold if θ is a root of unity.

[24] The factors e and f do appear to be the "ancestors" of the conventional e and f that stand for the ramification index and inertia degree of Hilbert ramification theory, as still used today. There is one essential difference, which can be blamed on Kummer's case failing to contain "all the germs of generality", namely, that here e represents not the power to which an ideal prime divides a rational prime, but rather the number of distinct ideal primes dividing a rational prime.

in the following way:

$$\begin{aligned}
\eta_0 &= \alpha^{\gamma^0} + \alpha^{\gamma^e} + \alpha^{\gamma^{2e}} + \cdots + \alpha^{\gamma^{(f-1)e}} \\
\eta_1 &= \alpha^{\gamma^1} + \alpha^{\gamma^{e+1}} + \alpha^{\gamma^{2e+1}} + \cdots + \alpha^{\gamma^{(f-1)e+1}} \\
\eta_2 &= \alpha^{\gamma^2} + \alpha^{\gamma^{e+2}} + \alpha^{\gamma^{2e+2}} + \cdots + \alpha^{\gamma^{(f-1)e+2}} \\
&\vdots \\
\eta_{e-1} &= \alpha^{\gamma^{e-1}} + \alpha^{\gamma^{2e-1}} + \alpha^{\gamma^{3e-1}} + \cdots + \alpha^{\gamma^{fe-1}}.
\end{aligned}$$

The periods will play a central role in his methods, and he will speak of numbers formed out of them, rather than formed freely out of powers of α. In our modern language, Kummer is simply talking about numbers in the subring $R = \mathbb{Z}\eta_0 + \mathbb{Z}\eta_1 + \cdots + \mathbb{Z}\eta_{e-1}$ of the cyclotomic integers $\mathbb{Z}[\alpha]$. We will proceed to speak in these terms, although it should be understood that Kummer did not.

Kummer fixes a rational prime q of order f mod λ, i.e. satisfying the congruence

$$q^f \equiv 1 \bmod \lambda$$

but having no lower power congruent to 1 mod λ, and we will review now how it is that he introduces the *ideal prime divisors* associated with this rational prime. [25]

At the beginning of §3 of the 1847 paper, Kummer states a crucial component of his method which will turn out to be the same as Hensel's notion of a prime number χ in a q-adic completion of an algebraic number field (see Appendix A). Notably, he finishes his statement with the characteristic mark of the computationalist, a promise that we will not only demonstrate the existence of this important object, but will also show how to compute it:

> For the study of the prime factors of any given complex number it is very important to show that there are always such complex numbers, built out of periods, whose norm is divisible by q, but not by q^2; and to show as well how these complex numbers can be found. [26]

[25] The case $q = \lambda$ requires a special treatment, which we do not review here.

[26] *Für die Untersuchung der Primfactoren jeder gegebenen complexen Zahl ist es noch sehr wichtig, zu beweisen, daß es stets solche complexe, aus Perioden gebildete Zahlen giebt, deren Norm durch q theilbar ist, aber nicht durch q^2; und zugleich zu zeigen, wie diese complexen Zahlen gefunden werden können.* (Kummer 1847b, p. 333).

Indeed, by the end of the section Kummer constructs two numbers, such that in all cases one of them must have the property in question, i.e., that its norm be divisible exactly once by q. In a particular case, one could check effectively which of these two numbers had the desired property.

Taking ψ to be such a number, and $\psi, \sigma\psi, \sigma^2\psi \ldots, \sigma^{e-1}\psi$ its conjugates in $\mathbb{Q}(\eta_0)$, Kummer is ready to introduce the *ideal prime divisors* of the rational prime q. Whereas, as we have seen, the ideals that Dedekind would later introduce would be sets of numbers, and the forms that Kronecker would introduce would be polynomials, the ideal divisors introduced by Kummer were not built up in this way out of formerly known objects of any kind; they were instead entirely new objects. [27] For a rational prime q of order f mod λ, Kummer introduced precisely $e = (\lambda - 1)/f$ divisors, telling us nothing more about them than an explicit test for the power to which any one of them divides a given complex number.

The test was given in the following way. With N_0 the norm from $\mathbb{Q}(\eta_0)$ down to $\mathbb{Q}$, Kummer defined Ψ_i for $i = 0, 1, \ldots, e-1$ by

$$\Psi_i = \frac{N_0\psi}{\sigma^{e-i}\psi}.$$

Then he said there were e prime divisors of q, denoted [28] by $\mathfrak{q}_0, \mathfrak{q}_1, \ldots, \mathfrak{q}_{e-1}$, and any given complex number $\beta \in \mathbb{Z}(\alpha)$ would be called divisible by $\mathfrak{q}_i$ to precisely the μ power when

$$q^\mu | \beta\Psi_i^\mu \quad \text{but} \quad q^{\mu+1} \not| \beta\Psi_i^{\mu+1}.$$

We note that not only did Kummer show that it was possible to compute a number ψ with the required properties, but the test for divisibility by ideal prime divisors was an effective one too.

Finally we come to Hensel. His approach is applicable to an arbitrary algebraic number field $\mathbb{Q}(\alpha)$, and begins by factoring the minimal polynomial $m_\alpha(x)$ of α into irreducible factors over the field $\mathbb{Q}_q$ of q-adic numbers, for a fixed rational prime q. Hensel provides an algorithm in Chapter 4 of (Hensel 1908) with which to compute this factorization.

---

[27] In calling Kummer's ideal divisors new "objects" we are brushing over ontological questions. Were they really objects? Kummer never defined what they *were*, but only what it meant for a given number to be *divisible by them* to a certain power. To Dedekind this was unsatisfactory, and in the opening to (Dedekind 1996) he presented his ideals as being improvements over Kummer's divisors in that, to paraphrase, in mathematics it is better to deal with a thing that really is a thing. In this thesis we will not however be concerned with such ontological problems.

[28] Actually, Kummer did not denote them by any symbols at all. We introduce symbols here for clarity, and to emphasize the similarity with Hensel's approach.

If the factorization is

$$m_\alpha(x) = k_0(x)k_1(x)\cdots k_{e-1}(x) \quad (q)$$

(where the "(q)" on the right indicates that the equation holds in $\mathbb{Q}_q[x]$) then Hensel introduces e prime divisors $\mathfrak{q}_0, \mathfrak{q}_1, \ldots, \mathfrak{q}_{e-1}$ associated with the rational prime q. There is one corresponding to each irreducible factor $k_i(x)$.

Fixing a single $\mathfrak{q}$ among the $\mathfrak{q}_i$, and letting $k(x)$ be the irreducible factor of $m_\alpha(x)$ that it corresponds to, we will examine Hensel's definition of the power μ to which he will say that $\mathfrak{q}$ divides any given algebraic number $\beta \in \mathbb{Q}(\alpha)$. We will see that, as with Kummer, the number μ is computable.

Leaving the details to Appendix A, the definition runs thus: Let α_1 be any one of the roots of $k(x)$. Compute a *prime number* χ in the q-adic completion $\mathbb{Q}_q(\alpha)$ of the field $\mathbb{Q}(\alpha)$. (Hensel provides an algorithm to compute χ on pages 142 - 143 of (Hensel 1908).) If $\beta = \varphi(\alpha)$, then let $\beta_1 = \varphi(\alpha_1)$, and compute the χ-adic order of β_1. (Using the norm from $\mathbb{Q}_q(\alpha)$ down to $\mathbb{Q}_q$, this amounts to computing a quotient in $\mathbb{Q}_q$, for which Hensel provides an algorithm in Chapter 2 §3 of (ibid.).) Let this χ-adic order be μ. Then μ is the power to which $\mathfrak{q}$ is said to divide β.

In this brief overview we only hope to have indicated that every step of Hensel's definition is computable. The way in which his theory is a direct generalization of Kummer's is centred on the fact that Kummer's key number ψ turns out to play the role of Hensel's number χ, when $\mathbb{Q}(\alpha)$ is a cyclotomic field, i.e. the sort of field Kummer was working in. For a full demonstration of this fact, along with an exploration of other ways in which Kummer's theory contained p-adic notions in nascent form, we refer the reader again to Appendix A.

Having reviewed the methods of Kummer, Dedekind, Kronecker, and Hensel, we are now in a position to say which aspects of the history of algebraic number theory we will be interested in, and which not. Clearly the four methods we reviewed differ in many ways. For one, we can speak of *ontological* differences, i.e. differences concerning the sorts of objects that are introduced. In this regard, Kronecker gave us nothing new, only a new way to use polynomials, which are symbolic objects that can be written down on the page. Dedekind gave us various infinite sets, such as "number fields" and "ideals", which were new things in the mathematical universe, but were constructed as collections of old things which we already knew about. Depending on one's viewpoint, Kummer and Hensel either gave us entirely new objects called "divisors", or else they used no objects at all, but only defined a

certain divisibility condition. For us, the ontological questions of algebraic number theory, and the ontological preoccupations of various prominent figures in the field, will be only peripheral matters.

As we have mentioned already, our main concern will instead be the question of the importance that various practitioners of algebraic number theory have placed on *computability*. To be sure, these questions intersect with ontological questions, but they are not identical to them. In Kronecker and Hensel we see consistent efforts to demonstrate that all objects with which the theory is concerned can be computed. The algorithms provided for their computation, however, are in all but the simplest cases too lengthy to carry out. This suggests that the underlying *motivation* for demonstrating this *computability in principle* may have been in part an ontological one: philosophically, Kronecker believed that an object had to be constructable in order to exist, and as his student, Hensel followed him in this.

Later, in a definitive statement written in 1945, Hensel's own student Hasse would call programmatically for practical computational work in algebraic number theory, i.e. he sought *computability in practice*. In these published statements, appearing in the foreword to Hasse's monograph (Hasse 1952) [29] (*Über die Klassenzahl abelscher Zahlkörper*, henceforth KAZ), we find no trace of the ontological concerns of Kronecker. Instead, as we will see in Section 4.4, Hasse seeks only the understanding of and insight into the theory that can be gained through development of the ability to generate and manipulate numerical examples at will.

We find therefore that we are concerned with a certain trichotomy: We have one group of theorists, such as Dedekind and Hilbert, who seem to have been hardly concerned with computability at all, and we may call these *existentialists*, since their proofs generally concerned only the existence, not the computability of the relevant objects; we have another group of theorists, such as Kronecker and Hensel, who demonstrated persistent concern with computability, but were happy with any algorithm, no matter how slow and impractical, who we may call *computationalists in principle*, or *constructivists*; finally we have those practitioners like Hasse, *computationalists in practice*, who actually wanted to compute the objects of the theory readily enough to fill tables. Later on, we will see Olga Taussky (1906 - 1995) and Hans Zassenhaus (1912 - 1991) in this group, along with Hasse. For that matter, in Chapter 2 we will find signs of slight leanings toward practical computation even in Hensel.

[29] While the work was not published until 1952, the foreword was completed in 1945.

It is important however to recognize that, although we may speak about such "groups" of mathematicians, this is really just a convenient way to talk about certain approaches to mathematics. It is easier to talk about a certain way of doing things if we have an example of someone who often did things this way. A key word here, however, is "often", since at one time or another we are apt to find any given mathematician taking any given approach to mathematics. The researchers we have singled out here have done a great deal to represent one approach or another within algebraic number theory, and we do not claim more than that.

The trichotomy between existentialism and computationalism in principle or in practice is quite distinct from the dichotomy between what we may call the ideal-theoretic and the divisor-theoretic approaches to algebraic number theory. As we have seen, there is the risk of confusing these two distinctions, since in Kummer, Kronecker, and Hensel the importance of computability was wedded to the theory of divisors, while in Dedekind and Hilbert a de-emphasis on the same, replaced by a concern for the mere existence of objects, was paired with the theory of ideals.

It is interesting therefore to ask to what extent this pairing, computability with divisors, and existence with ideals, was essential, and to what extent it was merely accidental. Is there a characteristic feature of divisor theory that makes it better disposed to computing than the theory of ideals? On the face of it the easy answer seems to be 'yes'. Kummer and Hensel defined divisors precisely by giving *effective* tests to say the power to which they divide a given number. Ideals, meanwhile, are defined as infinite sets, and no such tests are given along with their definition. However, despite such considerations, from today's standpoint the theory of divisors and the theory of ideals are equivalent, being basically just two different languages in which to discuss the same facts about algebraic numbers and their divisibility relations. The result might be unwieldy, but in principle any algorithm from one theory can be translated into an algorithm for the other theory. In Weyl's words,

> As both theories are actually equivalent one can dissent about questions of convenience only. (Weyl 1940, p. 67)

For these reasons, we will have to keep our wits about us when we consider at length Hasse's statement in the foreword to KAZ, where he simultaneously champions the popular adoption of the divisor-theoretic approach of Kummer and Hensel over the ideal-theoretic approach of Dedekind and Hilbert, while he just as energetically promotes greater emphasis

on the "computational control" of the theory, as opposed to the mere development of theorems, or at least proposes that these two aspects of the development of the theory keep step with one another, instead of allowing the latter to outstrip the former. This will be our main task in Section 4.4, which stands as something of the climax of the history we intend to tell. It is a definitive statement by a highly influential number theorist, signalling a call for a transition from *computability in principle* to *computability in practice* in algebraic number theory (if not explicitly in these terms). It was published in 1952, at just around the time that electronic computers were becoming available for academic research, a fact of obvious significance for the development of computational branches of mathematics in general.

We may think of the thesis as being built around this central point. We have some work to do in Chapters 2 and 3 before we can get there. To begin with, in Chapter 2 we examine in depth the distinction between the *existence* and the *computability in principle* viewpoints, by means of an example. Namely, by examining the treatment of the *integral basis* as found in four different authors – Kronecker (1882), Dedekind (1894), Hilbert (1897), and Hensel (1908) – we will be able to see in a particular case what it means to approach the theory from one or the other point of view. Apart from providing us with the clarity of a concrete example, this will also give us a chance to delve into the structure of Hensel's TAZ, and to compare side by side one of his derivations with one of Hilbert's. Hensel's work will resurface in Chapter 6. Kummer is left out of the comparison this time, because in his examination of the rings $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\eta]$ he had no explicit need of "an integral basis," since with $\alpha, \alpha^2, \ldots, \alpha^{\lambda-1}$ he already had one.

A comparison with Hilbert, on the other hand, is an important prerequisite for Chapter 3, where we build a historical picture in which we can ground the significance of Hasse's statement in the foreword to KAZ. We must provide at least enough of a picture to answer two relevant questions, namely: (1) Who was Hasse?, and (2) How did he come to be a champion of the computational perspective? In order to address these questions we take the following steps: We begin with Section 3.1 on Hensel and Hilbert, which allows us to explore the popular reception of their respective viewpoints on the theory of algebraic numbers, and to see in what sense the computational side was the "underdog". This gives background to Hasse's somewhat polemical remarks. Next, we have Section 3.2 on the existence and construction of class fields, which allows us both to understand more about Hilbert's central role in the development of algebraic number theory in this period, and also to study a crucial element in the construction of class fields – the *singular primary number*

– which will resurface in Section 6.3 when we study a research problem initiated by Hasse and aimed at performing such constructions over particular base fields, like $\mathbb{Q}(\sqrt{-47})$. In Section 3.3 we consider the work of Hasse and Artin on reciprocity laws, in which we will see in particular Hasse's special interest in *explicit* reciprocity laws, i.e., in the problem of computing the functions that appear in the reciprocity equations. We finish the chapter with brief looks at the lives of Taussky and Zassenhaus before the war.

On the other side, after we have read in Section 4.4 about the practical computational program for algebraic number theory that Hasse envisioned in the foreword to KAZ, we must examine for one thing the ways in which his vision came into being, and for another thing the ways in which the words, thoughts, and deeds of Hasse, Hensel, Kronecker, Weyl, or others might have had influence on modern researchers, linking the old tradition of computability in principle to the new field focused on computability in practice. Accordingly, we will pick up in our last chapters with postwar mathematics, when electronic computing machines first became available. In the first sections of Chapter 4, we will consider a bit about computation prior to stored-program electronic computers, and a bit about the significance of Weyl's textbook.

In Chapter 5 we look into correspondence and collaboration in the 1950s between Hasse and Taussky, an algebraic number theorist who had access to the earliest of electronic computers in the U.S. We also consider a survey talk on the emerging field of computational algebraic number theory, which Taussky gave in 1953 at a symposium devoted to uses of the then very new electronic computers. Here we will see Taussky stating a key idea for the field, in which we can see a reemergence of Kronecker's image of things; namely, that if you want to compute with algebraic numbers, you can do so by computing with integer-coefficient polynomials modulo other such polynomials.

In Chapter 6 we take a look at the work of Zassenhaus in computational algebraic number theory in the 1960s, beginning with the collaboration with Taussky which first brought him into the subject, and moving on to a collaboration with Hasse, and finally to work in which Zassenhaus took a very impractical algorithm of Hensel, and put it to practical use. Temporally, this brings us to about 1969. In the final Chapter 7, we sketch some of the developments and activities in that year and the following few years, which helped to cement computational algebraic number theory as a field of research in its own right.

Overall, our goals in this thesis can be explained in the following way. Consider, to begin with, that while Kronecker had many students, Hensel is in some sense his most important

one, at least from the point of view of number theory, or the theory of algebraic functions. He was the principle champion of divisor theory after Kronecker; the later chapters of TAZ deal with forms, as in Kronecker's theory; Hensel called the natural numbers the only numbers given to us by nature, as Kronecker had; he was the editor of Kronecker's collected works; he even referred to himself as the *Hauptschüler* (principal student) [30] of Kronecker.

Similarly, among Hensel's students Hasse seems to have been the most important to him. It was through Hasse's doctoral thesis and the *local-global principle* established there that Hensel's p-adic approach to number theory won a place in popular thought, in that it was now of use in the solution of a problem in the popular subject of quadratic forms; [31] Hensel rejoiced when his chair at Marburg was filled by Hasse upon his retirement, the arrangement he had hoped for; [32] Hasse thought of his *Zahlentheorie* of 1949, as he wrote in its foreword, as the third book in the series begun by Hensel's two number theory textbooks, TAZ of 1908, and his own *Zahlentheorie* of 1913, and he called Hensel the book's "spiritual father".

For all these reasons, we come away with a sense that there was a "succession" of a kind, from Kronecker to Hensel to Hasse, in which among other things the mantle of Kronecker's very controversial, unpopular, and idiosyncratic outlook on mathematics would have been passed along. We get the sense that, since Kronecker favoured a computational approach to mathematics, and to number theory in particular, it is natural that Hensel and Hasse should have done so too.

Such is the picture we have of the main proponents in the beginnings of our subject of computational algebraic number theory, but what about the situation at the other end, when we find Zassenhaus coauthoring with Michael Pohst the 1989 textbook (Pohst and Zassenhaus 1989) which Henri Cohen has called "a landmark in the subject"? [33] There is no such academic lineage linking Hasse to Zassenhaus, who studied instead with Emil Artin (1898 - 1962).

Something we hope to reveal in this thesis is the extent to which Olga Taussky can be viewed as providing a link between Hasse and Zassenhaus. We will be careful not to overstate

[30] Noted in (Ullrich 1998, p. 168), and (Petri 2011, p. 13). Original source: (Hensel and Fraenkel 1927, p. 754).

[31] Edwards (Edwards 2008a), for example, writes that Hasse's work "established Kurt Hensel's p-adic numbers as indispensable tools of number theory". Hasse's doctoral results were published in (Hasse 1923).

[32] (Edwards 2008a)

[33] (Cohen 1993)

the case; Zassenhaus read Weyl and Hensel, and often cited them, and he collaborated directly with Hasse, so his influences may indeed have been many. But when we look for what we may call *transformative collaborative influences*, i.e. for cases in which through a collaboration the interests of one mathematician became the new-found interests of another – which in large part is the sort of relation that connects Kronecker, Hensel, and Hasse – we will find some evidence of such collaboration linking Hasse to Taussky, and again linking Taussky to Zassenhaus. One of the interesting themes in the history of mathematics is the question of what sort of mathematics people thought was valuable, or worth doing, and why; and one of the simplest answers we can find to the "why" question is that one researcher got another one interested in a subject. In Chapters 5 and 6 we will reveal significant influences linking Hasse, Taussky, and Zassenhaus.

In the same regard, we will have occasion, however brief, to consider Arnold Scholz (1904 - 1942), a little-known mathematician who died relatively young, but whose computational ideas influenced Taussky very early in her career, through their shared research.

Generally, whether it be through communication and collaboration between Hasse, Taussky, and Zassenhaus, or through Weyl's 1940 textbook, or through Hensel's TAZ, or through other channels, we hope to reveal some of the ways in which the computational side of algebraic number theory, which began with largely impractical algorithms, evolved through the dawn of the electronic computer into a very practical subject, which could serve to enlighten the inner visions of number theorists by providing copious numerical examples of, and new kinds of cognitive control over, the otherwise elusive objects their theory deals with.

Chapter 5 of the thesis consists of original research into primary sources, namely, the letters written between Hasse and Taussky which are preserved in Hasse's *Nachlass*. I thank the Niedersächsische Staats- und Universitätsbibliothek Göttingen for permission to quote from Cod. Ms. H. Hasse 1:296, 1:976, 1:985, 1:1410, 1:1696, 1:1911, and 1:1920 in this and other chapters of the thesis.

All translations from German in this thesis, whether from letters or from any publications, are, unless otherwise noted, my own.

Throughout the thesis we will refer repeatedly to certain important works. We list a number of them here in Table 1, and introduce abbreviations for some.

Abbrev.	Author	Title	Year
Zahlbericht	D. Hilbert	*Die Theorie der algebraischen Zahlkörper*	1897
RAZ	D. Hilbert	*Über die Theorie der relativ-Abelschen Zahlkörper*	1898
RQZ	D. Hilbert	*Über die Theorie des relativquadratischen Zahlkörpers*	1899
TAZ	K. Hensel	*Theorie der algebraischen Zahlen*	1908
	K. Hensel	*Zahlentheorie*	1913
Weyl 1940	H. Weyl	*Algebraic Theory of Numbers*	1940
	H. Hasse	*Zahlentheorie*	1949
KAZ	H. Hasse	*Über die Klassenzahl abelscher Zahlkörper*	1952
	H. Zimmer	*Computational Problems, Methods, and Results in Algebraic Number Theory*	1972
	M. Pohst and H. Zassenhaus	*Algorithmic algebraic number theory*	1989
	Henri Cohen	*A Course in Computational Algebraic Number Theory*	1993
	Henri Cohen	*Advanced Topics in Computational Number Theory*	2000

Table 1.1: Abbreviations for certain important works.

Chapter 2

The Integral Basis

Let F be a number field of degree n, and $\mathcal{O}_F$ its ring of integers (for basic definitions see Appendix A). An *integral basis* for F is a set $B = \{\omega_1, \omega_2, \ldots, \omega_n\}$ of n integers of F which span $\mathcal{O}_F$ over $\mathbb{Z}$. It is clear that the span of B over $\mathbb{Z}$ will be contained in $\mathcal{O}_F$ since the ω_i are integers; the problem is to choose the integers ω_i so that *all* of $\mathcal{O}_F$ is spanned. On page 3 we saw the example of the integral basis $\left\{1, \sqrt{-5}\right\}$ for the number field $\mathbb{Q}(\sqrt{-5})$, and as hinted in the footnote on page 9, another example of an integral basis is $\left\{1, \zeta, \ldots, \zeta^{\lambda-2}\right\}$ for the number field $\mathbb{Q}(\zeta)$, when ζ is a primitive λ^{th} root of unity, for λ a positive rational prime.

The integral basis is among the number field objects whose computation Zassenhaus declared as a part of his research program for computational algebraic number theory around 1959 (Pohst 1994, pp. 7-8). Hasse too mentioned it in 1945 as one of the important objects that we should be able to compute (see page 125) as did Taussky (see page 168) in 1953. Indeed, we can easily see why this is important for any computational approach to the subject of algebraic number theory. Every number in an algebraic number field can be represented uniquely as a $\mathbb{Q}$-linear combination over an integral basis, with the coefficients written in least terms. If we can compute this representation, then we can decide whether a number is an integer or not, by checking whether all the coefficients are rational integers. This is important for example in that it yields a divisibility test: β divides α if and only if the quotient α/β is an integer.

Considering the importance of having an actual integral basis in hand for a computational approach to algebraic number theory, in the following sections we will review the treatment of the integral basis in the works of Kronecker, Dedekind, Hilbert, and Hensel,

in search of insight into their various attitudes towards computability.

Before beginning, we review here a fundamental concept which has played a role in every version of algebraic number theory, and in particular tends to arise in connection with integral bases, namely, the concept of the *discriminant*. For basic concepts used below, such as minimal polynomials and conjugates, we refer to Appendix A.

The term "discriminant" is actually highly polymorphic, in that many different sorts of things can have a discriminant, namely:

- a polynomial $f(x)$;
- an algebraic number $\beta \in \mathbb{Q}(\alpha)$;
- a set of n algebraic numbers $\beta^{(1)}, \ldots, \beta^{(n)}$ in a number field $\mathbb{Q}(\alpha)$ of degree n;
- a number field $\mathbb{Q}(\alpha)$.

The discriminant of a polynomial $f(x)$ has slightly varying definitions in different authors, but is always equal to a constant multiple of the product

$$\prod_{i<j} (\alpha_i - \alpha_j)^2 , \tag{2.1}$$

where the α_i are the roots of $f(x)$. It can be computed by evaluating the *resultant* $R(f, f')$ (for definition see page 40), which is equal to

$$(-1)^{\frac{\mu(\mu-1)}{2}} \cdot A_0^{2\mu-1} \Delta,$$

where μ, A_0, and Δ are the degree, lead coefficient, and discriminant (2.1) of f, respectively. (See e.g. (Hensel 1908, p. 61).)

The discriminant of an algebraic number is just the discriminant of that number's minimal polynomial. Thus, if β_1 is an algebraic number, and $\beta_1, \ldots, \beta_n$ all its conjugates, then the discriminant of β_1 is equal to the product

$$\prod_{i<j} (\beta_i - \beta_j)^2 .$$

Given a set of n algebraic numbers $\beta_1^{(1)}, \beta_1^{(2)}, \ldots, \beta_1^{(n)}$ in a number field $\mathbb{Q}(\alpha)$ of degree

n, let

$$\begin{array}{c} \beta_1^{(1)}, \beta_1^{(2)}, \ldots, \beta_1^{(n)} \\ \beta_2^{(1)}, \beta_2^{(2)}, \ldots, \beta_2^{(n)} \\ \ldots\ldots\ldots\ldots \\ \beta_n^{(1)}, \beta_n^{(2)}, \ldots, \beta_n^{(n)} \end{array}$$

be all the conjugates in $\mathbb{Q}(\alpha)$. Then the discriminant of the set $\beta_1^{(1)}, \ldots, \beta_1^{(n)}$ is equal to the squared determinant

$$\begin{vmatrix} \beta_1^{(1)} & \beta_1^{(2)} & \cdots & \beta_1^{(n)} \\ \beta_2^{(1)} & \beta_2^{(2)} & \cdots & \beta_2^{(n)} \\ \vdots & \vdots & & \vdots \\ \beta_n^{(1)} & \beta_n^{(2)} & \cdots & \beta_n^{(n)} \end{vmatrix}^2 .$$

Notice that squaring the determinant means that the value of the discriminant is independent of the ordering of the conjugates.

Finally, the discriminant of a number field $\mathbb{Q}(\alpha)$ is the discriminant of any set of n numbers in $\mathbb{Q}(\alpha)$ that form an integral basis for $\mathbb{Q}(\alpha)$. For example, consider the quadratic number field $\mathbb{Q}(\sqrt{-19})$, which has the integral basis

$$\left\{1, \frac{1+\sqrt{-19}}{2}\right\}.$$

The discriminant of the field is therefore

$$\begin{vmatrix} 1 & \frac{1+\sqrt{-19}}{2} \\ 1 & \frac{1-\sqrt{-19}}{2} \end{vmatrix}^2 = -19.$$

As we will see in the following sections, the essential reason why discriminants are important when we talk about integral bases is that an integral basis for a field of degree n is characterized as any set of n integers in that field whose discriminant is in absolute value positive and as small as possible. (See e.g. (Hensel 1908, p. 117).)

2.1 Kronecker's *Grundzüge*, 1882

In Section 7 of his 1882 *Grundzüge*, Kronecker presents the idea of an integral basis, and shows how to compute one. Kronecker sought to treat in a unified way what we now call number fields and function fields, and in fact his discussion of the integral basis is given

explicitly for the case of a field of rational functions of one variable. He remarks at the end of the discussion however that the same method is applicable to the case of interest to us here, the number field case:

> I note furthermore that precisely the same deduction is applicable in the case $\mathfrak{R} = 1$, with the provision that, in place of the magnitude of the degree with respect to v, the magnitudes of the numbers themselves are used.... [1]

Kronecker refers to numbers and to rational functions of one or more variables collectively as *Grössen*, which we may translate as *quantities*, and to the fields that they form as *Gattungsbereiche*. Instead of what we call the degree of a field, Kronecker refers to the *Ordnung* or *order* of a *Gattungsbereich*. The "integers" in a *Gattungsbereich* – algebraic integers in the case of a number field, or polynomials in the case of a function field – are referred to collectively as *ganzen algebraischen Grössen*, or *whole algebraic quantities*.

For the sake of clarity, we abandon this terminology of Kronecker, in favour of modern counterparts. We also give his algorithm in terms of a number field rather than a function field, since our purpose is to compare and contrast his treatment with those of Dedekind, Hilbert, and Hensel.

We will present Kronecker's algorithm twice: in the first rendition we will stay true to his manner of presentation by neither adding nor taking away from his clarifications, reasons, or explanations. This is important in order to actually get a sense for Kronecker's style of mathematical exposition in the *Grundzüge*. Afterward, we will present the algorithm a second time, using matrices and hopefully making the process more clear. Kronecker's *Grundzüge* is a notoriously difficult and sketchy document, and some of this quality may come through in our first description of the algorithm. [2]

Kronecker presents his algorithm to compute an integral basis for a field K as follows. He starts from the assumption that we are given $n+m$ algebraic integers $x_1, x_2, \ldots, x_{n+m} \in \mathcal{O}_K$ whose integer linear combinations span $\mathcal{O}_K$, and explains in the following way a procedure

---

[1](Kronecker 1882, p. 20) *Ich bemerke noch, dass genau dieselbe Deduction für den Fall* $\mathfrak{R} = 1$ *mit der Maßgabe anwendbar ist, dass an Stelle der Grösse des Grades in Bezug auf* v *die Grösse der Zahlen selbst tritt....* By "the case $\mathfrak{R} = 1$," Kronecker meant the case of a number field.

[2]See for example (Edwards, Neumann, and Purkert 1982) for a review of Dedekind's notes on the *Grundzüge*, showing how Dedekind reacted to its sketchiness and sometimes inconsistent definitions. Also noted is the cautiously laudatory reaction of Weierstrass (ibid., p. 50), who felt the material was so dense and compressed that, at least for the time being, the work would be only admired, and not actually studied.

whereby a spanning set of just n elements can be computed:

1. Assume the x_i are so ordered that the discriminant d of $\{x_1, x_2, \ldots, x_n\}$ is smallest possible; that is, is less than or equal to that of any other set of n of the x_i.

2. Then $x_{n+1}, x_{n+2}, \ldots, x_{n+m}$ can be written as $\mathbb{Q}$-linear combinations of $x_1, x_2, \ldots, x_n$ whose coefficients have as denominator either d or a divisor thereof.

3. Then for $j = 1, 2, \ldots, m$ we can set x'_{n+j} to be equal to x_{n+j} plus a $\mathbb{Z}$-linear combination of $x_1, x_2, \ldots, x_n$ in such a way that x'_{n+j} is equal to a $\mathbb{Q}$-linear combination of $x_1, x_2, \ldots, x_n$ in whose coefficients the numerator is smaller than the denominator, and is nonzero.

4. Let the x_{n+j} now be replaced by the x'_{n+j}.

5. After this modification, through which the number of (nonzero) elements as well as the size of the discriminants may have decreased, let the elements – that is, the n first ones along with those of the last m which have remained (nonzero) – once again be ordered as above, namely, so that the discriminant of the first n is as small as possible.

6. If now the above procedure is applied again to the new system of elements, and then repeatedly applied, eventually the case must arise in which the first n elements – since their discriminant is already as small as possible – remain in place (i.e. are not displaced by any of the x'_{n+j}).

7. In this case the last m elements must all be zero. For suppose we had a nonzero x_{n+1}. Then when we wrote x_{n+1} as a $\mathbb{Q}$-linear combination of $x_1, x_2, ..., x_n$, there would have to be at least one coefficient c such that $0 < |c| < 1$. [3] Supposing this were the coefficient of x_1, then the discriminant of the n elements $x_2, x_3, \ldots, x_{n+1}$ would be less than that of $x_1, x_2, \ldots, x_n$.

Edwards gives an explanation of this algorithm in (Edwards 1990, pp. 69-70), but presents it in terms of his own version of Kronecker's *divisors*. (The *ideal divisors* invented by Kummer were replaced in Kronecker's theory by something he called *divisors*.)

[3] Speaking in terms of polynomials in v instead of algebraic numbers, Kronecker writes here that at least one coefficient must be of negative degree in v. Since he has already established that the denominator have greater degree than the numerator in the case of a nonzero coefficient, this simply means that the coefficient is nonzero.

We give a modified explanation here, in terms only of numbers (not using divisors), and employing matrices for clarity.

Kronecker's integral basis algorithm:

Input: Algebraic integers $\alpha_1, \alpha_2, \ldots, \alpha_{n+m}$ which span $\mathcal{O}_K$, where K is a number field of degree n.

Output: Algebraic integers $\beta_1, \beta_2, \ldots, \beta_n$ which span $\mathcal{O}_K$.

Step 1: Order the $\alpha_1, \alpha_2, \ldots, \alpha_{n+m}$ so that the discriminant d of $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is as small as possible.

Step 2: Compute an m-by-n matrix $C = (c_{ij})$ over $\mathbb{Q}$ such that

$$\begin{bmatrix} \alpha_{n+1} \\ \alpha_{n+2} \\ \vdots \\ \alpha_m \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}$$

Step 3: Let $[x]$ and $\{x\}$ denote the integer and fractional parts of a rational number x, respectively. Thus, for all $x \in \mathbb{Q}$ we have $x = [x] + \{x\}$, $[x] \in \mathbb{Z}$, and $0 \leq \{x\} < 1$. Define

$$\begin{aligned} \mathbf{y} &= \begin{bmatrix} \alpha_{n+1} & \alpha_{n+2} & \cdots & \alpha_{n+m} \end{bmatrix}^T \\ \mathbf{x} &= \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{bmatrix}^T \\ C_0 &= ([c_{ij}]) \\ C_1 &= (\{c_{ij}\})\,. \end{aligned}$$

Then we have

$$\begin{aligned} \mathbf{y} &= C\mathbf{x} \\ \mathbf{y} &= (\ C_0 + C_1\ )\,\mathbf{x} \\ \mathbf{y} - C_0\mathbf{x} &= C_1\mathbf{x} \end{aligned}$$

and we now define $\mathbf{y}' = \begin{bmatrix} \alpha'_{n+1} & \alpha'_{n+2} & \cdots & \alpha'_{n+m} \end{bmatrix}^T$ by

$$\mathbf{y}' \leftarrow \mathbf{y} - C_0\mathbf{x}.$$

So

$$\mathbf{y}' = C_1\mathbf{x}.$$

We observe that since we have

$$\left[\begin{array}{c} \mathbf{x} \\ \hline \mathbf{y} \end{array}\right] = \left[\begin{array}{c|c} I_n & 0 \\ \hline C_0 & I_m \end{array}\right] \left[\begin{array}{c} \mathbf{x} \\ \hline \mathbf{y}' \end{array}\right]$$

$$\left[\begin{array}{c} \mathbf{x} \\ \hline \mathbf{y}' \end{array}\right] = \left[\begin{array}{c|c} I_n & 0 \\ \hline -C_0 & I_m \end{array}\right] \left[\begin{array}{c} \mathbf{x} \\ \hline \mathbf{y} \end{array}\right]$$

where the change of basis matrices have all integer entries, it follows that the sets

$$\{\alpha_1, \ldots, \alpha_n, \alpha_{n+1}, \ldots, \alpha_{n+m}\}$$

$$\{\alpha_1, \ldots, \alpha_n, \alpha'_{n+1}, \ldots, \alpha'_{n+m}\}$$

span the same $\mathbb{Z}$-module.

Step 4: If C_1 is the zero matrix, then from $\mathbf{y}' = C_1\mathbf{x}$ we see that $\alpha_1, \alpha_2, \ldots, \alpha_n$ span the same $\mathbb{Z}$-module as the original $\alpha_1, \alpha_2, \ldots, \alpha_{n+m}$, and the algorithm terminates with output $(\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Otherwise, redefine

$$\begin{aligned} \alpha_{n+1} &\leftarrow \alpha'_{n+1} \\ \alpha_{n+2} &\leftarrow \alpha'_{n+2} \\ &\vdots \\ \alpha_{n+m} &\leftarrow \alpha'_{n+m} \end{aligned}$$

and return to step 1. This completes the description of the algorithm.

In order to prove that the algorithm terminates, we need only prove that on returning to Step 1, the minimum possible discriminant d among all sets of n of the α_i will have strictly decreased. Then since d is a positive integer and therefore can decrease only a finite number of times, the algorithm must eventually terminate. But we return to Step 1 only if C_1 is nonzero. In that case, renumbering the α_i if necessary, we may assume without loss of generality that $\{c_{11}\} \neq 0$. In that case we have

$$\begin{bmatrix} \alpha_{n+1} \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{bmatrix} = T \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{bmatrix}$$

where

$$T = \begin{bmatrix} \{c_{11}\} & \{c_{12}\} & \{c_{13}\} & \cdots & \{c_{1n}\} \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix},$$

so that

$$\begin{aligned} \operatorname{disc}(\alpha_{n+1}, \alpha_2, \alpha_3, \ldots, \alpha_n) &= \det(T)^2 \operatorname{disc}(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n) \\ &= \{c_{11}\}^2 d \end{aligned}$$

and $0 < \{c_{11}\}^2 d < d$, since $0 < |\{c_{11}\}| < 1$.

It is clear that Kronecker was not concerned with the feasibility of his algorithm in practice. In Step 1 we are left to compute by brute force all $\binom{m+n}{n}$ discriminants in order to determine which one is the smallest. This binomial coefficient could easily be prohibitively large. Moreover we know no a priori bound on the number of iterations other than the magnitude of the smallest discriminant that we find on the first time through, another number which could be very large. Consider moreover that in (Kronecker 1882) Kronecker did not provide an example of an integral basis computation, further suggesting his lack of concern with the practical application of the algorithm. These considerations make it clear that Kronecker did not seek to actually compute an integral basis, but only to justify its existence in a way that was acceptable in his own philosophy of mathematics.

As for the purpose that the integral basis served in his theory of algebraic numbers, we cannot say much without a further study of the *Grundzüge*, except to note that the discriminant, which is defined in terms of an integral basis, must have been as important for Kronecker as it was for anyone else developing a theory of algebraic numbers. Hensel's PhD thesis (Hensel 1884), for example, written under Kronecker's supervision, was on *"Arithmetische Untersuchungen über Discriminanten und ihre ausserwesentlichen Theiler"*, that is, "Arithmetic investigations of Discriminants and their exceptional Divisors".

2.2 Dedekind's *Supplement XI*, 1894

Over the course of his career Dedekind published several versions of his theory of algebraic numbers, the final and definitive form appearing in Supplement XI to the fourth edition of

Dirichlet's *Vorlesungen über Zahlentheorie*, commonly referred to as "Dirichlet-Dedekind" (1894). Earlier versions appeared in the second and third editions (1871 and 1879), and in a work that was requested of Dedekind by Lipschitz and translated into French. [4]

In order to understand the role of each of the named authors in the creation of the book called "Dirichlet-Dedekind", we may consult the foreword to the first edition, written by Dedekind in Braunschweig, October 1863:

> Immediately after the death of Dirichlet I was asked repeatedly to publish in the truest possible form his university lectures, which have contributed so extraordinarily much to the spread of familiarity with newer and finer parts of mathematics; I thought this request should be easy to fulfil, as in the years 1855 to 1858 I heard the most important of these lectures in Göttingen, and had many opportunities besides, in personal communication with Dirichlet, to get to know the rationale behind his plan of lectures. Having been authorized by Dirichlet's relatives to do so, I hereby deliver to the mathematical public a draft of the Lectures on Number Theory, which sticks essentially to the course followed by Dirichlet in the Winter 1856 to 1857; he himself harboured at that time thoughts of a publication of these lectures, and since he never worked out his talks in writing, a notebook written by me, containing admittedly only the high points of the proofs, served for him as a brief overview of the contents of the various sections. In oft-recurring conversations about this plan he expressed the intent that in this publication many sections would be added, which in a textbook must not be missed, but which in that Winter course for lack of time had to be skipped over. In the present offering therefore the notebook just mentioned is, in essence, laid down as foundation; but, in part according to older notebooks, in part based on Dirichlet's papers, and finally also entirely at my own discretion, I have made supplements of not insignificant extent, which I believe I must mention here, in order to take responsibility for them; they are contained in sections 105 to 110, 121 to 144, and in the remarks placed immediately under the text. [5]

---

[4] Sur la Théorie des Nombres entiers algébriques, 1877.

[5] (Dedekind 1930-1932a, pp. 392-393) *Gleich nach dem Tode Dirichlets wurde ich mehrfach aufgefordert, die von ihm gehaltenen Universitäts-Vorlesungen, welche so außerordentlich viel zur Verbreitung der Bekanntschaft mit neueren und feineren Teilen der Mathematik beigetragen haben, in möglichst getreuer Form zu veröffentlichen; ich glaubte dieser Aufforderung um so eher nachkommen zu können, als ich in den Jahren*

As Dedekind indicates in the forewords to later editions, the theory of algebraic numbers, and of *ideals*, goes far beyond anything that was actually present in Dirichlet's lectures. He discusses this for example in the foreword to the second edition (in which this material appeared in the tenth, rather than the eleventh supplement):

> This new edition differs from the first principally in that it is enriched by the tenth supplement, which treats of the composition of forms. This subject remained entirely excluded from the first edition, since the one paper of Dirichlet concerned expressly with it treats only the first fundamental theorem, whence I had to fear that I would in a complete presentation of this theory remove myself too far from the original purpose of the publication. [6]

In order to get the best representation of Dedekind's viewpoint, we turn to the final and most fully evolved expression of his theory, which appeared in Supplement XI of the fourth edition of Dirichlet-Dedekind. The Supplement is 224 pages long, and divided into 29 sections; it occupies roughly one third of the entire book. There, it is in §175 (the 17th of the 29 sections, and starting on the 102nd page of the supplement) that the integral basis is introduced. As we will see, the basis itself, the *object*, is in fact de-emphasized, whereas the main focus is put instead on a *theorem* which states the *existence* of a basis for the ring of integers.

1855 bis 1858 die wichtigsten dieser Vorlesungen in Göttingen gehört und außerdem vielfach Gelegenheit gehabt hatte, im persönlichen Verkehr Dirichlets Gründe für die von ihm befolgte Methode des Vortrags kennenzulernen. Nachdem die Verwandten Dirichlets mich dazu ermächtigt haben, so übergebe ich dem mathematischen Publikum hiermit eine Ausarbeitung der Vorlesung über Zahlentheorie, bei welcher im wesentlichen der im Winter 1856 bis 1857 von Dirichlet befolgte Gang eingehalten ist; er selbst faßte damals den Gedanken einer Herausgabe dieser Vorlesungen, und da er seinen Vortrag nie schriftlich ausgearbeitet hatte, so diente ihm ein von mir geschriebenes, allerdings nur die Hauptmomente der Beweise enthaltendes Heft dazu, einen ungefähren Überschlag über die Ausdehnung der einzelnen Abschnitte zu machen. In öfter wiederkehrenden Gesprächen über diesen Plan äußerte er die Absicht, bei der Veröffentlichung manche Abschnitte hinzufügen zu wollen, die in einem Lehrbuch nicht fehlen dürften, die aber in jener Winter-Vorlesung aus Mangel an Zeit übergangen werden mußten. Bei der jetzigen Herausgabe ist daher im wesentlichen zwar das eben erwähnte Heft zugrunde gelegt, aber ich habe teils nach älteren Heften, teils nach Dirichletschen Abhandlungen, endlich auch ganz nach eigenem Ermessen Zusätze von nicht unbedeutender Ausdehnung gemacht, welche ich hier anführen zu müssen glaube, um für sie die Verantwortlichkeit zu übernehmen; sie sind in den Paragraphen 105 bis 110, 121 bis 144 und in den unmittelbar unter den Text gesetzten Anmerkungen enthalten.

[6](Dedekind 1930-1932a, p. 396) *Diese neue Auflage unterscheidet sich von der ersten hauptsächlich dadurch, daß sie um das zehnte Supplement bereichert ist, welches von der Komposition der Formen handelt. Dieser Gegenstand war bei der ersten Auflage gänzlich ausgeschlossen geblieben, weil die einzige Abhandlung Dirichlets, welche sich unmittelbar hierauf bezieht, nur den ersten Fundamentalsatz behandelt, weshalb ich befürchten mußte, bei einer vollständigen Darstellung dieser Theorie mich zu weit von dem ursprünglichen Zwecke der Herausgabe zu entfernen.*

It is very important to acknowledge however that Dedekind's methodological viewpoint evolved over time, starting off closer to the traditional, computational norm and heading steadily farther away from computational methods as time went on. [7] In fact, in the first appearance of his theory of ideals, published 23 years earlier in the 2nd edition of Dirichlet-Dedekind (Dedekind and Lejeune Dirichlet 1871), he actually went over (in §161) a procedure essentially the same as the one we will see in Hilbert and Hensel in the following sections. [8] The Dedekindian methodology that we want to understand though is the one that he grew into with time, and it is for this reason that we choose to examine his work in (Dedekind and Lejeune Dirichlet 1894).

As we have suggested (and as is explored more thoroughly in (Avigad 2006)), the highly conceptual and non-computational methodology evolving with Dedekind, and earlier with others like B. Riemann (1826-1866), represented a departure from time-honoured mathematical values, in which computing had always been central. Surely the most obvious sort of activity that a lay person would expect to see in mathematics is computation, after all. Therefore part of the job of understanding the contrast between the computational and conceptual approaches is exploring just what sorts of "actions" are taken and goals achieved in the latter kind of mathematics. [9] Since Dedekind's treatment is not computational, we will attempt to give a step-by-step analysis to see what sort of mathematical "actions" (in some informal sense) he does take.

The basic steps that Dedekind works through in §175, beginning with the introduction of the ring of integers on page 537, are as follows.

1. Introduce the ring of integers of a field [10] Ω:

> We denote by $\mathfrak{o}$ *the set of all whole numbers of the field* Ω, and our task lies therein, to develop *the laws of divisibility of numbers* inside this domain $\mathfrak{o}$. [11]

[7] This evolution is examined in (Avigad 2006).

[8] See (Edwards 1980, p. 336) for further discussion.

[9] This sort of reflection on the components of mathematical practice is a recent theme in the philosophy of mathematics, to which volumes such as (Mancosu 2008) have been devoted.

[10] For Dedekind a number field was contained in the field of complex numbers, his first published definition thereof beginning, "By a *field* we will understand any system of infinitely many real or complex numbers, which ..." (Dedekind 1930-1932a, p. 224). It was not until E. Steinitz (1871-1928) that we got a completely axiomatic theory of fields (Steinitz 1910). Hensel's p-adic fields were an early departure, and were in fact among the primary motivators for Steinitz. See (Corry 1996, Ch. 4).

[11] (Dedekind and Lejeune Dirichlet 1894, p. 537) *Wir bezeichnen mit* $\mathfrak{o}$ *den Inbegriff aller ganzen Zahlen*

2. Demonstrate that $\mathfrak{o}$ is both a module, and an order, and that it contains $\mathfrak{z}$, the ring of rational integers. [12]

3. Define the concept of an integral basis (*ganze Basis*): a basis of Ω consisting entirely of whole numbers. Note that this is not what we call an integral basis today, as it need not span the ring of integers $\mathfrak{o}$ over $\mathbb{Z}$. We therefore continue to use the German term, here.

4. Demonstrate that a field Ω always has a *ganze Basis*.

5. Observe that for any *ganze Basis* $\alpha_1, \ldots, \alpha_n$, the module $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$ is contained in $\mathfrak{o}$. Any such module will be called an integral module (*ganzen Modul*).

6. Show that for an integral module $\mathfrak{a}$ we have $\Delta(\mathfrak{a}) \in \mathbb{Z}$, where $\Delta(\mathfrak{a})$ denotes the discriminant of $\mathfrak{a}$.

7. Observe that any $\omega \in \mathfrak{o}$ can be written as

$$\omega = \frac{m_1\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n}{m}$$

where $m, m_1, m_2, \ldots, m_n$ are rational integers with no common divisor.

8. Deduce the following theorem (we omit the proof):

> If $\mathfrak{a}$ is a finite and integral module, whose basis also forms a basis of the field Ω, and if m is the smallest natural factor by which an algebraic integer ω can be multiplied so that the product $m\omega$ lies in the module $\mathfrak{a}$, then the discriminant $\Delta(\mathfrak{a})$ is divisible by m^2, and the quotient $\frac{\Delta(\mathfrak{a})}{m^2}$ is the discriminant $\Delta(\mathfrak{b})$ of the integral module $\mathfrak{b} = \mathfrak{a} + [\omega]$.

9. Observe that one of these modules must have a discriminant which is least in absolute value. By the previous theorem every algebraic integer must lie in such a module $\mathfrak{a}$, and so we must have $\mathfrak{a} = \mathfrak{o}$.

---

des Körpers Ω, und unsere Aufgabe besteht darin, die Gesetze der Theilbarkeit der Zahlen innerhalb dieses Gebietes $\mathfrak{o}$ zu entwickeln. Dedekind defined the ring of integers earlier, in §173.

[12] Dedekind was the first to introduce the German terms *Modul* and *Ordnung*, which we translate into English as *module* and *order*.

10. Note: Dedekind does *not* now say that the basis of such a module is an object of fundamental importance, as Kronecker and Hensel do; instead he calls the following theorem fundamental, and then goes on to note that the discriminant $D = \Delta(\mathfrak{o})$ is of the greatest significance (*von der größten Bedeutung*) for the properties of the field Ω, second only to the degree n of the field in this respect. He will call it either the "fundamental number" (*Grundzahl*) or the discriminant of the field.

11. State the fundamental theorem:

    > The collection $\mathfrak{o}$ of all whole numbers of a finite field [13] Ω is a finite module[14], whose basis forms as well a basis of Ω.

Dedekind's treatment of the integral basis is thus entirely existential. We do not get a way to compute an integral basis, but only a theorem that states its existence. He has omitted entirely the procedure for computing a basis, which he had included in the second edition, 23 years earlier.

On the other hand, this is not to say that in his presentation of mathematical theory Dedekind is entirely unconcerned with concreteness. On the contrary, he finishes §175 by exploring the concept of the integral basis through the case of fields of degree 2. He works out completely the form of an integral basis for such a field, giving the now well-known result that, for a field $\mathbb{Q}(\sqrt{d})$ where d is squarefree and different from 1, we have

$$\mathfrak{o} = [1,\sqrt{d}], \quad d \equiv 2, 3 \bmod 4$$
$$\mathfrak{o} = \left[1, \frac{1+\sqrt{d}}{2}\right], \quad d \equiv 1 \bmod 4.$$

He even goes on to note that there are precisely 61 quadratic fields whose discriminants D are in absolute value less than 100, and he lists the 30 positive and 31 negative values that D takes on.

The presence of such numerical examples reminds us that while Dedekind may have favoured pure existence proofs, he was still capable of responding to the same desire for familiarity with particular examples which in part drove the computationalists. Working out the form of the integral basis for quadratic number fields however is in no way the same as giving a way to compute them for arbitrary number fields.

---

[13] This means that the degree of the field, not its number of elements, is finite.

[14] This means that the module is finitely generated.

2.3 Hilbert's *Zahlbericht*, 1897

Hilbert introduces the integral basis very early on in his *Zahlbericht*, implicitly attesting to its fundamental place in the theory. He refers to it as *a basis of the system of all whole numbers of the field* k, or, for short, *a basis of the field* [15] k.

Section 3 of the *Zahlbericht*, beginning on the third page of the report, starts with definitions and basic facts about the norm, different, and discriminant of an algebraic number, and then states and proves Theorem 5:

> Theorem 5. In a number field of mth degree there are always m whole numbers $\omega_1, \omega_2, \ldots, \omega_m$ with the property that every other whole number ω of the field can be represented in the form
>
> $$\omega = a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m,$$
>
> where $a_1, \ldots, a_m$ are rational integers.

Section 3 closes with citation of just two sources, namely, the very same Dedekind 1894 and Kronecker 1882 that we have surveyed above.

The proof that Hilbert gives for Theorem 5 occupies a certain middle-ground, as regards constructivity. It is not so nonconstructive as to merely prove the existence of an integral basis, say, by showing that its nonexistence would be contradictory; on the other hand, the construction that it gives is not an effective one. We are given no way in which to actually perform such a computation.

This is not at all what we would expect from Hilbert, given the picture of his number theory painted by Hasse (see Section 4.4). Hilbert's presentation bears no resemblance at all to Dedekind's. His use (see below) of the discriminant of a power basis as the denominator of the rational coefficients in a representation of an arbitrary element of the field recalls Kronecker's use of the same, and yet overall Hilbert's construction of the integral basis is entirely different from Kronecker's.

---

[15] As regards the stage in the evolution of the *field* concept, as used by Hilbert, Corry indicates (Corry 1996, p. 149) that Hilbert treated fields much as Dedekind had. He quotes Purkert (Purkert 1971, p. 18), who writes that (my translation), "Hilbert's works concern finite algebraic number field [extensions]. The concept of 'number field' as Dedekind originally introduced it, is fundamental. Consistent with the objective of these works, reference is not made to the abstract field concept."

While Hilbert's presentation is to some extent constructive, he does not reach the same level of constructivity as Hensel, who, as we will see in the next section, explains thoroughly how each step can be performed effectively.

Using the modern notation "$\mathcal{O}_k$" and "$\mathbb{Q}(\alpha)$" for clarity (Hilbert did not), the steps of Hilbert's proof are as follows. We do not claim that all the steps are easy to follow; in particular, steps 6 and 7 may appear problematic, as it is precisely in these steps that Hilbert forgoes effective constructability.

1. Let α be a primitive integer for the field k; that is, $\alpha \in \mathcal{O}_k$ and $k = \mathbb{Q}(\alpha)$.

2. Then for every integer $\omega \in \mathcal{O}_k$ we have

$$\omega = r_1 + r_2\alpha + \cdots + r_m\alpha^{m-1}$$

for some rational numbers $r_1, r_2, \ldots, r_m$.

3. Then denoting the conjugates of α and of ω by $\alpha, \alpha', \ldots, \alpha^{(m-1)}$ and $\omega, \omega', \ldots, \omega^{(m-1)}$, we have

$$\begin{bmatrix} 1 & \alpha & \cdots & \alpha^{m-1} \\ 1 & \alpha' & \cdots & \alpha'^{m-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{(m-1)} & \cdots & \left(\alpha^{(m-1)}\right)^{m-1} \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{bmatrix} = \begin{bmatrix} \omega \\ \omega' \\ \vdots \\ \omega^{(m-1)} \end{bmatrix}$$

4. Then for $s = 1, 2, \ldots, m$, the coefficient r_s is given by Cramer's rule. Hilbert does not mention Cramer's rule by name, but instead expresses it using a somewhat unusual notation (he implicitly acknowledges that it is unusual by referring to it as a *"leicht verständlicher Abkürzung,"* or "easily understandable abbreviation"), which we note now, since we will see it again in Hensel, in Section 2.4 below. Hilbert displays these equations:

$$\begin{aligned} r_s &= \frac{\left|1, \alpha, \ldots, \omega, \ldots, \alpha^{m-1}\right|}{|1, \alpha, \ldots, \alpha^{s-1}, \ldots, \alpha^{m-1}|} \\ &= \frac{\left|1, \alpha, \ldots, \omega, \ldots, \alpha^{m-1}\right| \left|1, \alpha, \ldots, \alpha^{s-1}, \ldots, \alpha^{m-1}\right|}{|1, \alpha, \ldots, \alpha^{s-1}, \ldots, \alpha^{m-1}|^2} \\ &= \frac{A_s}{d(\alpha)}. \end{aligned}$$

Here, the number A_s in the numerator was obtained only by adding, subtracting, and multiplying the number 1 as well as α and ω and their conjugates, and therefore is an

algebraic integer. On the other hand, A_s is equal to the rational number $r_s d(\alpha)$ and is thus a rational integer.

5. Every integer $\omega \in \mathcal{O}_k$ therefore admits a representation
$$\omega = \frac{A_1 + A_2\alpha + \cdots + A_m\alpha^{m-1}}{d(\alpha)} \tag{2.2}$$
where $A_1, A_2, \ldots, A_m \in \mathbb{Z}$ and $d(\alpha)$ is the discriminant of α.

6. Now, fixing s as one of the numbers $1, 2, \ldots, m$, we suppose that
$$\begin{aligned}
\omega_s &= \frac{O_1 + O_2\alpha + \cdots + O_s\alpha^{s-1}}{d(\alpha)}, \\
\omega_s^{(1)} &= \frac{O_1^{(1)} + O_2^{(1)}\alpha + \cdots + O_s^{(1)}\alpha^{s-1}}{d(\alpha)}, \\
\omega_s^{(2)} &= \frac{O_1^{(2)} + O_2^{(2)}\alpha + \cdots + O_s^{(2)}\alpha^{s-1}}{d(\alpha)}, \\
&\vdots
\end{aligned}$$
is the sequence of all integers of k of this form, where the coefficients $O_i^{(j)}$ are rational integers. That is, if $M_1, M_2, \ldots, M_s$ is any sequence of rational integers such that $\frac{M_1 + M_2\alpha + \cdots + M_s\alpha^{s-1}}{d(\alpha)}$ is in $\mathcal{O}_k$, then there is some j such that $M_i = O_i^{(j)}$ for $i = 1, 2, \ldots, s$.

7. We may assume that O_s is nonzero, and is the greatest common divisor of all the numbers $O_s, O_s^{(1)}, O_s^{(2)}, \ldots$.

8. Then the m first numbers $\omega_1, \omega_2, \ldots, \omega_m$ form a system with the desired property. (That is, they form an integral basis.)

9. For let an arbitrary integer ω be given, in the form (2.2). Then we must have $A_m = a_m O_m$ for some $a_m \in \mathbb{Z}$. But then the difference $\omega^* = \omega - a_m\omega_m$ is of the form
$$\omega^* = \frac{A_1^* + A_2^*\alpha + \cdots + A_{m-1}^*\alpha^{m-2}}{d(\alpha)},$$
and here again we have $A_{m-1}^* = a_{m-1}O_{m-1}$ for some $a_{m-1} \in \mathbb{Z}$. By considering now the difference
$$\omega^{**} = \omega^* - a_{m-1}\omega_{m-1}$$
and carrying on in this way, we see the correctness of Theorem 5.

While Hensel will give essentially the same construction of the integral basis as Hilbert, we will see major differences in the way in which steps 6 and 7 are handled.

2.4 Hensel's *Theorie der algebraischen Zahlen*, 1908

In his *Theorie der algebraischen Zahlen* (1908, henceforth TAZ), Kurt Hensel gives a p-adic treatment of algebraic number theory in twelve chapters, the book having been intended as the first of a two-volume series, of which, unfortunately, the second volume never appeared.

Hensel viewed his version of the theory of algebraic numbers as yet another in the series of renderings thereof which were in existence by that time, each one idiosyncratic and marked by the personality of its creator. In particular, he observed that each of Kummer, Dedekind, and Kronecker had a different way of so enlarging the domain of number theory that the fundamental arithmetic theorem of unique factorization would be recovered, and Hensel had his own way too.

Hensel believed, moreover, that since his p-adic numbers achieved an analogous construction for number theory to that present in analysis in the form of the power series expansions of functions, his version of algebraic number theory would involve essential simplifications over the work of his predecessors, as a result of the borrowed power of analytic methods. He therefore wrote as follows, in his foreword:

> ... Here [Kummer, Dedekind, and Kronecker] were met right away with the very difficult and at first almost unsolvable-looking problem of systematically expanding the newly opened domain of algebraic numbers in such a way that in the new, enlarged domain this fundamental theorem would regain its complete verity. The manner in which this difficult problem, naturally arising right at the outset of the investigation, was conquered by each of these three researchers through an approach uniquely peculiar to him, can well be viewed as one of his greatest scientific achievements; and the edifice of higher arithmetic raised atop this hard won foundation belongs among the most beautiful results for which the mathematics of the second half of the last century is indebted. ... Since my first involvement with the questions of higher number theory, I believed that the methods of function theory must also be applicable to this domain, and that a theory of algebraic numbers in many respects simpler could be built on this foundation. ... Let me finally be permitted briefly to mention in which points the theory of algebraic numbers developed here appears to give a simplification over the above mentioned outstanding presentations of this discipline. ... [16]

[16]... Hierdurch wurden sie sofort vor die sehr schwere und zunächst fast unlösbar scheinende Aufgabe

He thus wrote respectfully and reverentially about the work of his predecessors, but ultimately believed that his own version of the theory would offer essential improvements. And indeed he gives in TAZ his own version of the theory of *divisors*, i.e., he shows yet a fourth way in which the domain of algebraic number theory can be so expanded that unique factorization is recovered. To be sure, it is in some sense the same as the other three, but, as the others did, Hensel performs the construction in a new way, using new objects.

The application of the p-adic approach to algebraic number fields begins however only in the sixth chapter of TAZ, and Hensel's treatment of the integral basis comes already in the fifth. Our primary goal in this final section of the chapter is to see how Hensel handled the integral basis in Chapter 5 of TAZ. We will see that his construction is almost the same as Hilbert's except that in those steps in which Hilbert was not constructive, Hensel perseveres and shows us how to compute the objects involved.

In the process however we will address the broader goal of understanding what kind of computability Hensel gives us. We have set the goal in this thesis of understanding how, with Hensel and those who came after him, theoretical computability in algebraic number theory gradually became more and more practical. Hensel's procedure for computing an integral basis in Chapter 5 of TAZ relies on other procedures he has given earlier in the book, and we will therefore begin by briefly reviewing the contents of the first four chapters of TAZ, taking note of the ways in which Hensel's computability seems sometimes geared only toward theoretical demands, and other times leans toward practical applicability.

A striking feature of TAZ overall is the consistency with which Hensel supplies constructions in his proofs. Any object, it seems, that the theory is concerned with, is not simply proved to exist, but is actually constructed; that is, we are shown a way to compute such an object. Hensel does use proof by contradiction, at least once. For example on TAZ page

---

gestellt, das soeben erst erschlossene Gebiet der algebraischen Zahlen systematisch so zu erweitern, daß in dem neuen größeren Bereiche dieser Fundamentalsatz wieder seine volle Gültigkeit gewinnt. Die Art, wie dieses naturgemäß ganz am Anfang der Untersuchung auftretende schwere Problem von jedem dieser drei Forscher durch eine ihm allein eigentümliche Betrachtung bezwungen wurde, kann wohl als eine ihrer größten wissenschaftlichen Leistungen angesehen werden, und das auf diesem schwer gewonnenen Untergrunde sich erhebende Gebäude der höheren Arithmetik gehört zu den schönsten Ergebnissen, welche die Mathematik der zweiten Hälfte des vorigen Jahrhunderts verdankt. ... Seit meiner ersten Beschäftigung mit den Fragen der höheren Zahlentheorie glaubte ich, daß die Methoden der Funktionentheorie auch auf dieses Gebiet anwendbar sein müßten, und daß sich auf dieser Grundlage eine in mancher Hinsicht einfachere Theorie der algebraischen Zahlen aufbauen lassen könnte. ... Es sei mir endlich noch gestattet, kurz zu erwähnen, in welchen Punkten die hier entwickelte Theorie der algebraischen Zahlen eine Vereinfachung gegenüber den oben erwähnten ausgezeichneten Darstellungen dieser Disziplin zu ergeben scheint. ...

54 he proves that two polynomials $f(x)$, $g(x)$ have a common divisor if and only if a certain condition holds, and when assuming this condition in the proof, he does not construct a common divisor of $f(x)$ and $g(x)$, but instead supposes they are relatively prime and derives a contradiction. However, this proof comes only after Hensel has just finished showing us how to compute the greatest common divisor of two polynomials by the Euclidean algorithm, on the previous page of the book. I have not combed every last page in order to confirm it, but am confident that Hensel maintains such a commitment to constructivity throughout TAZ.

We will devote considerable space in this section to Hensel's polynomial factorization procedure in TAZ Chapter 4, which provided the basis for Zassenhaus's polynomial factorization algorithm some sixty years later, a subject we return to in Section 6.4.

The reader is referred to Appendix A for background on concepts related to the p-adic numbers, discussed throughout this section.

2.4.1 TAZ Chapters 1 and 2

In the first two chapters Hensel introduces the field $\mathbb{Q}$ of rational numbers – which he calls $K(1)$ – and the field $\mathbb{Q}_p$ of p-adic numbers for an arbitrary rational prime p – which he calls $K(p)$. He shows how to perform the four arithmetic operations on the numbers in $\mathbb{Q}_p$, and examines the idea of p-adic convergence.

At the end of the first chapter Hensel makes it clear, though perhaps without having considered the fact himself, that the collection of p-adic numbers, for fixed p, is countable. This notion will come initially as a surprise to many modern number theorists, for whom p-adic number fields are thought of as uncountable, but ultimately appears predictable, given the philosophy of mathematics that Hensel inherited from Kronecker. The countability of $\mathbb{Q}_p$ is the result of Hensel's requirement that an algorithm exist to generate the coefficients of any p-adic number:

> By a *quantity in the realm of* p or a *p-adic number* I will understand any series
>
> $$c_0 + c_1 p + c_2 p^2 + c_3 p^3 + \cdots$$
>
> with modulo p reduced coefficients, whether it terminate or not, provided a procedure exists whereby its digits or coefficients can be computed as far as one

may wish. [17]

Cantor's demonstration that there was more than one kind of infinity had appeared in an article of 1874 (Cantor 1874), and thus was by no means recent news in 1908. It could be that Hensel made no mention of the matter since perhaps, like Kronecker, he might have dismissed Cantor's set theory as a kind of improper mathematics. [18] On the other hand, it was not until the 1930s that Church, Kleene, Turing and others began work which would eventually produce the Church-Turing thesis, from which one can argue for the countability of the collection of all algorithms. It could be then that Hensel simply lacked the grounds for an argument as to the countability of the p-adic numbers. Perhaps the simplest explanation, however, is that Hensel simply didn't care about this question, and for that reason said nothing about it.

Hensel's definition of p-adic numbers is an excellent example of his concern with theoretical computability, not practical computability. he could easily have chosen to omit the clause about the existence of an algorithm altogether, and his definition would have remained acceptable to perhaps a majority of the mathematicians of his day. In accordance however with the constructive tradition he was brought into as a student of Kronecker, Hensel evidently felt that a p-adic series whose coefficients we could not compute either was an object simply not worth talking about, or else, more severely, was an object whose very existence we could not be entirely certain about. This example of Hensel's interest in purely theoretical computability should be kept in mind for contrast, when we later see him leaning somewhat more toward a concern with practical computability.

After defining the p-adic numbers, Hensel goes on in Chapter 2 to show that the four basic arithmetic operations can be performed on p-adic numbers effectively; that is, given p-adic numbers A and B – which really means that we are given algorithms with which to compute the coefficients of A and B – we can compute $A+B$, $A-B$, AB, and (in the case that $B \neq 0$) A/B, really meaning, again, that we have an algorithm with which to compute the coefficients of these numbers as far as we might wish.

---

[17] (Hensel 1908, p. 16) Unter einer Zahlgröße für den Bereich von p oder einer p-adischen Zahl will ich jede Reihe:

$$c_0 + c_1 p + c_2 p^2 + c_3 p^3 + \cdots$$

mit modulo p reduzierten Koeffizienten, mag sie nun abbrechen oder nicht, verstehen, wenn eine Vorschrift existiert, nach welcher ihre Ziffern oder Koeffizienten soweit berechnet werden können als man nur immer will.

[18] I do not know of any documentation of Hensel's having had such a view, however.

2.4.2 TAZ Chapters 3 and 4

In the third and fourth chapters of TAZ Hensel studies univariate polynomials with coefficients in $\mathbb{Q}_p$, and their factorization.

Chapter 3

In the short Chapter 3 Hensel merely provides some tools for working with polynomials, which he will apply in Chapter 4. Namely, he presents the Euclidean algorithm to compute the GCD of two polynomials; he defines the resultant of two polynomials, and the discriminant of a polynomial; he derives some of the basic properties of the resultant and discriminant.

When showing on page 53 how to apply the Euclidean algorithm to two polynomials $f(x)$, $g(x)$ of degrees μ, ν, with $\mu \geq \nu$, Hensel observes that the process must come to a conclusion "after a finite number of divisions", but makes no mention whatsoever of this number being bounded by ν. This is typical for Hensel, his concern in general being not with how many steps a process takes, except that the number be *finite*. In this respect Hensel appears to be concerned mostly with theoretical, not practical, computability, although we will see one exception later, in TAZ Chapter 4 §4, where he looks for faster ways to carry out certain procedures fundamental to his theory. Hensel's book has many small numerical examples in it, and we can easily imagine that he would want to find easier ways to compute these.

On page 55 Hensel defines the resultant $R(f, g)$ of two polynomials

$$f(x) = A_0 x^\mu + A_1 x^{\mu-1} + \cdots + A_\mu$$
$$g(x) = B_0 x^\nu + B_1 x^{\nu-1} + \cdots + B_\nu$$

to be the determinant of the Sylvester matrix of those polynomials, although he does not

call the matrix by this name. Thus, he defines

$$R(f,g) = \begin{vmatrix} A_0 & A_1 & \cdots & A_\mu & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & A_0 & A_1 & \cdots & A_\mu & \cdots & \cdots & \cdots & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & \cdots & 0 & A_0 & A_1 & \cdots & \cdots & A_\mu \\ B_0 & B_1 & \cdots & \cdots & B_\nu & 0 & \cdots & \cdots & 0 \\ 0 & B_0 & B_1 & \cdots & \cdots & B_\nu & 0 & \cdots & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & \cdots & 0 & B_0 & B_1 & \cdots & \cdots & B_\nu. \end{vmatrix}$$

where the top ν rows of the matrix feature the coefficients A_i of $f(x)$, and the bottom μ rows the coefficients B_i of $g(x)$. This matrix comes up again in Hensel's factorization procedure in TAZ Chapter 4, as we will see later. There, he actually uses the transpose of the matrix that he defined here.

Chapter 4

The subject of TAZ Chapter 4 is the decomposition of polynomials over $\mathbb{Q}_p$ into their irreducible factors. After presenting his factorization algorithm, Hensel discusses a few applications, such as a demonstration that for any rational prime p the field $\mathbb{Q}_p$ contains the $(p-1)^{\text{st}}$ roots of unity. One general application is the computation of a linear factor, which amounts to the computation of a root of a polynomial, and for this special case Hensel presents a better method, namely a p-adic version of Newton's method for root approximation. We review Hensel's factorization and p-adic Newton's method algorithms below. We note that as a part of his polynomial factorization algorithm, Hensel will use the Euclidean algorithm for the computation of the greatest common divisor of two polynomials (see page 45).

Polynomial factorization

Hensel's theory of algebraic numbers required an algorithm to factor polynomials over $\mathbb{Q}_p$, primarily because Hensel's definition of ideal prime divisors was based on such factorizations (see Appendix A), and secondarily because it seems that for Hensel, as for Kronecker, a mathematical theory was morally obligated to provide a way to compute any object that it

dealt with. At least these seem the most obvious reasons. Below we will examine Hensel's algorithm, and consider the possible reasons why he included it in his theory.

Since the factors that Hensel's algorithm computes are polynomials with p-adic numbers for coefficients, it follows that the computability that this algorithm provides is of the same kind as the computability of p-adic numbers themselves, namely, in a sense only "potential" and never actually completed, since the numbers involved are infinite series. The only thing guaranteed is that you can compute p-adic approximations of the factors of a given polynomial to as high a degree of accuracy as you might wish.

This is very different from the situation with Zassenhaus sixty years later, as we will see in Chapter 6, where he will apply some of Hensel's ideas in a practical factorization algorithm for polynomials over $\mathbb{Z}$, which terminates in finite time with an exact factorization.

Hensel's lemma

We begin with "Hensel's lemma", which is a common ingredient in both Hensel's and Zassenhaus's factorization procedures. The lemma that goes by this name has a long history, going back all the way to Gauss, and the story is complicated by the existence of various versions of the lemma. In particular, the full generality of the lemma that appears in Hensel's TAZ on page 68 is not used in the algorithm due to Zassenhaus, which instead relies on a statement closer to the lemma stated by Gauss.

TAZ Chapter 4 was not the first place where Hensel published his lemma. The book was to some extent cobbled together out of papers that Hensel published over the years from 1897 to 1908 such as (Hensel 1904a) and (Hensel 1904b), the first of which featured on page 80 his first publication of the lemma.

As observed by Frei (Frei 2007, p. 176), we can point to at least three occurrences of the lemma in print before Hensel. The earliest work we know of on such a lemma, though not the earliest publication, was by Gauss, who planned to put it in the eighth section he was preparing for the *Disquisitiones Arithmeticae*. The book went to press with only the first seven sections however, and the planned eighth section was finally published by Dedekind in 1863, eight years after Gauss's death, in the second volume of Gauss's collected works. The lemma ran:

> There is a factorization of a polynomial $P(x)$ mod p^k for any $k \geq 0$, once a factorization of $P(x)$ is known mod p, under the hypothesis that the factors of

> $P(x)$ are relatively prime mod p. (Frei 2007, p. 185)

Earlier T. Schönemann (1812-1868) had published a version of the lemma in a paper of 1846 (Schönemann 1846). H. Kühne (1867-1907) published just the year before Hensel, in 1903 (Kühne 1903), his paper appearing in fact in *Crelle's Journal*, of which Hensel was editor at that time. Frei discusses the question of whether Hensel may have been influenced by Kühne, and says that the answer is not yet clear (Frei 2007, p. 176).

Hensel's own result of 1904 runs as follows:

> If the discriminant of $F(x)$ is of the order δ, then the function $F(x)$ decomposes into factors of lower degree if and only if its δ^{th} approximant $F^{(\delta)}(x)$ decomposes modulo $p^{\delta+1}$. In fact, to each decomposition
>
> $$F^{(\delta)}(x) \equiv \bar{f}(x)\bar{g}(x) \ \left(\mathrm{mod}\, p^{\delta+1}\right)$$
>
> corresponds a uniquely determined decomposition of $F(x)$ in p-adic factors
>
> $$F(x) = f(x)g(x) \quad (p)$$
>
> such that $\bar{f}(x)$ and $\bar{g}(x)$ are approximants of $f(x)$ and $g(x)$.

In order to compare Hensel's and Gauss's results, we begin by noting that their conclusions are the same: when Hensel says "the function $F(x)$ decomposes into factors of lower degree" he is talking about decomposition over his field $\mathbb{Q}_p$, so this simply means that $F(x)$ can be factored mod p^k for any $k \geq 0$, which is precisely Gauss's conclusion.

As for their hypotheses, first let us clarify the meaning of Hensel's. If two of the roots of $F(x)$ are congruent modulo p^k, for any exponent k, then p^k divides the discriminant $D(F)$. Therefore if p^δ is the highest power of p dividing $D(F)$, it follows that no two of the roots of $F(x)$ are congruent modulo $p^{\delta+1}$. If then the δ^{th} approximant $F^{(\delta)}$ of F, which satisfies

$$F^{(\delta)} \equiv F \bmod p^{\delta+1},$$

decomposes modulo $p^{\delta+1}$ as in Hensel's hypotheses, then the factors into which it decomposes must be relatively prime mod $p^{\delta+1}$, since none of their roots are congruent with respect to that modulus.

Thus, both Hensel and Gauss want to start with a decomposition of $F(x)$ modulo some power of p, into relatively prime factors, and for Gauss that power is restricted to the first.

Gauss ensures relative primality of the factors by asking directly for it; Hensel gets it by imposing the stronger condition that $F(x)$ have no repeated roots modulo some power of p. To see that Gauss's hypothesis is actually weaker, consider that a polynomial with repeated roots may very well be decomposed into relatively prime factors, as for example in the decomposition of $(x-1)^2(x-2)^5$ as $(x-1)^2$ times $(x-2)^5$.

We note however that in the important special case in which $F(x)$ is assumed from the outset to have no repeated roots, Hensel's result is actually stronger than Gauss's. For in that case $F(x)$ might still have repeated roots mod $p, p^2, \ldots$ up to some p^δ, so that Gauss will not get a factorization mod p into relatively prime factors, whereas Hensel will get one mod $p^{\delta+1}$. For example, consider the polynomial $F(x) = x^2 - 35x + 286 = (x-13)(x-22)$, and the prime $p = 3$. Considered mod 3, $F(x)$ reduces to $(x-1)(x-1)$, and even mod 3^2 it reduces to $(x-4)(x-4)$. But mod 3^3 it is $(x-13)(x-22)$, and can be decomposed into the relatively prime factors $(x-13)$ and $(x-22)$.

Finally, we note that Hensel's *proof* of his lemma is a *constructive* one: the content of the proof is a procedure with which, given a factorization of F mod p^{r+1} for any $r \geq \delta$, we can "lift" (in the modern terminology) to a factorization of F modulo p^{r+2}. By applying this procedure repeatedly, we can lift to a factorization modulo as high a power of p as we might wish. We discuss this procedure in Step 4 of the algorithm below.

The factorization procedure

In this section we will occasionally want to give lower bounds on the runtimes of Hensel's algorithms, in order to show how badly they would scale. Therefore instead of the usual "$\mathcal{O}$" notation for upper bounds on runtime, we will use the less common "Ω" notation for lower bounds.

Given a polynomial $F(x) \in \mathbb{Q}_p[x]$, Hensel's procedure should either say that $F(x)$ has no factors of lower degree over $\mathbb{Q}_p$, or else it should produce a factorization $F(x) = f(x)g(x)$ with $f(x), g(x) \in \mathbb{Q}_p[x]$ each of lower degree than $F(x)$. By applying this procedure iteratively, Hensel can split $F(x)$ into irreducible factors over $\mathbb{Q}_p$.

It is important to note that Hensel does not present his algorithm in a stylized step-by-step format as is common in modern presentations, and as we will give below. His procedure, like all the procedures in TAZ, is simply embedded in the prose. The steps we extract from his discussion are as follows.

Hensel's factorization algorithm.

Input: A rational prime p, and a polynomial $F(x) \in \mathbb{Q}_p[x]$ all of whose coefficients are p-adic integers.

Output: Either two polynomials $f(x), g(x) \in \mathbb{Q}_p[x]$ such that $F = fg$, with $1 \leq \deg f < \deg F$ and $1 \leq \deg g < \deg F$, or else the (correct) assertion that no such factorization exists.

1. In order to determine whether F has any repeated roots, compute the discriminant $D(F)$ by evaluating the resultant $R(F, F')$. If F does have repeated roots, then compute the GCD of F and F' using the Euclidean algorithm. This will be a proper divisor f of F, so we can simply compute $g = F/f$, return the factors (f, g) of F, and halt.

2. Otherwise, F has no repeated roots. Therefore its discriminant $D(F)$ is nonzero, and has some positive p-adic order δ. Compute δ. (We know δ is positive since the coefficients of F are all p-adic integers.)

3. In order to be able to apply Hensel's lemma and compute a factorization of F modulo arbitrarily high powers of p, we need to first find an initial factorization of $F^{(\delta)}$ mod $p^{\delta+1}$. We compute that now *by brute force*.

   Namely, if $\deg F = n$, then for every pair of degrees (μ, ν) such that $\mu + \nu = n$ and $\mu \leq \nu$, we may consider every polynomial f of degree μ with coefficients reduced mod $p^{\delta+1}$ (there are only $\Omega(p^{\delta\mu})$ of them), and every polynomial g of degree ν with coefficients similarly reduced (there are only $\Omega(p^{\delta\nu})$ of them), and check whether $fg \equiv F \bmod p^{\delta+1}$.

   There are only finitely many cases to check, so after a finite number of steps we will either find a factorization of F mod $p^{\delta+1}$, or else we will know that there is none. In the latter case we can finish the procedure by asserting that F is irreducible over $\mathbb{Q}_p$; in the former case we move on to Step 4.

4. Assuming we have computed

$$F^{(r)} \equiv f_0 g_0 \bmod p^{r+1},$$

   where $r \geq \delta$, we can apply the lifting procedure given in the proof of Hensel's lemma, in order to lift the factorization $f_0 g_0$ to one that holds modulo the next higher power

of p, namely p^{r+2}. By repeating this process indefinitely, we can factor F to as high a power of p as we might wish.

The steps of the lifting procedure are as follows:

(a) Consider the difference

$$F^{(r+1)} - f_0 g_0 \bmod p^{r+2}$$

between our current factorization $f_0 g_0$ and the next closest approximant $F^{(r+1)}$ of F. Hensel demonstrates that this function is divisible by p^{r+1}. Therefore set

$$p^{r+1}\mathscr{F}_0 = F^{(r+1)} - f_0 g_0.$$

(b) We now apply a result which Hensel proves on page 63, which gives us two functions f_1, g_1 of degrees less than μ and less than ν, respectively, such that

$$p^{\delta}\mathscr{F}_0 \equiv f_0 g_1 + g_0 f_1 \bmod p^{\delta+1}$$

and such that $f_1 g_1$ is divisible by $p^{2\delta-2\rho}$,where ρ is the order of the resultant $R(f_0, g_0)$.

(c) It follows that

$$F^{(r+1)} \equiv \left(f_0 + p^{r+1-\delta} f_1\right)\left(g_0 + p^{r+1-\delta} g_1\right) \bmod p^{r+2}$$

so the new factors of $F^{(r+1)}$ that we have lifted to are $f_0 + p^{r+1-\delta} f_1$ and $g_0 + p^{r+1-\delta} g_1$.

What we have omitted is how to compute the functions f_1, g_1 provided by the result on page 63. As is typically the case in TAZ, Hensel leaves it up to us to piece the procedure together. In the proof of Hensel's lemma he merely cites the result on page 63, and it is when we review the proof of that result that we find the way to construct f_1, g_1. This is generally the way in which we can extract algorithms out of TAZ: each proof involves a construction, and by consulting all the right proofs we can put together a procedure with which to compute a desired result.

The proof of the result on page 63 reveals that computing f_1, g_1 is a matter of solving the n-by-n linear system $Ax = b$ whose matrix A is precisely the transpose of the Sylvester matrix for the resultant of f_0, g_0 which we saw in TAZ Chapter 3, and where b lists the coefficients of $p^{\delta}\mathscr{F}_0$.

Hensel's brute-force search for an initial factorization in Step 3 above shows again a case in which he appears to be concerned more with the theoretical than the practical side of computability. Even if we regard polynomial multiplication as an atomic operation (which is very generous), the expected runtime of this search is $\Omega(n^2 p^{\delta n})$, exponential in both the degree n of F, and the order δ of its discriminant.

Were we to apply this general procedure to the polynomial $F(x) = x^2 - 35x + 286$ that we considered earlier (although for such a low-degree polynomial there are much smarter tricks we could apply, surely known to Hensel, such as simply checking for a root) then we would begin by computing its discriminant. Its derivative is $F'(x) = 2x - 35$, so that the discriminant $D(F)$, computed as the resultant $R(F, F')$, is equal to

$$\begin{aligned}\begin{vmatrix} 1 & -35 & 286 \\ 2 & -35 & 0 \\ 0 & 2 & -35 \end{vmatrix} &= \begin{vmatrix} -35 & 0 \\ 2 & -35 \end{vmatrix} - 2 \begin{vmatrix} -35 & 286 \\ 2 & -35 \end{vmatrix} \\ &= 1225 - 1306 \\ &= -81\end{aligned}$$

which is of 3-adic order $\delta = 4$. In this case we already have the estimated lower bound of $p^{\delta n} = 3^8 = 6561$ polynomial multiplications on our runtime. In fact if we were to factor $F(x)$ by brute force search through all pairs $x - a, x - b$ of linear factors reduced mod $3^{\delta+1} = 243$, and if we avoided repeats by the constraints $0 \le a \le b < 243$, then we would have

$$\sum_{b=0}^{3^5-1} (b+1) = \sum_{b=1}^{3^5} b = \frac{3^5\left(3^5+1\right)}{2} = 29646$$

possible combinations to try. Without the foreknowledge that we would find the factorization $(x - 13)(x - 22)$ quite early in the process, we would be faced with potentially 82.35 hours of hand calculation, at one multiplication every ten seconds.

Hensel provided several small examples in TAZ, such as the factorization of $F(x) = x^3 - 2$ over $\mathbb{Q}_5$. We find that $D(F) = -2^2 \cdot 3^3$ is of 5-adic order 0, so that the factorization procedure can be initialized with a factorization mod 5. It is hard to believe that Hensel would have done weeks of computation to get his initial factorization, instead of simply observing that $F(3) \equiv 0 \bmod 5$, and dividing $F(x)$ by the linear factor $(x - 3)$, working mod 5. That he does not however *mention* the method of factoring a polynomial of degree 2 or 3 by looking for a root, suggests again that he was mainly concerned with demonstrating theoretical

computability, not with giving the reader a set of tools with which to actually carry out computations.

In order to clarify Hensel's factorization procedure, we now complete the factorization of $x^3 - 2$ over $\mathbb{Q}_5$ up to four 5-adic places right of the comma. [19] This will reveal that, as opposed to the brute-force initialization in Step 3, Step 4 of Hensel's algorithm is actually not too heavy to carry out by hand through several iterations. Below we put 5-adic coefficients in brackets. We also write these coefficients out as p-adic series, where we understand $p = 5$.

Completing the division of $x^3 - 2$ by $x - 3 \bmod 5$, we get

$$x^3 - 2 \equiv (x + 2)\left(x^2 + 3x + 4\right) \bmod 5,$$

so we have

$$f_0 = x + 2 \qquad\qquad g_0 = x^2 + 3x + 4.$$

We have $\delta = 0$, and for the first lifting we compute $\mathscr{F}_0 = 4x^2 + 3x + 3$.

Since $\delta = 0$ we will always solve for f_1, $g_1 \bmod 5$ (that is, mod $p^{\delta+1}$), and therefore we can invert the transposed Sylvester matrix on $f_0, g_0 \bmod 5$ just once, and can use it in every lifting iteration. The matrix is

$$\begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 3 \\ 0 & 2 & 4 \end{bmatrix}$$

and its inverse mod 5 is

$$\begin{bmatrix} 4 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 4 & 3 \end{bmatrix}.$$

Then representing $\mathscr{F}_0$ by $[\,4\ \ 3\ \ 3\,]$ we have

$$\begin{bmatrix} 4 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 4 & 3 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \\ 3 \end{bmatrix} = \begin{bmatrix} D_0 \\ D_1 \\ C_0 \end{bmatrix},$$

where

$$f_1 = C_0 \qquad\qquad g_1 = D_0 x + D_1.$$

[19] Our computation reveals that Hensel has an error on TAZ page 64.

Note that we have set f_1 to be of degree less than $\mu = \deg f_0 = 1$, and g_1 of degree less than $\nu = \deg g_0 = 2$. We get

$$\begin{bmatrix} 4 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 4 & 3 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 4 \end{bmatrix},$$

so

$$f_1 = 4 \qquad\qquad g_1 = 1$$

and we perform the updates

$$f_0 \leftarrow f_0 + 5f_1 \qquad\qquad g_0 \leftarrow g_0 + 5g_1$$

resulting in

$$\begin{aligned} f_0 &= x + (2 + 4p) \\ g_0 &= x^2 + (3 + 0p)\, x + (4 + 1p)\,. \end{aligned}$$

Note that the entries of the column vector $[0, 1, 4]^T$ have simply been tacked on as the new 5-adic digits. This will generally be the case, on each iteration.

For the second iteration we compute $\mathscr{F}_0 = 4x^2 + 2x + 2$, and get

$$\begin{bmatrix} 4 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 4 & 3 \end{bmatrix} \begin{bmatrix} 4 \\ 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 2 \end{bmatrix},$$

so that we update to

$$\begin{aligned} f_0 &= x + \left(2 + 4p + 2p^2\right) \\ g_0 &= x^2 + \left(3 + 0p + 2p^2\right) x + \left(4 + 1p + 2p^2\right). \end{aligned}$$

Third iteration: $\mathscr{F}_0 = 4x^2 + 4x + 1$,

$$\begin{bmatrix} 4 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 4 & 3 \end{bmatrix} \begin{bmatrix} 4 \\ 4 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \\ 2 \end{bmatrix},$$

$$\begin{aligned} f_0 &= x + \left(2 + 4p + 2p^2 + 2p^3\right) \\ g_0 &= x^2 + \left(3 + 0p + 2p^2 + 2p^3\right) x + \left(4 + 1p + 2p^2 + 4p^3\right). \end{aligned}$$

Fourth iteration: $\mathscr{F}_0 = 4x^2 + 3x + 2$,

$$\begin{bmatrix} 4 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 4 & 3 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \\ 1 \end{bmatrix},$$

$$\begin{aligned} f_0 &= x + \left(2 + 4p + 2p^2 + 2p^3 + 1p^4\right) \\ g_0 &= x^2 + \left(3 + 0p + 2p^2 + 2p^3 + 3p^4\right) x + \left(4 + 1p + 2p^2 + 4p^3 + 4p^4\right). \end{aligned}$$

This process could be carried on indefinitely, and our 5-adic approximations of factors of $x^3 - 2$ would improve by one digit on each iteration. The root of the linear factor

$$-2,4221\ldots = 3,0223\ldots$$

is converging to a cube root of 2 in $\mathbb{Q}_5$.

Our demonstration has shown that for small enough polynomials, Hensel's procedure can be feasible to carry out by hand. Still, we have argued that the algorithm seems to have served theoretical purposes for Hensel as well. Insofar as his purpose in giving his factorization algorithm might have been to justify theoretically the existence of a factorization into irreducibles over $\mathbb{Q}_p$, this would recall Kronecker, who [20] considered that even the *definition* of "irreducible divisor" was not fully well-founded until a procedure was given with which to decide whether any given divisor was irreducible or not.

But we have not yet considered Hensel's final word on the matter, and in this case his motivations prove a bit difficult to analyze. This time he does address concerns over the practical applicability of the algorithm, even offering a refinement of Hensel's lemma in which he lowers the initial order δ to 2ρ, where ρ is the order of the resultant of the factors f_0, g_0 in the initial factorization. But we must take a moment to consider what Hensel says.

Immediately after finishing the proof of Hensel's lemma on page 70, he writes,

> Herewith is the problem, to decompose an arbitrary polynomial of degree n into irreducible p-adic factors, completely solved, and it is easy to actually carry out such a decomposition. [21]

[20] See (Edwards, Neumann, and Purkert 1982, p. 53).

[21] (Hensel 1908, p. 70): Hiermit ist die Aufgabe, eine beliebige Funktion n^{ten} Grades in irreduktible p-adische Faktoren zu zerlegen, vollständig gelöst, und es ist leicht, eine solche Zerlegung wirklich durchzuführen.

and it is interesting that he uses the phrase *wirklich durchzuführen* – "to actually carry out". At this point he finishes Chapter 4 § 3 by spelling out how the procedure he has just given, to factor a polynomial into precisely two factors of lower degree, can be applied repeatedly in order to eventually reach the irreducible factors. I believe that where Hensel speaks of "actually carrying out" the decomposition into irreducible factors, he really only means that *in theory*, this process of repeated splitting of one factor into two is a simple one. Namely, it is *simple to describe*, and it is *easy to see* that it proves the theoretical possibility of factorization into irreducibles. Such a reading, though it seems to go against Hensel's choice of words, appears necessary in order to avoid contradiction with what comes next.

The next section is called

> Conclusions. Simpler Criteria for the Decomposability of Polynomials. The Eisenstein Polynomials.

and Hensel begins by addressing directly the question of computability in theory versus practice. He writes, (my emphasis):

> By the fundamental theorem proved in the previous section, the problem of decomposing a polynomial $F(x)$ with p-adic coefficients into its irreducible factors is *theoretically completely solved*. If however the order δ of the discriminant $D(F)$ is somewhat large, then the decomposition of $F(x)$ modulo $p^{\delta+1}$ is *not always easy to manage*. [22]

If here Hensel admits the potential for the algorithm to run unmanageably long, then the reading we gave earlier to his *wirklich durchzuführen* seems the only way to avoid contradiction.

He continues,

> For these reasons we will handle a few special cases important for the sequel, in which these questions either can be more easily solved, or in which the irreducibility of the function $F(x)$ can be directly recognized. [23]

[22](Hensel 1908, pp. 70-71): Nach dem im vorigen Abschnitt bewiesenen Fundamentalsatz ist die Aufgabe, eine Funktion $F(x)$ mit p-adischen Faktoren zu zerlegen, theoretisch vollkommen gelöst. Ist aber die Ordnungszahl δ der Diskriminante $D(f)$ etwas groß, so ist die Zerlegung von $f(x)$ modulo $p^{\delta+1}$ nicht immer leicht zu bewerkstelligen. (In the English translation I have corrected the two occurrences of lowercase f to the uppercase F with which the paragraph began.)

[23](ibid., p. 71): Aus diesem Grunde sollen noch einige für das Folgende wichtige Fälle behandelt werden,

and the very first result he states and proves is the one we mentioned earlier, in which δ is lowered to 2ρ, with ρ the order of the resultant $R(f_0, g_0)$. Considering that we found the lower bound $\Omega(p^{\delta n})$ on the complexity of Hensel's procedure, with δ in the exponent, any lowering of this quantity would be desirable. We can imagine how this would be particularly important to Hensel, who needed to apply his process at least for the computation of the many small numerical examples that he uses in his book, such as the factorization of $x^3 - 2$ over $\mathbb{Q}_5$ that he gives on page 64. Any little advantage, such as lowering δ to 2ρ, might allow Hensel to handle a few more cases: perhaps a polynomial of degree 4, or with a larger discriminant, or over $\mathbb{Q}_p$ for a prime p a bit larger than 5.

Newton iteration

Following this in TAZ Chapter 4 § 4 comes a simple test to determine whether a given polynomial $F(x)$ has a p-adic root $\xi \in \mathbb{Q}_p$ congruent modulo some power of p to a rational integer $\xi_0 \in \mathbb{Z}$. Namely, this is the case if and only if the quotient

$$\frac{F(\xi_0)}{(F'(\xi_0))^2}$$

has positive p-adic order. In combination with Hensel's factorization algorithm, in particular starting with the linear factor $(x - \xi_0)$ of an approximant $F^{(r)}$ of F, this gives a way to find roots of F.

No sooner has Hensel finished adducing the proof of this result, however, than he states – again betraying an interest in practical computation – that we can do better:

> As useful as this theorem is in most cases, still we will replace it by one which is essentially sharper, and which can now be easily deduced. The approximate computation of p-adic roots arising from this theorem is none other than the well-known Newton Approximation Method, carried over to the p-adic numbers. [24]

Hensel goes on to derive the familiar recursion rule for Newton's method, in the p-adic

---

in denen diese Frage entweder einfacher gelöst werden, oder in denen die Irreduktibilität der Funktion $f(x)$ direkt erkannt werden kann.

[24] So brauchbar dieser Satz in den meisten Fällen auch ist, so wollen wir ihn doch noch durch einen wesentlich schärferen ersetzen, der jetzt sehr einfach abgeleitet werden kann. Die aus ihm sich ergebende angenäherte Berechnung der p-adischen Gleichungswurzeln ist nichts anderes als die bekannte Newtonsche Approximationsmethode, übertragen auf die p-adischen Zahlen.

case. Namely, if ξ_0 is an approximant of order ρ of a root of $F(x)$, i.e. if

$$F(\xi_0) \equiv 0 \bmod p^\rho,$$

then the next best approximation will be computed as $\xi_0 + h$, where h satisfies

$$h = -\frac{F(\xi_0)}{F'(\xi_0)} \quad (p)\,.$$

Hensel does not give an example of the application of this iterative approximation procedure, but instead later in the book, in Chapter 8 § 5, he puts this method to *theoretical* use.

In order to illustrate the process in a numerical case, we show how it can be applied to compute a root of $F(x) = x^3 - 2$ in $\mathbb{Q}_5$, with initial approximation $\xi_0 = 3$.

In general, on the iteration computing ξ_{i+1}, we will need to divide by $3\xi_i^2$, but only mod 5. Since the ξ_i are all congruent to 3 mod 5, we can compute this quantity and invert it once and for all. Namely,

$$\left(3 \cdot 3^2\right)^{-1} \equiv 3 \bmod 5.$$

Therefore our update rule becomes: $\xi_{i+1} = \xi_i - 3(\xi_i^3 - 2)$, or

$$\xi_{i+1} = \xi_i + 2(\xi_i^3 - 2).$$

The convergence is linear, so in general when computing ξ_i we can work mod 5^{i+1}. For the first four iterations we find (again putting 5-adic notation in square brackets)

$$\begin{aligned}
\xi_1 &= \xi_0 + 2(\xi_0^3 - 2) \\
&= 3 + 2(3^3 - 2) \\
&\equiv 3 \bmod 5^2
\end{aligned}$$

$$\begin{aligned}
\xi_2 &= \xi_1 + 2(\xi_1^3 - 2) \\
&= 3 + 2(3^3 - 2) \\
&\equiv 53 \bmod 5^3 \\
&= [3, 02]
\end{aligned}$$

$$\begin{aligned}\xi_3 &= \xi_2 + 2(\xi_2^3 - 2)\\ &= 53 + 2(53^3 - 2)\\ &\equiv 53 + 250 \bmod 5^4\\ &= [3, 02] + [0, 002]\\ &= [3, 022]\\ &= 303\end{aligned}$$

$$\begin{aligned}\xi_4 &= \xi_3 + 2(\xi_3^3 - 2)\\ &= 303 + 2(303^3 - 2)\\ &\equiv 303 + 1875 \bmod 5^5\\ &= [3, 022] + [0, 0003]\\ &= [3, 0223]\end{aligned}$$

and the first five digits $3, 0223$ now agree with those we computed on page 50, using Hensel's factorization procedure.

2.4.3 TAZ Chapter 5 and the integral basis

The results of TAZ Chapters three and four on polynomials with p-adic coefficients are applied in Chapter five to polynomials over the rationals (as a special case). Here Hensel works out the basic facts about ordinary algebraic number fields (not their p-adic completions).

The integral basis, or in Hensel's language inherited from Kronecker, the *Fundamentalsystem*, is developed at the end of Chapter 5. Like Kronecker before him, Hensel emphasizes the importance of the *Fundamentalsystem*, saying that it "forms the foundation for all subsequent investigations" [25]

Hensel's construction of the integral basis is essentially the same one that we saw in Hilbert, but differs in a few respects. For one, Hensel explains how to actually perform the steps of the construction effectively. For another, Hensel gives overall much more explanation and clarification, using four pages where Hilbert used only one and a half. Finally, while Hensel uses mostly different letters, the fact that he continues to make the same use of 's' in the latter part of the construction is, along with his use of the same unusual notation for

[25] *"... die Grundlage für alle folgenden Untersuchungen bildet,"* (p. 111).

Vandermonde matrices that Hilbert used, further evidence either that Hensel was drawing on Hilbert, or else that the two both drew on some prior, unidentified, third source. Given the diligence of Hilbert's attributions in the *Zahlbericht*, the former seems the more likely theory.

We go now through the steps of Hensel's argument, given on pages 111 through 116 of TAZ. In general, Hensel's verbose clarifications will not be reflected here, as we strive instead to demonstrate the similarity with Hilbert's argument, as presented in Section 2.3. Again, we use modern language and notation that did not appear in the original. Hensel's first steps mirror Hilbert's:

1. Let β be a primitive integer for the field K; that is, $\beta \in \mathcal{O}_K$ and $K = \mathbb{Q}(\beta)$.

2. Then for every integer $\gamma \in \mathcal{O}_K$ we have

$$\gamma = u_0 + u_1\beta + u_2\beta^2 + \cdots + u_{\lambda-1}\beta^{\lambda-1}$$

for some rational numbers $u_0, u_1, u_2, \ldots, u_{\lambda-1}$.

3. Then denoting the conjugates of β and of γ by $\beta_1, \beta_2, \ldots, \beta_\lambda$ and $\gamma_1, \gamma_2, \ldots, \gamma_\lambda$, we have

$$\begin{bmatrix} 1 & \beta_1 & \cdots & \beta_1^{\lambda-1} \\ 1 & \beta_2 & \cdots & \beta_2^{\lambda-1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta_\lambda & \cdots & \beta_\lambda^{\lambda-1} \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{\lambda-1} \end{bmatrix} = \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_\lambda \end{bmatrix}$$

4. Then for $k = 0, 1, \ldots, \lambda - 1$, the coefficient u_k is given by Cramer's rule. Here Hensel uses the same notation as Hilbert:

$$\begin{aligned} u_k &= \frac{\left|1, \beta_i, \beta_i^2, \ldots, \gamma_i, \ldots, \beta_i^{\lambda-1}\right|}{\left|1, \beta_i, \beta_i^2, \ldots, \beta_i^k, \ldots, \beta_i^{\lambda-1}\right|} \\ &= \frac{\left|1, \beta_i, \ldots, \gamma_i, \ldots, \beta_i^{\lambda-1}\right| \left|1, \beta_i, \ldots, \beta_i^k, \ldots, \beta_i^{\lambda-1}\right|}{\left|1, \beta_i, \ldots, \beta_i^k, \ldots, \beta_i^{\lambda-1}\right|^2} \\ &= \frac{v_k}{d}. \end{aligned}$$

Hensel explains by essentially the same reasoning that Hilbert used, that v_k is an algebraic integer. In order to argue that it is rational, however, instead of noting that it is equal to $u_k d$ he observes that it is a symmetric function in $(\beta_1, \ldots, \beta_\lambda, \gamma_1, \ldots, \gamma_\lambda)$.

5. Every integer $\gamma \in \mathcal{O}_K$ therefore admits a representation

$$\gamma = \frac{v_0 + v_1\beta + v_2\beta^2 + \cdots + v_{\lambda-1}\beta^{\lambda-1}}{d} \tag{2.3}$$

where $v_0, v_1, \ldots, v_{\lambda-1} \in \mathbb{Z}$ and $d = d(\beta)$ is the discriminant of β.

Here Hensel's discussion diverges from Hilbert's. Where Hilbert goes on to discuss, in non-constructive terms, sequences of integers of the form (2.2), Hensel addresses the issue of how we can actually decide, by a finite procedure, which of the elements of the form (2.3) are integers and which are not. He writes:

> Not all numbers represented in the form (2.3) are algebraically integral, but one can decide for each of them whether they are algebraically integral or not, by forming the associated equation. One need carry out this inquiry at most for the d^λ algebraic numbers γ for which in their representation in the form (2.3) all coefficients v_i are non-negative and less than d. Namely, if for a number γ this is not the case, and if one writes each of the λ coefficients v_i in the form:
>
> $$v_i = du_i + v_i^{(0)},$$
>
> where $v_i^{(0)}$ is the least non-negative residue of v_i on division by d, then γ equals the sum of two algebraic numbers
>
> $$\begin{aligned}\gamma &= \left(u_0 + u_1\beta + \cdots + u_{\lambda-1}\beta^{\lambda-1}\right) + \frac{v_0^{(0)} + v_1^{(0)}\beta + \cdots + v_{\lambda-1}^{(0)}\beta^{\lambda-1}}{d} \\ &= \bar{\gamma} + \gamma_0\end{aligned}$$
>
> of which the first $\bar{\gamma}$ ... is certainly algebraically integral. Since the two numbers γ and γ_0 therefore differ by the algebraic integer $\bar{\gamma}$, it follows that the one is algebraically integral if and only if the other is. (Hensel 1908, pp. 112-113)

Hensel thus provides a decision procedure, and shows that it requires only finitely many tests. He shows us how we can actually determine for a number given in the form (2.3) whether it is an algebraic integer or not.

There is, however, no further discussion here as to how the equation associated to a given number γ is to be computed. In this respect Hensel's work appears very different from a modern computational textbook, in which we would expect to see numbered routines and

subroutines, and explicit indications as to when one procedure is to call on a prior one. It is indeed possible to piece together a way in which the equation associated to γ can be computed, based on ideas which Hensel presented earlier in TAZ Chapter 5 § 3, but it is noteworthy that he does not piece it together for us. In Section 2.4.4 below we consider the method that Hensel likely intended.

At this point in the argument, recall that Hilbert asks us to imagine the sequence of integers of degree s in α, and notes that among the lead coefficients of all these numbers there must be a greatest common divisor. He then says that integers in which the lead coefficient is this GCD will form an integral basis.

Hensel on the other hand shows us how to actually compute this basis, by leading us through the following steps:

1. Having actually computed all the integers of the form (2.3) with modulo d reduced coefficients v_i, we now fix s as one of the numbers $0, 1, 2, \ldots, \lambda - 1$, and find, among all integers $\gamma^{(s)}$ of the form
$$\frac{v_0 + v_1\beta + \cdots + v_s\beta^s}{d} \tag{2.4}$$
with modulo d reduced coefficients, one in which the coefficient v_s of the highest power of β is positive and smallest possible. We call this number
$$\beta^{(s)} = \frac{v_0^{(s)} + v_1^{(s)}\beta + \cdots + v_s^{(s)}\beta^s}{d}.$$

2. If for a given value of s there turn out to be no integers of the form (2.4), then we take
$$\beta^{(s)} = \frac{0 + 0 \cdot \beta + \cdots + d\beta^s}{d}.$$

3. The minimal coefficients $v_s^{(s)}$ are therefore always among the numbers $1, 2, \ldots, d$.

Finally Hensel demonstrates that $\beta^{(0)}, \beta^{(1)}, \ldots, \beta^{(\lambda-1)}$ forms an integral basis in essentially the same way that Hilbert did in his final step.

2.4.4 Hensel's "subroutines"

Hensel's derivation of an integral basis is manifestly constructive, but his discussion leaves two subproblems:

1. computing the discriminant d of β, and

2. deciding whether a number of the form (2.3) is integral,

which Hensel does not address in this section of the book. The reader, evidently, is to understand how to solve these problems after having read the book up to this point. In this something of the deliberateness of modern computational treatments is conspicuously absent, namely the explicit identification of algorithms and reference to subroutines.

Here again the purpose of algorithms in Hensel's mathematics appears strange to modern eyes. We observed before that the prohibitive runtime of Hensel's algorithms prevents their actual application in all but the simplest cases, and here again we detect a de-emphasis on the actual execution of algorithms, insofar as Hensel leaves it to his reader to assemble all the scattered parts of these procedures, instead of writing them out clearly himself, as step-by-step processes.

Computing the discriminant

First, there is the problem of computing the discriminant $d(\beta)$. In defining the discriminant of an algebraic number β in Chapter 5 § 4, Hensel uses that power

$$g(y) = m_\beta(y)^\mu \tag{2.5}$$

of the irreducible polynomial $m_\beta(y)$ for β that is obtained by forming the product of all $(y - \beta_i)$, where $\beta_1, \beta_2, \ldots, \beta_\lambda$ are the conjugates of β in the field K_α.

On page 105 he then deduces that, up to sign, the discriminant $d(\beta)$ is equal to the resultant $R(g(y), g'(y))$, where $g'(y)$ is the formal derivative of $g(y)$. That is, it is equal to the discriminant of the function $g(y)$, as defined on page 56, in Chapter 3 § 3.

As we saw, the resultant was introduced in Chapter 3, as the determinant of the Sylvester matrix, which we know how to compute.

Deciding integrality

Finally, there is the second subproblem of deciding whether a number γ given in the form (2.3), with β a primitive integer of the field, is integral or not. Hensel says that this can be done by forming the monic polynomial F_γ having all the γ_i as its roots, where γ_i for $i = 1, 2, \ldots, \lambda$ is the conjugate of γ obatined by replacing β by its conjugate β_i in (2.3).

As he proves on page 103, this polynomial is either the minimal polynomial for γ, or else a power of it, and so its coefficients are all rational integers if and only if γ is an algebraic integer.

The closest Hensel comes to showing how to construct this polynomial, however, is in Chapter 5 § 3, where he proves that the sum, difference, and product of two algebraic integers are again algebraic integers. His method is constructive: given that we know the minimal polynomials for algebraic integers η, θ, he shows how to construct a monic polynomial with integer coefficients satisfied by any of $\eta + \theta, \eta - \theta, \eta\theta$.

It is fairly straightforward to modify Hensel's construction in order to compute F_γ. Namely, using the minimal polynomial for β we can easily compute the rational matrix $G = (g_{ij})$ such that

$$\gamma \begin{bmatrix} 1 \\ \beta \\ \vdots \\ \beta^{\lambda-1} \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1\lambda} \\ g_{21} & g_{22} & \cdots & g_{2\lambda} \\ \vdots & \vdots & & \vdots \\ g_{\lambda 1} & g_{\lambda 2} & \cdots & g_{\lambda\lambda} \end{bmatrix} \begin{bmatrix} 1 \\ \beta \\ \vdots \\ \beta^{\lambda-1} \end{bmatrix}. \tag{2.6}$$

Then it is easily seen that F_γ is simply the characteristic polynomial c_G of the matrix G. For by replacing β by each of its λ conjugates in (2.6), we obtain λ equations in which G is unaltered since its entries are rational, and in which the λ conjugate vectors $[1, \beta_i, \ldots, \beta_i^{\lambda-1}]^T$ are seen to be λ eigenvectors of G. These eigenvectors are distinct, since β is of degree λ, and therefore exhaust all the eigenvectors of the λ-by-λ matrix G. It follows that any root of c_G, being an eigenvalue of G, must equal one of the conjugates γ_i. Therefore c_G is the monic polynomial of degree λ having precisely the λ conjugates of γ as its roots, i.e. it is exactly F_γ.

2.4.5 Algorithms and efficiency in Hensel

Hensel's algebraic number theory seems to have been oriented heavily toward theoretical computability, with occasional nods toward practical computability.

Some of his choices reflect a purely philosophical concern that the objects of his theory should be computable, such as his definition of p-adic numbers in TAZ Chapter 1, which requires a procedure to compute their coefficients. In Chapter 4 § 4 on the other hand he provides a speedup for his factorization procedure which can only serve the practical purpose of making actual computations easier to carry out. Then again, this sort of move

is a rare one for Hensel; he does not discuss speedups of any kind for his procedures for computing an integral basis in Chapter 5, or for computing the units or the prime numbers in a p-adic algebraic field $\mathbb{Q}_p(\alpha)$ in Chapter 6, §§ 4-5. All of these involve blind search through a space whose size is exponential in the degree of the algebraic extension. In most cases, Hensel only wants to show that the number of steps in a process is *finite*, i.e. he only seeks computability in principle.

Another way in which Hensel's book TAZ is strikingly different from modern computational treatises is in the absence of explicitly enumerated, step-by-step procedures. Hensel never seems to say, "Here is an algorithm; here is its name; here are the steps." Instead, the procedures that he gives come up in the proofs of theorems, and if procedure A uses procedure B as a subprocess, you will know this only because the proof in which A appears will cite a theorem whose proof required B. For example, this is how we found out that solving a linear system with Sylvester matrix was involved in Hensel's lifting process in his factorization algorithm. All this makes Hensel's book look less like instructions for computers, and more like a theoretical system in which all the objects are constructible in principle. While it is true that even in modern day research papers, algorithms may be buried in the text in a similar way, Hensel's book still seems different from what we expect today in a textbook.

To be fair, Hensel's procedures *do* have some practical value. If you stick to algebraic numbers whose minimal polynomials over $\mathbb{Q}$ have low degree – say, 2, 3, or maybe even 4 – and whose discriminants are small, and if you concern yourself with the prime divisors associated to small rational primes p – say the single-digit ones $2, 3, 5, 7$, or maybe even a bit farther – then you can actually work through a good number of examples, and in that way attain a solid understanding of much that goes on in Hensel's algebraic number theory.

It might be argued, meanwhile, that the scope and variety of examples one could lay one's hands on with Hensel's procedures, while sufficient for grounding one's understanding of the basic theory, were not however adequate for what one would call "table work". To fill large tables with widely varying examples adequate for the detection of patterns and formulation of new conjectures seems to have required developments that came somewhat later than Hensel.

The electronic computer was no doubt a crucial part of these later developments, but it was by no means the whole story. If one were given only Hensel's procedures, and a computer to carry them out at great speed, one could indeed push the boundaries a significant bit

farther than where one could go working by hand. Now one might be able to look at polynomials of higher degrees, maybe getting up into double digits, and so forth. But with computer science came the realization that there was a very important difference between polynomial-time, and exponential-time algorithms. Your ability to carry out algorithms of the latter type tends to abruptly cut off, beyond a certain input size. You "hit a wall" so to speak, at which point any larger inputs would require a computation longer than you can reasonably wait, or longer than your life expectancy, or even outlasting the heat-death of the universe. If nothing else, the activity of the researchers we will consider in Chapters 4 through 7 of this thesis is testament to the fact that Hensel's algorithms, which are in many cases exponential-time, were not fast enough.

In any case, when it comes to explaining Hensel's motivations, the limited practical applicability that his procedures do offer does not seem to be quite the whole story. It is hard to imagine someone, who was not driven by a specific methodological commitment, supplying as assiduously and unfailingly as Hensel did, a construction for every existence claim in every proof in a book-length treatise. We are aware of the influence Kronecker likely had on Hensel's philosophy of mathematics, as regards ontological questions like when we are justified in saying that a certain object exists, and this might have had some part in Hensel's purpose. Still, I will take the remainder of this section to reflect informally on a third possibility, that the constructivity to which Hensel was so clearly committed provides a special kind of understanding of the theory of algebraic numbers. It is not simply the confidence that certain objects exist, as might please Kronecker; nor is it quite the understanding that we gain by putting pencil to paper and actually working some examples through to completion, since it is available even for an algorithm too long to complete by hand. Instead, I would suggest that Hensel's constructive proofs provide a certain *sense of mobility* between the objects of the theory, in that they provide us with an *imaginable path* that would get us *from* one type of object *to* another type of object.

I believe that a couple of analogies help to explain this idea. Imagine first that these mathematicians were instead astronomers, and instead of mathematical objects they wanted to tell us about distant galaxies. In that case, a non-constructive mathematician like Dedekind might tell us all about the Andromeda galaxy. He would talk about its size, mass, and luminosity; how many stars it has; its shape and its structure. He would not however tell us how to get there. Hensel, on the other hand, would draw us a star map. He would say how far and in what directions we would have to travel to reach the Andromeda

galaxy. He might meanwhile fail to mention that the destination is light-years away, and that we would never actually be able to get there during our lifetime.

It would then be up to us to decide how to react to this information. I think we could reasonably feel satisfied at knowing where the Andromeda galaxy is. Whereas Dedekind only told us what the galaxy looks like, Hensel gave us a way to think about how we could get there. It is probably far too distant an object for us ever to actually reach, yet still we now have a way to at least *imagine what it would be like* to get there. This contributes to our understanding of the object, in that now we may not only picture the object itself, but can also think about where it stands in relation to ourselves.

Perhaps one more analogy is worth thinking about. Every algorithm specifies its input and output, and it tells you how to get the outputs when you feed in the inputs, and is in that way like a description of a machine. For example, given the prime number $p = 11$, and the polynomial $F(x) = x^3 - 2$, Hensel gives us an algorithm with which to compute the number of prime divisors of p in the field $\mathbb{Q}(\sqrt[3]{2})$, and the degree and order of each one. In turns out that there are two: one of degree 1 and one of degree 2, and each of order 1. The algorithm Hensel gives us describes to us a series of mechanical motions, which when carried out will lead us from the input $(p, F(x))$ to the output:

$$11 = \mathfrak{p}_1\mathfrak{p}_2 \text{ in } \mathbb{Q}(\sqrt[3]{2}) \qquad \deg \mathfrak{p}_1 = 1 \qquad \deg \mathfrak{p}_2 = 2.$$

If we then imagine the whole of algebraic number theory as a vast and complex machine, with a receptor for primes here, and one for polynomials there, an output chute for divisors, and so on, then it is as though Hensel has lifted up the cover to expose the internal workings of the machine, and has taught us all there is to know about each of the various moving parts and linkages, so that we can see how they transfer motion all the way from the input receptors at one end, to the outputs at the other. As we read through his book we can gradually build a mental image of every last moving part, and of the ways they are connected, until finally we feel that we understand the machine completely. [26]

When an existence-oriented approach to algebraic number theory is taken instead, relying always on proof by contradiction, then it is as though we are never allowed to peek inside the machine at all. Supposing another great nineteenth century invention, the locomotive,

[26] Or yet again, instead of imagining the algorithms and procedures of algebraic number theory as machine parts linked rigidly together, we can think of them as free-standing tools, which can always be used together in new ways by the number theorist.

were introduced in this way, the description might go something like this: "It has a furnace where you can burn fuel, and it has wheels that turn, and there must be some connection in between, or else the train wouldn't move." This might be a good enough description for certain passengers, but one would hardly expect it to satisfy an engineer who wanted to fully understand the mechanisms involved. [27] Given only this meagre information, we might believe *that* the locomotive works, but we can scarcely say that we know *how*. Perhaps then it all amounts to a question of occupational specialization: Is it the mathematician's job to be concerned with what you believe, or with what you know how to do? [28]

To be fair, a great deal more might be derived about the locomotive from the existence standpoint. We might be told about all sorts of operational parameters, such as the fact that for such and such a combustion temperature in the furnace, the wheels will turn precisely so fast, presuming a level track, and so on; that is to say, we might be given a great deal of quantitative information about the relations holding between various parts of the system. But still, something would always be omitted about the process, which we needed in order to be able to envision the precise mechanism by which energy was transferred from one point to the other. Every ideal *has* a unique factorization into prime ideals, but how do we get *from* an ideal *to* its factorization? We don't know. Every number field *has* an integral basis, but how do we get *from* a specification of the field *to* an integral basis? We don't know.

It is remarkable that such a great theory could be built in this existence-oriented way, and that it was is a testament to the genius of those who discovered the proofs on which this particular approach relies. Still, to some people this manner of presentation must be very dissatisfying. Perhaps Hensel was among them, and perhaps some of the motivation for his constructivity might have come from reflections such as these, although I cannot offer any documentary evidence to this effect.

Hensel's own student, Hasse, would in any case publish in several places arguments in favour of a more computational style of algebraic number theory, illustrating his discussions with metaphors somewhat like the ones we have considered here. In particular he would talk about the desire for "mobility", and it could be that what he meant was something like

[27] The author realizes the irony of this statement coming from himself, given that he is much more a passenger than an engineer of number theory! Suffice it to say, he is not a passenger of the particular type mentioned.

[28] Compare Gordan's infamous remark that Hilbert's proof of the Hilbert basis theorem was not mathematics but theology.

what we have discussed above. Considering that Hasse was inspired to leave Göttingen to work with Hensel by a chance encounter with Hensel's book (Hensel 1913), it could be that Hasse saw already in Hensel's methods a striving after the same kind of "mobility" that he would later express the need for. We will return to Hasse's reflections on these matters in Section 4.4.

Chapter 3

Turn of the Century through World War II

The two defining characteristics of Hensel's *Theorie der algebraischen Zahlen*, its use of p-adic numbers and its computational style, were both unfashionable when the book was published in 1908. The reputation of the p-adic numbers had suffered a blow when Hensel used them in a flawed proof of the transcendence of e, presented at the DMV [1] and published in 1905. [2] As for the Kroneckerian-Henselian ideas of computability in proofs, these held no special place in the class field program laid out by Hilbert in 1898, [3] already well under way with Furtwängler's proofs of 1903 - 1904, [4] and dominating the number theory scene. It would take two innovations to elevate the status of the ideas that Hensel stood for: one a theorem, namely his student Hasse's local-global theorem, and the other a machine, the electronic computer.

By the time we reach the 1960's, we will find Zassenhaus writing algorithms for algebraic number theory which are to be executed on electronic computers, and which rely on the use of two p-adic techniques whose presence in Hensel's book we noted in Chapter 1: the p-adic Newton iteration, and Hensel's lemma.

In the present chapter we will attempt to weave together the story of relevant events

[1] That is, the *Deutsche Mathematiker-Vereinigung*, or German mathematical society.

[2] Hensel's paper is (Hensel 1905). See (Ullrich 1998, p. 172) for further discussion.

[3] (Hilbert 1898)

[4] The proofs originally appeared in (Furtwängler 1903a,b, 1904), and then were collected together in (Furtwängler 1906)

in the lives of Hensel, Hasse, Taussky, and Zassenhaus, along with several other mathematicians, in order both to show how these four wound up being involved in computational algebraic number theory, and in order to examine the circumstances under which certain important work in the field emerged.

As we give a sketch of algebraic number theory from 1897 to 1945, the main themes must be class field theory and the quest for the most general reciprocity law, and in Section 3.2 we will briefly review a bit about the origins of class field theory. As for computational efforts, we will have to see either how they were pursued during this time, or else how their main proponents would find computational motivations through other, more mainstream algebraic number theoretic work.

In the final two sections of this chapter, 3.5 and 3.6, we will review relevant points in the lives of Olga Taussky and Hans Zassenhaus up to the time of the War. We will return to Taussky in Chapter 5 and Zassenhaus in Chapter 6, but feel it makes sense chronologically to study their prewar lives in the present chapter.

3.1 Hensel and Hilbert

In many ways the lives of Hensel and Hilbert run parallel. The two were born 25 days apart, Hensel on 29 December 1861, Hilbert on 23 January 1862, both in Königsberg. Hensel was awarded his PhD in 1884, and Hilbert his in 1885. Apart from a few years in Hensel's childhood spent in Königsberg, both men spent their lives in just two cities: one where they earned their doctorate (Berlin for Hensel and Königsberg for Hilbert), and one where they were appointed full professor (Marburg for Hensel and Göttingen for Hilbert). See Figure 3.1. Both men retired in 1930. Hensel died in June 1941, and Hilbert twenty months later in February 1943.

They began to make major contributions to number theory at the same time as well, although their works were received by the community in vastly different ways. Hilbert was an immediate success, whereas Hensel would have to wait about a quarter century before the importance of his work would begin to be understood.

In fact Hensel began talking and writing about his p-adic numbers in 1897, the same year that Hilbert's *Zahlbericht* was published. It is therefore easy to view his work as having begun its life in the shadow of a much more popular work, that was telling a very different story. It is hard to overstate the impact of Hilbert's *Zahlbericht* on algebraic number theory.

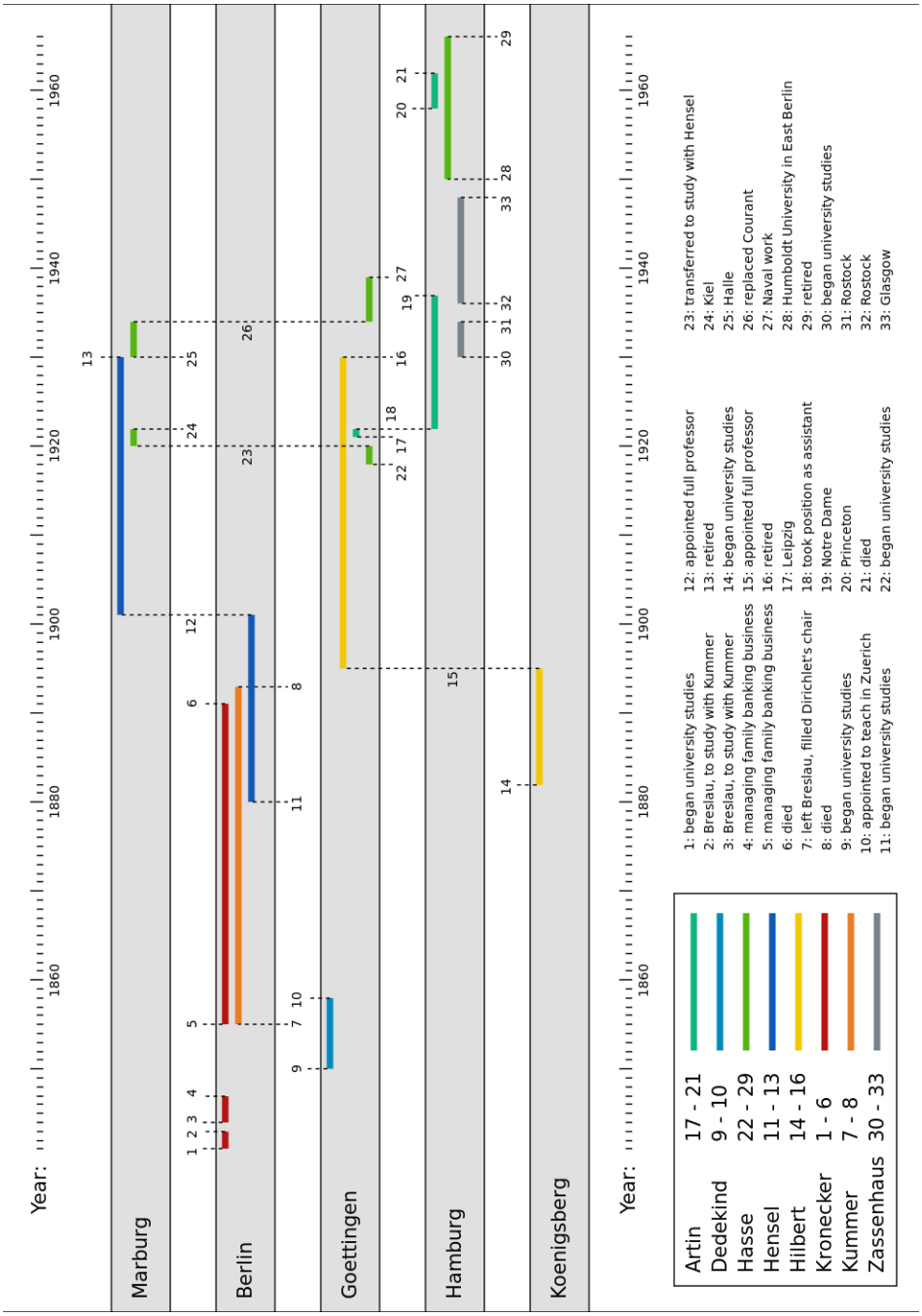

Figure 3.1: Movements of selected mathematicians among selected German universities, 1841 to 1966.

It has been written, for example, that "For half a century it was the bible of all who learned algebraic number theory, and perhaps it is still." (Freudenthal 2008) Hasse wrote ca. 1932 that,

> The work is still today the given starting point for all who would penetrate the mysteries of the theory of algebraic numbers, and trace the heights of modern number theoretic research. [5]

If this were not enough, Hensel's proud announcement of his p-adic numbers to the Deutsche Mathematiker-Vereinigung at the Braunschweig meeting of 1897 was followed immediately by a talk of Hilbert [6] which was leading directly toward class field theory, a dominant theme in the field of number theory for years to come, and thus somewhat overshadowing Hensel's work.

By this time Germany had a Mathematical Society. After failed efforts in the late 1860's and early 70's by Clebsch to form a separate mathematical division of the Society of German Natural Scientists and Physicians (the *Gesellschaft Deutscher Naturforscher und Ärzte* or GDNÄ), at last Cantor and others were able to bring together the German Mathematical Society (*Deutsche Mathematiker-Vereinigung* or DMV) in 1890. It began holding annual meetings, co-located with the GDNÄ, a practice the two groups persisted in until 1931. [7]

The format of the *Jahresbericht* (the annual report) of the DMV was a record of the proceedings of the meeting, typically occupying about a hundred pages, and containing talks by mathematicians on their latest work, followed by a *Bericht* (a report), requested by the society and written by one or more mathematicians, on the history and development of some subject in mathematics. The proceedings would not be published until the *Bericht* was completed, typically one or more years after the meeting. Some years there were two or even three such reports, and they ranged anywhere from around 50 to nearly 500 pages in length. See Table 3.1.

Volume 4 of the *Jahresbericht* chronicled the proceedings of two meetings of the DMV, those of 1894 and 1895 in Vienna and in Lübeck, and the *Bericht*, already commissioned

---

[5](Hasse 1981, p. 529) Das Werk ist noch heute der gegebene Ausgangspunkt für jeden, der in die Geheimnisse der Theorie der algebraischen Zahlkörper eindringen und der modernen zahlentheoretischen Forschung auf ihre Höhen folgen will.

[6]This at least is the print order in the *Jahresbericht*. It is not clear whether this reflects the order in which the lectures were given at the meeting, but the order is at any rate not alphabetical.

[7]`http://de.wikipedia.org/wiki/Deutsche_Mathematiker-Vereinigung`

Table 3.1: Early *Jahresbericht* data.

Vol.	Meeting(s)	Pub.	Meeting pp.	Report pp.	Location(s)
1	1890 - 91	1892	78	210	Halle
2	1891 - 92	1893	74	84	Nürnberg
3	1892 - 93	1894	106	460, 35	München
4	1894 & 1895	1897	176	372	Wien & Lübeck
5	1896	1901	94	486	Frankfurt
6	1897	1899	142	42, 48, 20	Braunschweig

at the 1893 meeting in München (Freudenthal 2008; Reid 1970), was to be on the subject of number theory. The task was to be shared by Minkowski, handling elementary number theory, and Hilbert, handing the theory of algebraic number fields, but Minkowski withdrew from the project. [8] Hilbert's work filled 372 pages in the DMV's fourth volume, which was finally published in 1897. His *Bericht über die Theorie der algebraischen Zahlkörper* ("Report on the Theory of algebraic Number Fields") is known simply as the *Zahlbericht*.

Meanwhile, the meeting of the DMV in the same year, 1897, took place from the 20th to the 25th of September in Braunschweig. In the intervening years Hilbert had done more than just write a report in which he gathered and systematized the theretofore scattered theory of algebraic number fields as it had been developed by Kummer, Dedekind, Kronecker, and others. He had gone beyond, and begun to advance the theory. See Figure 3.2 for the number of works cited in Hilbert's bibliography each year from 1825 to 1896. This table omits just three earlier references in the *Zahlbericht*, namely, (Lagrange 1796), (Legendre 1798), and (Gauss 1801). See Figure 3.3 for the list of all authors cited more than once in Hilbert's bibliography, along with the number of their works cited.

Hasse wrote (Hasse 1981),

> In this report Hilbert collected all knowledge reached up to that time in the theory of algebraic number fields, and assembled it into a unified theory, supported by broad points of view. ... Due to this fundamental significance of the Zahlbericht as handbook for the study, it will often be viewed as the pinnacle of the Hilbertian contribution to the number theoretic domain. It must be stated

[8] On the history of the interactions between Minkowski and Hilbert on this subject, including valuable insight into Hilbert's thoughts about the work, see the letters from Minkowski to Hilbert, published in (Rüdenberg and Zassenhaus 1973), as well as Hilbert's biography (Reid 1970) Chapters VI - VII.

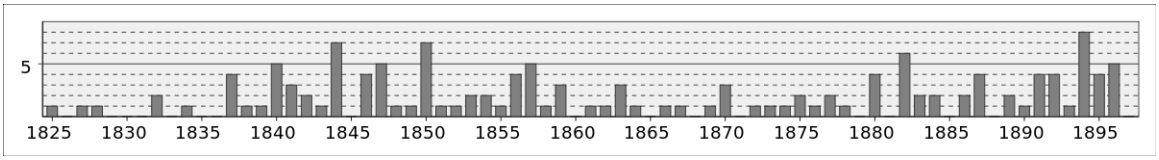

Figure 3.2: Number of works cited per year in bibliography of Hilbert's *Zahlbericht* from 1825 forward, omitting three earlier references, from 1796, 1798, and 1801.

```
   Kummer: 26  ##########################
 Kronecker: 21  ######################
 Dirichlet: 16  ################
Eisenstein: 12  ############
  Dedekind:  9  #########
    Hensel:  5  #####
   Hilbert:  5  #####
    Jacobi:  4  ####
     Weber:  4  ####
   Hurwitz:  4  ####
 Schwering:  4  ####
 Minkowski:  4  ####
      Lame:  3  ###
  Lebesgue:  3  ###
     Gauss:  3  ###
   Gmeiner:  3  ###
  Bachmann:  3  ###
    Cauchy:  2  ##
  Schering:  2  ##
     Fuchs:  2  ##
   Hermite:  2  ##
```

Figure 3.3: List of authors cited more than once in Hilbert's *Zahlbericht*, together with number of citations.

> clearly here, that this in no way corresponds to the truth. ... Hilbert's actual new results, on the contrary, begin only now; they build on the foundation that the Zahlbericht has laid down, and lead from there in new, unimagined directions. [9]

The next steps in the mainstream development of the theory, namely, the steps toward class field theory, were sketched in Hilbert's talk in Braunschweig. He spoke on the theory of quadratic extension fields, [10] giving a preview of the large treatise on the subject that he would publish in Volume 51 of the *Mathematische Annalen*, in 1899. This line of investigation would lead to his class field conjectures, which he stated in 1898, in (Hilbert 1898). Of this last work, Hasse has written (Hasse 1981),

> The pinnacle of Hilbert's number theoretic contribution is without question to be seen in the last of his works on algebraic number theory, in (Hilbert 1898), even if – or perhaps precisely because – this work has a more programmatic character. [11]

Even Hasse, Hensel's student, would likely admit that this talk of Hilbert's, printed immediately after Hensel's in the *Jahresbericht*, completely drowned out the other in terms of impact on the overall direction of the field. Hensel's news was big enough, for a matter of tying up loose ends, of reformulating, and finding new and interesting perspectives on, and understandings of, old material, but he was not shaping the mainstream research program. He was suggesting new approaches, but not yet showing just what could be done with them.

Hensel began his talk (Hensel 1897c) by describing the nature of his approach to algebraic number theory through p-adic expansions of numbers, indicating continually the ways in which what he was doing was analogous to the theory of algebraic functions, expanded in power series.

---

[9] In diesem Bericht hat Hilbert alles zur damaligen Zeit in der Theorie der algebraischen Zahlkörper erreichte Wissen gesammelt und zu einer einheitlichen, von großen Gesichtspunkten getragenen Theorie zusammengestellt. ... Wegen dieser grundlegenden Bedeutung des Zahlberichts als Handbuch für das Studium wird er vielfach als der Gipfel der Hilbertschen Leistung auf zahlentheoretischem Gebiet angesehen. Es muß hier klar gesagt werden, daß das keineswegs den Tatsachen entspricht. ... Hilberts eigentliche neuen Resultate dagegen setzen jetzt erst ein; sie erwachsen auf dem Boden, den der Zahlbericht geebnet hat, und führen von dort in neue ungeahnte Höhen.

[10] *Über die Theorie der relativquadratischen Zahlkörper.* Jahresbericht der Deutschen Mathematiker-Vereinigung v. 6, p. 88 - 94 (1899).

[11] Den Gipfel von Hilberts zahlentheoretischer Leistung hat man ohne Frage in der letzten seiner Arbeiten zur algebraischen Zahlentheorie, in (Hilbert 1898), zu sehen, wenn auch – oder vielleicht gerade weil – diese Arbeit einen mehr programmatischen Charakter hat.

He believed that his new and unique approach to algebraic number theory would provide ways around old difficulties, which had beset prior approaches:

> ... The only exception is the very special case in which the number d of the conjugate roots (2a) for a ramification point is divisible by the prime number p being considered, a case which can occur only for truly special divisors of the field discriminant, namely only for those which are $\leq n$. Meanwhile precisely these numbers have given the science great and up to now not yet overcome difficulties; and the circumstance that even here the expansions of the roots is essentially the same as for the ordinary ramification points, that therefore those difficulties do not occur here at all, appears to me to be a proof of the merits and necessity of this theory. [12]

Hensel emphasized the fact that his theory was an independent alternative to Dedekind's theory of ideals:

> All these theorems can be established, as will be done in a paper soon to appear in the "Mathematische Annalen," by very simple means, and completely independently of the theory of ideals. [13]

He then went on to explain how the various parts of his theory corresponded to the various parts of ideal theory. [14] Finally, he closed with a statement showing that he was very conscious of the need for his new ideas to compete for acceptance, against the already prominent theory of ideals:

> In two further works the principles explained here will be applied to the solution of several problems, whose solution has not yet succeeded with the help of ideal theory. [15]

---

[12] Eine Ausnahme macht nur der ganz specielle Fall, wenn die Anzahl d der für einen Verzweigungspunkt conjugirten Wurzeln (2a) durch die betrachtete Primzahl p teilbar ist, ein Fall, der nur für ganz specielle Teiler der Körperdiscriminante, nämlich nur für diejenigen vorkommen kann, welche $\leq n$ sind. Indessen haben gerade diese Zahlen der Wissenschaft große und bisher noch nicht überwundene Schwierigkeiten bereitet, und der Umstand, daß also jene Schwierigkeiten hier überhaupt nicht auftreten, scheint mir ein Beweis für die Berechtigung und Notwendigkeit dieser Theorie zu sein.

[13] Alle diese Sätze können, wie in einer demnächst in den "Mathematischen Annalen" erscheinenden Abhandlung dargelegt werden soll, mit sehr einfachen Hülfsmitteln und völlig unabhängig von der Theorie der Ideale begründet werden.

[14] Here we mean ideal theory as a generalization of Kummer's theory of ideal numbers, not as a chapter in ring theory, about subrings with certain closure conditions.

[15] (Hensel 1897c, p. 88) *In zwei weiteren Arbeiten sind die hier auseinandergesetzten Principien auf die*

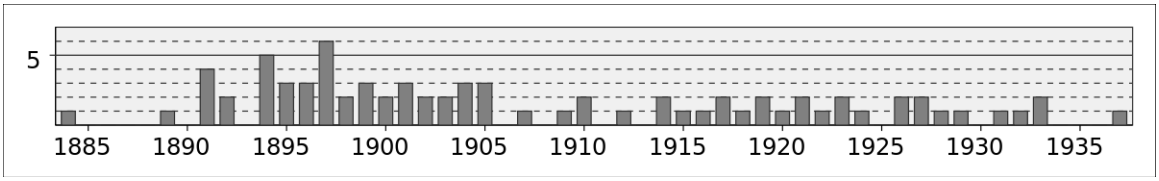

Figure 3.4: Number of papers published by Kurt Hensel each year, from 1884 to 1937. Source: (ibid.).

Thus, while Hilbert's class field conjectures ultimately captured the interest of many important researchers, Hensel had his own game, which he continued to play in the background. He was out of the way, not just in terms of his work but geographically, serving from 1901 until his retirement in 1930 as full professor at the University of Marburg, 130 kilometres south-west of Göttingen, even farther from Berlin, and in no way a major centre for mathematics. Between his first talk on the p-adic numbers in 1897, and the publication of TAZ in 1908, he would publish several papers on the subject. (See Table 3.4 for Hensel's publication histogram, covering all his papers, not just those on the p-adics). His work must certainly have been noticed – it was appearing in *Crelle's Journal*, the oldest mathematical periodical in Germany. Nor should one imagine that Hensel was in any way out of touch with the mathematical world – he was in fact the sole editor in chief of *Crelle* from 1903 to 1928 (and continued on until 1936, with Hasse and L. Schlesinger (1864-1933) sharing the reins). As Ullrich has put it, Hensel was, "a renowned expert both in algebraic number fields and in the theory of algebraic functions" (Ullrich 1998, p. 172). In 1902 he published the book (Hensel and Landsberg 1902) with G. Landsberg (1865-1912) on algebraic function theory.

Still his work on the p-adics seems not to have generated much interest in the broader mathematical community. Sadly for Hensel, the event in which his early work on p-adic numbers seems to have made the greatest impact on popular opinion was an episode in 1906, in which it was demonstrated by Oskar Perron (1880 - 1975) that Hensel had made an error in his claimed proof of the transcendence of e by p-adic methods. The result is that Hensel's p-adics appear to have been regarded widely as an "unfruchtbarer Seitenweg," or

Lösung einiger Aufgaben angewendet worden, deren Lösung mit Hülfe der Idealtheorie noch nicht gelungen war. The two works referred to are (Hensel 1897a) and (Hensel 1897b).

"unfruitful sidetrack," [16] an opinion which would be reversed in 1922 with Hasse's local-global theorem, which we return to below. [17]

In the meantime, Hilbert was leading the march. If in 1898 his class field conjectures charted a course for number theory, his famous list of unsolved problems stated at the Second International Congress of Mathematicians at Paris in 1900 did likewise for the whole of mathematics. Among the twenty-three problems, the ninth enunciated the other side of number theory, running parallel to the class field conjectures, namely, "To state and prove the most general reciprocity law."

Arguably, this last problem had been the core motivation in algebraic number theory from the beginning. Lemmermeyer [18] for example has written that "The history of reciprocity laws is a history of algebraic number theory." [19] Edwards (Edwards 1977, p. 79) has argued convincingly that even Kummer in his invention of ideal divisors was motivated not by Fermat's Last Theorem, as is often supposed, but rather by the goal of exploring reciprocity laws, as prompted by an article of Jacobi (Jacobi 1839b).

Number theorists working in the early 20th century understood that the studies of class field theory and of the reciprocity law were intimately related, a fact which has been stated again and again in the literature. In a paper (Furtwängler 1906) on the existence of the Hilbert class field, for example, Furtwängler would refer to

> ... the study of the reciprocity law in arbitrary algebraic number fields, which in terms both of content and of method is of the closest connection with the theory of class fields ... [20]

Hasse, at the very opening of Part I of his *Klassenkörperbericht* of 1927 wrote,

> Since the appearance of *Hilbert*'s "Zahlbericht" (Jahresbericht der Deutsch-etc., 1897) as well as his two fundamental works:

---

[16] This is related by Hasse, in (Hasse 1975, p. VIII).

[17] See (Ullrich 1998) for discussion of this.

[18] Lemmermeyer (b. 1962) earned his PhD for the dissertation *Die Konstruktion von Klassenkörpern* ("The Construction of Class Fields") at the University of Heidelberg in 1995, under Peter Roquette (b. 1927), who studied under Hasse, PhD 1953 at the University of Hamburg, for the dissertation *Arithmetischer Beweis der Riemannschen Vermutung in Kongruenzfunktionenkörpern beliebigen Geschlechts* ("Arithmetic Proof of the Riemann Hypothesis in Congruence Function Fields of arbitrary Genus").

[19] Lemmermeyer outlines the history in the Preface to (Lemmermeyer 2000).

[20] *... das Studium der Reziprozitätsgesetze in beliebigen algebraischen Zahlkörpern, das sowohl inhaltlich wie methodisch mit der Theorie des Klassenkörpers auf das engste zusammenhängt ...*

"On the Theory of the relative-quadratic number field" (Hilbert 1899)

"On the Theory of the relative-Abelian number field" (Hilbert 1898) [21]

algebraic number theory is represented by the following two big, closely linked problems:

1. Proof of the existence of the class field of an arbitrary algebraic number field,
2. Proof of the reciprocity law of the power residues for an arbitrary prime number exponent ℓ in an arbitrary extension field of the field of ℓth roots of unity.

Ultimately the pursuit of class field theory would indeed lead to Artin's reciprocity law of 1927, which would be considered the fulfilment of Hilbert's ninth problem, at least in the case of Abelian extensions. In this sense Hilbert can be viewed as having led the charge in the mainstream pursuit of algebraic number theory in this era. If we seek to understand *why* this cluster of questions captured the imagination of so many mathematicians, perhaps the simplest explanation is that the reciprocity law represented a long-standing mystery, whose importance had been trumpeted by Gauss.

3.2 Existence and construction of class fields

For several reasons, we must now review the class field conjectures of Hilbert, and the work done on these problems by Furtwängler. To begin with, this forms one of the main chapters in the story of algebraic number theory. While it will certainly represent a large hole in that story for us to forgo an equally detailed discussion of T. Takagi's (1875-1960) work, unfortunately to include a proper treatment would lead us too far from our focus, and so we must leave it out, except for a brief discussion at the end of this section. We must make ourselves familiar with Furtwängler on the other hand, since he was the doctoral advisor to Olga Taussky, who will play a major part in the story we recount. In Hilbert and Furtwängler moreover we find *singular primary numbers*, objects which fell into disuse in class field theory as early as Takagi, but which will reappear for us when we examine

[21] Hilbert's work on relative-quadratic fields was fundamental for his work on relative-Abelian fields, but was published later, surely because its great size simply made the publishing process more laborious.

Hasse's constructive work, namely, in his work on the construction of Hilbert class fields with Zassenhaus and Liang in the 1960s.

The basic facts of Furtwängler's life are recounted by his student Anton Huber (PhD 1924) in a memorial article (Huber 1940). English-language biographies of Furtwängler seem scant at present, so let us review at least a little of his story here. Furtwängler was born in the little town of Elze, Germany, on 21 April 1869. In Easter 1889 he passed the university entrance examinations and began his studies at the University of Göttingen. There he took courses under Hölder, Schönflies, and Klein, among others, the last of whom was Furtwängler's doctoral advisor, for the dissertation, *Zur Theorie der in Linearfaktoren zerlegbaren ganzzahligen ternären kubischen Formen* (On the theory of integral ternary cubic forms decomposable into linear factors) of 1896.

While best known for his work in number theory, Furtwängler also worked in other areas, and began his scientific career at the geodätischen Institut, or Institute of Geodesy, in Potsdam, in the year 1897. He was appointed to a teaching position in 1903 at the agricultural academy in Bonn, returned there after a post as lecturer from 1907 to 1910 at the Technischen Hochschule in Aachen, and finally in 1912 followed a call to the University of Vienna, as successor to Franz Mertens (1840 - 1927). He retired in the winter semester of 1937/1938 due to failing health, and died of a stroke on 19 May 1940.

From 1927 Furtwängler was a member of the Akademie der Wissenschaften in Vienna, and from 1931 corresponding member of the Prussian Akademie der Wissenschaften in Berlin. Among his PhD students at the University of Vienna were Wolfgang Gröbner, whose own student Bruno Buchberger would name Gröbner bases after him; Henry Mann, who would be a collaborator with Zassenhaus at the Ohio State University; Otto Schreier, of the Schreier Refinement Theorem; and of course Olga Taussky, to whom we will return shortly.

The oft mentioned close connection between the two problems of the general reciprocity law in algebraic number fields, and the existence of the class field, was, as Huber writes, apparent in the alternation back and forth between these two problems in the relevant publications of Furtwängler, in their historical sequence of appearance. Furtwängler would concern himself with these problems actively for thirty years (ibid.). He achieved notable results on the reciprocity law in papers published between 1902 and 1927, but his work was soon overshadowed by Artin's 1927 reciprocity law. Again, he proved the existence of the Hilbert class field in papers published in 1903 and 1904, only to have this result

overshadowed by Takagi's proof of the existence of the general class field. [22]

One major result of Furtwängler that was *not* to be outdone by any of his contemporaries was his proof of the *principal ideal theorem*, which states that every ideal in an algebraic number field k becomes principal in that field's Hilbert class field K. Furtwängler proved this in 1930 (Furtwängler 1930), thus achieving what is commonly regarded as the final and concluding result in the classical phase of class field theory. Hasse, for one, referred to it as "a particularly beautiful coronation" to the theory (*"eine besonders schöne Krönung"*) (Hasse 1965, p. 2), and wrote that,

> Therewith is the last, and one can say even the most popular, of the claims made by Hilbert for the (absolute) class field, now finally proved. (ibid.)

Meanwhile, according to Lang (Lang 1970, p. 176), it is instead *Artin reciprocity* that is to be viewed as "completing the basic statements of class field theory," so, between Lang and Hasse at least, there is some disagreement on this.

For us, Furtwängler's construction of the Hilbert class field remains of great interest, even given Takagi's more general existence proof, since here, as in Hilbert's own work on the quadratic case, the construction was achieved by means of an object called a *singular primary number*, which Hasse would later revive for his own constructive work in computational algebraic number theory, after its having vanished from mainstream class field theory. Takagi's proof, on the other hand, was not constructive.

We are lucky to have occasion to review this construction, for, as Lang wrote in the closing of his brief overview of the history of class field theory in (ibid.),

> If there is one moral which deserves emphasis, however, it is that no one piece of insight which has been evolved since the beginning of the subject has ever been "superseded" by subsequent pieces of insight. They may have moved through various stages of fashionability, and various authors may have claimed to give so-called "modern" treatments. You should be warned that acquaintance with only one of the approaches will deprive you of techniques and understandings reflected by the other approaches....

[22] Takagi's work was published in Japan in 1920 (Takagi 1920), but did not come to the attention of German mathematicians until 1922. We elaborate on this story at the end of this section.

Before beginning, we must first briefly recount the path that led to Furtwängler's work. We begin with Hilbert, and the concept of the class field.

The monumental stature of Hilbert's work in algebraic number theory is only accentuated by the fact that all of his publications on the subject appeared in the short period between 1894 and 1899. He produced a great amount of material in this time. After his *Zahlbericht*, he published one more work of large size, his *Über die Theorie des relativquadratischen Zahlkörpers*, of 1899. In this treatise of 127 pages, Hilbert worked out the theory of extension fields of degree 2 over an arbitrary base field. In this most basic case, to quote the mathematician himself (though he spoke perhaps at a different time, and on a different subject), Hilbert found "all the germs of generality," so that he could go on to publish the much shorter *Über die Theorie der relativ-Abelschen Zahlkörper* (27 pages), in which he stated conjectures generalizing what he had learned about the quadratic case. These conjectures would guide the future development of class field theory.

In order to understand the purpose of singular primary numbers, we must review the context in which they were used. What exactly is a class field, and what was the purpose of constructing one?

Class field theory had its roots in work of Kronecker, and of Weber, and when Hilbert gave his 1897 DMV talk he cited several works of Weber. [23] One major result in the theory even bears their names, the "Kronecker-Weber theorem", which states that every Abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension, i.e. a field of the form $\mathbb{Q}(\zeta)$ where ζ is a root of unity. According to Hilbert (Hilbert 1981a, p. 53), Kronecker had stated this result in 1853, in the form that the roots of all Abelian equations over the rational numbers can be expressed as rational functions in roots of unity, but it seems he did not give a proof. The first complete proof is attributed to Weber (Weber 1886), who used transcendental methods. Hilbert gave an alternative proof in (Hilbert 1896), of a more purely arithmetic nature. Also notable is Kronecker's *Jugendtraum* ("dream of his youth"), which refers to his dream of showing that all Abelian extensions over imaginary quadratic base fields are generated in a certain way.

The notion of a "class field" changed over the years, eventually returning to a definition

[23] References were to a three part work of Weber that appeared in issues of the *Mathematische Annalen* in 1897 and 1898 (Weber 1897) (the DMV proceedings were not published until 1899, so Hilbert might have added the reference in proof), and to Weber's 1891 book *Elliptische Funktionen und algebraische Zahlen* (Weber 1891), which in its second edition would be subsumed as Volume III of Weber's monumental *Lehrbuch der Algebra*. See (Frei 1989) for more about Weber's work.

closer to what Weber had stated, prior to Hilbert (see (Hasse 1967)), under which a field had many extensions which would be called class fields over it. In Hilbert's work however a number field had just one extension field called its "class field," the name arising from the fact that the Galois group of this extension was isomorphic to the base field's ideal class group. Since then, this particular extension has come to be known as the "Hilbert class field."

As the title of Hilbert's talk, "On the Theory of relative-quadratic Number fields," indicates, Hilbert's purpose was to study relative-quadratic number fields, not class fields. On the contrary, the latter arise naturally as an object of study when one sets out to study the former; at least, this happens if one is Hilbert.

Likewise, the class field concept arises again in a later paper of Hilbert, "On the Theory of relative-Abelian Number fields," the paper in which he makes his famous class field conjectures. And here again, Hilbert's primary goal was to master the extension fields of a given type over an arbitrary base field, in this case, the Abelian extensions. The class field enters the picture as the largest extension of the type in question, where "largest" simply means that it contains all the others of this type. In (ibid., p. 269), Hasse emphasizes that Hilbert's conception was quite different from that of Kronecker and Weber, who had viewed class field theory instead as a means toward generalizing Dirichlet's prime number theorem, and toward proving the theorem named after them. Neumann (Neumann 2007, p. 87) suggests that Kronecker's motivation was to construct a field in which all ideal elements were represented by numbers, which again appears different from Hilbert's motivation.

Let us review now the definition of the class field that Hilbert gave in his DMV talk. *Here he worked in a relatively restricted context, namely, in the case in which the base field k is assumed, along with all its conjugate fields, to be imaginary, and to have class number* 2. His definition is therefore quite different from the one we would recognize today. He wrote,

> ... In fact the proof then succeeds for the existence of a relative field K with the relative discriminant 1. This field will be named the *class field* of k. The class field K has the following fundamental properties:
>
> 1. The class field K has with respect to k the relative discriminant 1.
> 2. The class number of the class field K is odd.

3. (a) Those prime ideals in k which are principal ideals decompose in K in the product of two prime ideals.

   (b) Those prime ideals in k which are not principal ideals remain prime in K; they are however principal ideals in K.

Of these four properties 1, 2, 3a, 3b, each alone, by our assumptions, defines uniquely the class field K; we have therefore the theorems:

1. There is besides K no other relative quadratic field with the relative discriminant 1 with respect to k.
2. If a relative quadratic field to k has an odd class number, then it coincides with the class field K.
3. If all prime ideals in k, which in k are principal ideals, decompose in a relative quadratic field, or if all prime ideals in k, which in k are not principal, remain prime in a relative quadratic field, then it follows every time that this relative quadratic field is none other than the class field K.

These laws for the class field K are capable of a broad generalization; they indicate a wonderful harmony, and open up, as it appears to me, a world rich in new arithmetic truths. (Hilbert 1981b, p. 369)

While in this context the class field is the one and only unramified quadratic extension of the base field, Hilbert at this time already had in his sights the more general question of unramified Abelian extensions of any relative degree. He said, at the end of his talk,

> We have restricted ourselves in this lecture to the study of relative Abelian fields of the *second* degree. This restriction is however only a provisional one, and since the methods I applied in the proofs of the theorems are all capable of generalization, it may therefore be hoped that the difficulties will not be insurmountable, which the founding of a general theory of relative Abelian fields presents. [24]

[24] (Hilbert 1981b, p. 369) Wir haben uns in diesem Vortrage auf die Untersuchung relativ Abelscher Körper vom *zweiten* Grad beschränkt. Diese Beschränkung ist jedoch nur eine vorläufige, und da die von mir bei den Beweisen der Sätze angewandten Schlüsse sämtlich der Verallgemeinerung fähig sind, so steht zu hoffen, daß die Schwierigkeiten nicht unüberwindliche sein werden, die die Begründung einer allgemeinen Theorie der relativ Abelschen Körper bietet.

When Furtwängler later proved the existence of the class field in this more general context, it was characterized in the following way, which will appear more familiar to readers acquainted with more modern renditions of class field theory:

> The class field of an arbitrary base field k is an extension field thereof, displaying the following characteristic properties:
>
> 1. Its Galois group over k is isomorphic to the group of ideal classes in k; it is thus relative-Abelian with respect to k.
> 2. It is unramified over k, i.e. its relative discriminant is equal to 1.
> 3. All ideals of the base field are principal ideals in the class field; they are thus represented by actual numbers of the class field.
> 4. All prime ideals belonging to one and the same class of the base field decompose in the same way in the class field, or, more precisely: If the class number of the base field is h, and if g is the smallest exponent for which the equivalence $\mathfrak{p}^g \sim 1$ is satisfied in k, then the prime ideal $\mathfrak{p}$ of k decomposes in the class field in $\frac{h}{g}$ distinct prime factors. (Furtwängler 1906, p. 2)

With this background in place, we can now understand the purpose of the construction that Hilbert performed in (Hilbert 1898), and which Furtwängler would later generalize, referring to the key numbers involved as "singular primary numbers." Namely, if ω is a singular primary number in k, then $k(\sqrt{\omega})$ will be the Hilbert class field over k in the quadratic case. When Furtwängler considered the general case, he first reduced the problem to the construction of a cyclic extension of prime degree ℓ, and then performed a construction that was perfectly analogous to Hilbert's, so that the extension field was obtained as $k(\sqrt[\ell]{\omega})$.

Since the construction in Hilbert's quadratic case is simpler than that performed by Furtwängler in the general case, we review the former here. There are several steps involved, which were carried out by Hilbert as enumerated below. We note that there is an error in steps 4 and 5, in that $\varepsilon_{\frac{m}{2}}$ should be a generator of all roots of unity in k, which might easily be other than -1, in order for every integer ξ to be representable in the form stated. The error is fixed in Furtwängler's more general treatment (Furtwängler 1906, pp. 7-8).

1. Introduce a system of fundamental units $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\frac{m}{2}-1}$ for k. Note that it follows from Dirichlet's unit theorem and from the assumption that k and all of its conjugate fields are imaginary that, indeed, the number of fundamental units in k must be $\frac{m}{2} - 1$.

2. Introduce a prime ideal $\mathfrak{r}$ of k which is prime to 2, and which is not principal in k

3. Introduce an integer ρ of k such that $\mathfrak{r}^2 = (\rho)$.

4. Define $\varepsilon_{\frac{m}{2}} = -1$ and $\varepsilon_{\frac{m}{2}+1} = \rho$.

5. Observe that every integer ξ of k which is the square of an ideal of k can be represented in the form

$$\xi = \varepsilon_1^{x_1}\varepsilon_2^{x_2}\cdots\varepsilon_{\frac{m}{2}+1}^{x_{\frac{m}{2}+1}}\alpha^2,$$

where the exponents $x_1, x_2, \ldots, x_{\frac{m}{2}+1}$ have certain values $0, 1$, and α is an integral or fractional number in k.

6. With existence guaranteed by Theorem 18 of Hilbert's earlier treatise on relative quadratic fields[25], introduce a system of prime ideals $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_{\frac{m}{2}+1}$ in k, which are prime to 2, so that

$$\left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right) = -1, \quad \left(\frac{\varepsilon_j}{\mathfrak{q}_i}\right) = +1, \quad (i \neq j) \qquad \left(i, j = 1, 2, \ldots, \frac{m}{2}+1\right).$$

7. Introduce exponents $w_1, \ldots, w_{\frac{m}{2}+1}$ with values $0, 1$ such that the products

$$\mathfrak{q}_1\mathfrak{r}^{w_1}, \mathfrak{q}_2\mathfrak{r}^{w_2}, \ldots, \mathfrak{q}_{\frac{m}{2}+1}\mathfrak{r}^{w_{\frac{m}{2}+1}}$$

are principal ideals in k. In particular, introduce integers $\chi_1, \ldots, \chi_{\frac{m}{2}+1}$ of k such that

$$\mathfrak{q}_1\mathfrak{r}^{w_1} = (\chi_1), \ldots, \mathfrak{q}_{\frac{m}{2}+1}\mathfrak{r}^{w_{\frac{m}{2}+1}} = \left(\chi_{\frac{m}{2}+1}\right).$$

8. Consider the expression

$$\varepsilon_1^{u_1}\cdots\varepsilon_{\frac{m}{2}+1}^{u_{\frac{m}{2}+1}}\chi_1^{v_1}\cdots\chi_{\frac{m}{2}+1}^{v_{\frac{m}{2}+1}}, \tag{3.1}$$

in which the exponents $u_1, \ldots, u_{\frac{m}{2}+1}$ take on arbitrary values $0, 1$, and the exponents $v_1, \ldots, v_{\frac{m}{2}+1}$ such values $0, 1$ as satisfy the congruence

$$v_1w_1 + v_2w_2 + \cdots + v_{\frac{m}{2}+1}w_{\frac{m}{2}+1} \equiv 0 \bmod 2.$$

Observe that there are 2^{m+1} such numbers.

[25] Über die Theorie des relativquadratischen Zahlkörpers

9. Define two integers ω_1, ω_2 of k prime to 2 to be *of the same kind*, when their product $\omega_1\omega_2$ is a *primary* number. [26]

10. Observe that it follows from considerations at the end of §21 of (Hilbert 1899) that the integers of k fall into precisely 2^m different kinds.

11. Note that therefore there must be two distinct numbers of the form (3.1) that are of the same kind. The product of two such numbers is a primary number of the form

$$\omega = \varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}+1}^{u_{\frac{m}{2}+1}} \chi_1^{v_1} \cdots \chi_{\frac{m}{2}+1}^{v_{\frac{m}{2}+1}} \alpha^2$$

    where the exponents u_i, v_j have certain values 0, 1, but are not all equal to 0, and α denotes an integer of k.

12. Hilbert notes that this number is *primary*. Furtwängler will later apply the descriptor "singular" to a primary number of this particular form.

Finally, the definition of a mathematical object is never enough to give insight into why it is an object of importance, or why it should have been constructed in the way that it was; these reasons emerge only in the course of a proof in which such an object plays a critical role. We therefore conclude our study of the singular primary number here by explaining the outline of Hilbert's proof that $k(\sqrt{\omega})$ is the class field over k, and also filling in some of the gaps that Hilbert left in the proof.

Let

$$\omega = \varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}+1}^{u_{\frac{m}{2}+1}} \chi_1^{v_1} \cdots \chi_{\frac{m}{2}+1}^{v_{\frac{m}{2}+1}} \alpha^2$$

with $\alpha \in \mathcal{O}_k$, $u_i, v_j \in \{0, 1\}$ be a primary number. Then $\omega \in \mathcal{O}_k$, $(\omega, 2) = 1$, and we have $\omega \equiv \beta^2 \bmod 2^2$ for some $\beta \in \mathcal{O}_k$, since ω is primary. Then we prove that $k(\sqrt{\omega})$ is an unramified quadratic extension over k.

The basic structure of the proof is a case split, in which we assume either that $v_1, \ldots, v_{\frac{m}{2}+1}$ are all zero, or that this is not the case. In the first case, we demonstrate why it is that by

[26] In this context, an algebraic integer α in a number field k is called primary when it is relatively prime to 2, and is congruent to the square of an algebraic integer in k modulo 2^2. Observe that Hilbert writes "2^2", not "4," as a way of anticipating the appropriate generalization beyond the quadratic case.

Note meanwhile that notions of "primariness" had been around at least since Kummer, and that a great number of variations on the idea have been used. Compare Lemmermeyer, who writes (Lemmermeyer 2000) p. xiv, "the sheer multitude of definitions prohibits the introduction of a globally consistent notion of primariness."

adjoining the square root of such a number ω we get the class field over k. The remainder of the proof – and by far most of the work – consists in deriving a contradiction in the second case, and thereby ruling this case out.

We give here the proof for the first case, namely, that $K = k(\sqrt{\omega})$ is an unramified quadratic extension of k, when the v_i are all zero.

There are two things to confirm: (1) that $\sqrt{\omega} \notin k$, so that K is in fact a quadratic extension, and (2) that K is unramified over k, that is, that no ideal of k divides the relative discriminant $\mathfrak{d}$ of K over k.

(1) We suppose that $\gamma = \sqrt{\omega}$ is in k and derive a contradiction. Let $\eta = \varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}}$, so that $\omega = \eta \varepsilon_{\frac{m}{2}+1}^{u_{\frac{m}{2}+1}}$. Now suppose first that $u_{\frac{m}{2}+1} = 1$. Then we have $(\gamma^2) = (\rho)$, so that $(\gamma^2) = \mathfrak{r}^2$, and we get $(\gamma) = \mathfrak{r}$ by unique factorization into ideals. This contradicts the assumption that $\mathfrak{r}$ is not principal. Thus we must have $u_{\frac{m}{2}+1} = 0$. But in this case we have $\omega = \eta$, a unit, so $\gamma | \omega$ says γ is also a unit. Then by the Dirichlet unit theorem we can write $\gamma = \varepsilon_1^{t_1} \cdots \varepsilon_{\frac{m}{2}}^{t_{\frac{m}{2}}}$ for some integers $t_1, \ldots, t_{\frac{m}{2}}$. From $\gamma^2 = \omega$ we then have $\varepsilon_1^{2t_1} \cdots \varepsilon_{\frac{m}{2}}^{2t_{\frac{m}{2}}} = \varepsilon_1^{u_1} \cdots \varepsilon_{\frac{m}{2}}^{u_{\frac{m}{2}}}$, but since at least one of the u_i is equal to 1, this contradicts the uniqueness clause in the Dirichlet unit theorem.

(2) In order to show that K is unramified over k, we let an arbitrary prime ideal of k be given, and show that it does not divide the relative discriminant $\mathfrak{d}$ of K over k. To this end we use Theorems 4 and 5 from Hilbert's treatise on relative quadratic number fields (Hilbert 1899). In the proof in RAZ Hilbert does nothing more than cite these two theorems. We fill in the gaps here.

The theorems run as follows, in terms of an extension $K = k(\sqrt{\mu})$ of k with relative discriminant $\mathfrak{d}$:

> Theorem 4. Let $\mathfrak{p}$ be a prime ideal of the field k, prime to 2. If then $\mathfrak{p}$ divides the number μ to precisely the a^{th} power, then $\mathfrak{d}$ is prime to $\mathfrak{p}$ if and only if a is even.
>
> On the other hand, let $\mathfrak{l}$ be a prime ideal of k that divides 2 to precisely the ℓ^{th} power (ℓ positive), and that divides μ to precisely the a^{th} power. Then $\mathfrak{d}$ is prime to $\mathfrak{l}$ if and only if there is an integer α in k for which we have
>
> $$\mu \equiv \alpha^2 \quad \left(\mathfrak{l}^{2\ell+a}\right).$$
>
> Theorem 5. If μ is an integer of k which is prime to 2, and which is not the

square of any number in k, then $\mathfrak{d}$ is prime to 2 if and only if μ is congruent to the square of an integer of k mod 2^2.

Thus, since we have just shown in step (1) that ω is not the square of an integer in k, and since ω is primary, it follows directly from Theorem 5 that $(\mathfrak{d}, 2) = 1$. We therefore are left only to consider a prime ideal $\mathfrak{p}$ of k that is prime to 2, and to show that it must be prime to $\mathfrak{d}$. Supposing that $\mathfrak{p}$ divides ω to precisely the a power, we recall that $\omega = \eta\rho^{u_{\frac{m}{2}+1}}$, where $u_{\frac{m}{2}+1}$ is either 0 or 1. If $u_{\frac{m}{2}+1} = 0$, then $a = 0$ as well. If $u_{\frac{m}{2}+1} = 1$, then a is even since $(\rho) = \mathfrak{r}^2$. Therefore in any case a is even, so by Theorem 4 we find that $(\mathfrak{d}, \mathfrak{p}) = 1$, as desired. It follows thus that K is an unramified extension of k.

By generalizing the methods of Hilbert, Furtwängler was able to demonstrate the existence of the Hilbert class field in general. His proofs were constructive like Hilbert's, in that he showed how to generate a cyclic class field of prime degree ℓ over its base field, by adjoining an ℓ^{th} root of a singular primary number ω. A more general, but less constructive existence proof for class fields was later to be achieved by Takagi.

Teiji Takagi (1875 - 1960) was a gifted student of mathematics who had recently begun graduate studies at the Imperial University in Tokyo after having obtained his undergraduate degree there in 1897, when he was awarded a government scholarship to study for three years in Germany. He chose to spend the first half of that time in Berlin, and the second half in Göttingen. (Edwards 2008b)

During his time in Berlin he read Hilbert's *Zahlbericht*, and became interested in the class field theory program, as enunciated in Hilbert's post-*Zahlbericht* work. By the time he made it to Göttingen however, Hilbert had moved on from number theory, and so Takagi had little direct influence from him. He returned home to Tokyo in December 1901, and completed his doctorate at the Imperial University in Tokyo in December 1903, on the basis of work done while in Göttingen, on the Kronecker *Jugendtraum*. (ibid.)

On his own, in Tokyo, Takagi worked through World War I on Weber's version of class field theory, which involved generalized ideal class groups and generalized class fields (instead of just the usual ideal class group and the Hilbert class field). He came up with major results which answered all but a few of the main questions in class field theory. Due to the disruption of communication during the war, and a few false starts in finding recognition afterward, it was not until Artin read one of Takagi's papers in 1922 that the significance of his work was discovered by the mathematical community at large. (ibid.)

3.3 Reciprocity laws

3.3.1 Artin's law, explicit laws

The early 1920s were a time full of possibilities for number theory. The major class field conjectures had already been proved by Takagi, but local methods had just been established as a powerful tool, and there was the potential to apply them to this theory, even if in the course of history this was an avenue that would be explored only in the subsequent decade. Hilbert's Ninth Problem remained unresolved, meanwhile, and this became a hotly pursued goal.

Emil Artin and Helmut Hasse entered the world in the same year that Hilbert's RAZ was published, 1898. Artin was born March 3, in Vienna, and Hasse August 25, in Kassel, Germany. In their twenties they would each pursue the answer to Hilbert's Ninth Problem. As Lemmermeyer writes (Lemmermeyer 2000),

> Between 1923 and 1926, Artin and Hasse were looking for simpler (and more general) formulations of Takagi's reciprocity law in the hope that this would help them finish Hilbert's quest for the "most general reciprocity law" in number fields.

Both mathematicians devoted a good deal of effort to the problem, before Artin arrived at the decisive victory in 1927. According to Lemmermeyer (my emphasis),

> In a way, Artin's reciprocity law closed the subject (*except for the subsequent work on explicit formulas*, not to mention ... dramatic progress into non-Abelian class field theory ...), and the decline of interest in the classical reciprocity laws was a natural consequence. (ibid.)

Indeed, Hasse continued to work on explicit reciprocity laws after this time, i.e. he worked on the problem of computing the functions that appear in the expression of the reciprocity law (in a form that we will consider below). As he wrote in (Hasse 1929), he had already dedicated a long series of works to the question before 1927.

Hasse explained his interest in explicit reciprocity laws in a letter of 1931 to Hermann Weyl:

> I recollect very well your first words to me on the occasion of my lecture in Innsbruck on the first explicit reciprocity formula for higher exponents. At that

> time you expressed some doubts about the essential justification of such investigations, by marshaling the argument that it is precisely Hilbert's achievement to have freed the theory of the reciprocity law from the explicit computations of former researchers, in particular, those of Kummer. ... I can well understand that things such as these explicit reciprocity formulas speak less to a man of your high intellect and taste than to me as I am never entirely satisfied by the abstract mathematics of the Dedekind-E. Noether kind, at least until I can also place next to it an explicit formula based on a constructive treatment. Only against the latter can the elegant methods and beautiful ideas of the former really profitably stand out. [27]

Nor was Hasse's interest in explicit reciprocity laws any passing fancy: he returned to the problem in 1961, after about thirty years away from it, in (Hasse 1961). Moreover, he awarded his student Helmut Brückner at the University of Hamburg a PhD in 1965 for the dissertation, *"Eine explizite Formel für das p-te Normsymbol in diskret bewerteten vollständigen Körpern der Charakteristik 0 mit vollkommenem Restklassenkörper der Charakteristik p"* ("An explicit Formula for the p^{th} Norm Symbol in discrete valued complete Fields of Characteristic 0 with perfect Residue Class Field of Characteristic p"). As another mathematician, S.V. Vostokov, wrote in a paper on this subject in 1978,

> The explicit calculation of the reciprocity law for an algebraic number field reduces [reference to Hasse's *Klassenkörperbericht* Part II] to the calculation of the Hilbert norm residue symbol in a local field (a finite extension of the p-adic field $\mathbb{Q}_p$. (Vostokov 1978, p. 198)

3.3.2 Hasse

In 1913 Hensel published his second book working out parts of number theory in the medium of p-adic numbers. This time he treated elementary number theory. His book, *Zahlentheorie*, seems not to have attracted any more notable attention than did TAZ, at least, until it attracted the attention of Hasse.

Fifteen years of age when the book was published, Hasse eventually, and serendipitously, discovered the book in a secondhand bookshop in Göttingen at the age of 21 in the spring

[27] Translated in (Schwermer 2007, pp. 172-173).

of 1920. [28] By his own account, so taken was he by the novelty of Hensel's methods, that he decided to complete his PhD studies in Marburg. It was a fateful decision, resulting in his proof of the *local-global principle* for his PhD dissertation of 1922, the idea for which he insists was in part inspired by Hensel:

> I feel urged to make only one remark, namely that I did not "devise" the *Local-Global-Principle*, as the publisher has said. Much more, it was "suggested" to me by my teacher *Kurt Hensel*. [29]

This Hasse wrote in 1975, at the age of 77. At the very beginning of his career too, he characterized his PhD problem as being entirely Henselian:

> The question that concerns us here ... is typical for the entire approach introduced by Mr. Hensel, not only here with binary quadratic forms, but also generally in all such studies. [30]

Hasse's theorem, as stated in the 1923 publication in *Crelle* based on his doctoral thesis, ran as follows:

> Fundamental theorem: For a rational number m to be rationally representable by a quadratic form f with rational coefficients, it is necessary and sufficient that m be representable by f in all $K(p)$. [31]

Here $K(p)$ is Hensel's notation for the field of p-adic numbers, which we would today denote by $\mathbb{Q}_p$.

Finally, in closing his introductory section, Hasse referred to his result as,

> ... this theorem, which clearly reveals the fruitfulness of the *Hensel*ian ("p-adic") approach ... [32]

---

[28] The story is recounted by Hasse in his foreword to his own collected works. (Hasse 1975, p. VIII).

[29] Nur eines drängt es mich zu bemerken, daß ich nämlich das *Lokal-Global-Prinzip* nicht, wie die Herausgeber sagen, "ersonnen" habe. Vielmehr ist es mir durch meinen Lehrer *Kurt Hensel* "suggeriert" worden. (ibid., p. VIII)

[30] Diese hier auftretende Frage ... ist typisch für die ganze durch Herrn *Hensel* eingeleitete Behandlungsweise, nicht allein hier bei den binären quadratischen Formen, sondern auch allgemein bei allen derartigen Untersuchungen. (Hasse 1923)

[31] Fundamentalsatz: Damit eine rationale Zahl m durch eine quadratische Form f mit rationalen Koeffizienten rational darstellbar ist, ist notwendig und hinreichend, daß m durch f in allen $K(p)$ darstellbar ist. (ibid.)

[32] ... diesen Satz, der die Fruchtbarkeit der *Hensel*schen ("p-adischen") Behandlungsweise klar hervortreten läßt...

Was Hasse's mention of this "Fruchtbarkeit" perhaps a deliberate retort to the "unfruchtbar Seitenweg" he had been cautioned against getting involved with, before leaving Göttingen?

This was a major victory for p-adic methods. Up to this point they had been at best a curiosity. Now they were a fundamental tool, needed in order to prove a major theorem. Hasse would moreover go on, with others such as Chevalley, to reformulate class field theory in the 1930s on the basis of a local framework, work foreshadowed by his dissertation. By the time of his talk on the history of class field theory toward the end of his career in 1967 (Cassels and Fröhlich 1967), he would be able to say,

> Thus one can say that by Chevalley's ideas (not to say: idèles) the *local-global principle* has taken root in class field theory.

3.3.3 Artin

Emil Artin, after having begun his studies at the University of Vienna around 1916, was called away to military service after only one semester, and returned to studies only in January 1919, now at the University of Leipzig. There he worked with Herglotz, and received his PhD in 1921 for the dissertation, *Quadratische Körper im Gebiete der höheren Kongruenzen* ("Quadratic Fields in the Domain of higher Congruences") (Schoeneberg 2008).

His first employment was at the University of Göttingen, but he stayed for only one year before moving to the University of Hamburg. There he was appointed lecturer in 1923, extraordinary professor in 1925, and ordinary professor in 1926, a position he held until he emigrated to the U.S. in 1937. Thus, it was in Hamburg that he would do his work in the 1920s on the reciprocity law (ibid.).

Before proving his reciprocity law in 1927 in (Artin 1927), which he himself had conjectured and proven special cases of four years earlier in (Artin 1923), Artin published a paper (Artin and Hasse 1925) on the reciprocity law in collaboration with Hasse, in 1925.

3.3.4 Explicit reciprocity laws

After the appearance of Artin's reciprocity law, Hasse wrote in 1929, in a paper entitled *Zum expliziten Reziprozitätsgesetz*, that the further problem remained to express this law in *explicit* formulae, which should be "in the broadest sense" ("*im weitesten Sinne*") analogous to the familiar explicit formulae for the quadratic reciprocity law in the field of rational numbers. (I.e. the formulae relating Legendre symbols in terms of powers of -1.)

For m^{th} power reciprocity, Hasse indicated that the laws should have the form

$$\left(\frac{\alpha}{\beta}\right) : \left(\frac{\beta}{\alpha}\right) = \zeta^{f(\alpha,\beta)}$$
$$\left(\frac{\varepsilon}{\alpha}\right) = \zeta^{g_\varepsilon(\alpha)}$$
$$\left(\frac{\lambda}{\alpha}\right) = \zeta^{h_\lambda(\alpha)}$$

and stated that,

> The problem named then lies therein, to seek for these functions [$f(\alpha,\beta)$, $g_\varepsilon(\alpha)$, and $h_\lambda(\alpha)$] the simplest possible computable expressions. [33]

We find here a perfect example of the way in which the computational and the conceptual approaches can sometimes truly be diametrically opposed to one another, promoting opposing formulations of one and the same subject matter, for entirely contrary reasons. This moreover will prove to be a case in which Hasse's opposition to Hilbert, which as we have seen he will state in his own words in the Foreword to KAZ, comes to the fore. For it was in his 1897 DMV talk that Hilbert wrote:

> The quadratic reciprocity law in the domain of the rational numbers runs familiarly:
>
> $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$
> $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$
>
> where p, q denote arbitrary odd rational positive prime numbers. But this form of the reciprocity law is, as soon as we put before us the goal of the generalization thereof, on many grounds – I note here only the muddled form of the exponents, the lack of unity, and the exceptional role of the number 2 – an imperfect one.

This talk serves as preamble to Hilbert's introduction of his norm-residue symbol, through which the reciprocity law takes on a especially clean formulation.

Thus, Hasse's call for a return to the familiar explicit formulation of the reciprocity law came about thirty years after Hilbert's insistence on a necessary departure from the very same thing.

---

[33] *Die genannte Aufgabe besteht dann darin, für diese Funktionen möglichst einfache rechnerische Ausdrücke aufzusuchen.*

The opposition between the conceptual and computational approaches, particularly as it is expressed through this example, throws into sharp relief a key phrase in Hilbert's statement, which explains what *non-computational* mathematics, at least in part, and at least in number theory, was about. As we mentioned in Section 2.2, since the most obvious thing one would do in mathematics is compute, we must take some care to explain what it is that mathematicians were doing when they were doing something else. Hilbert motivates his formulation with the phrase, "as soon as we put before us the goal of the generalization thereof," and indeed *generalization* seems to be the goal in terms of which the overall arc of algebraic number theory, which was always more conceptual than computational, is most easily understood. If there was one central goal in the whole development, it was probably to state and prove a simple, elegant, unified, and extremely general reciprocity law. We will return to these thoughts again when we consider Taussky's opening observations in her talk on number theoretic computation at a conference in 1953.

Meanwhile, while we are busy emphasizing this opposition, let us not neglect to also point out the irony that Hilbert's norm-residue symbol would eventually come to be best understood in the p-adic, local framework of Hensel and Hasse.

Or, yet again, we must observe that in the same talk before the DMV Hilbert himself made several analogies between number theory and function theory, of just the kind that drove Hensel's work: he compared his form of the reciprocity law with the Cauchy integral theorem; he stated that the distinction between numbers that were and were not norm residues in a sense corresponded to the distinction between functions that are expanded in whole powers of a variable or fractional powers; he compared a fact relating the property of dividing the relative discriminant to the property of being or not being a norm residue to a theorem on the ramification points of a Riemann surface.

These examples remind us that, outside of any dualities or oppositions within number theoretic practice that we may care to delineate, ultimately all these mathematicians were working on one and the same theory, and their methods and approaches often overlapped.

Hasse pointed out that this paper on the explicit reciprocity law was only one in a series of works that he had devoted to this problem; he named (Artin and Hasse 1925; Hasse 1924, 1925a,b,c) from the years 1924 and 1925 as prior work in this direction, and noted that one of these papers (Artin and Hasse 1925) from 1925, was coauthored with Artin. [34]

[34]The two show themselves to have been quite chummy during this time, as a footnote on the title page

Artin, it turns out, was quite an influence on Hasse in the latter's pursuit of explicit reciprocity laws. They collaborated again on a paper (Artin and Hasse 1928) in 1928, in which they deduced an explicit formula for the case of an exponent m which was a prime power $m = \ell^n$. As for the 1929 paper we are considering now, Hasse states that the methods he applies come entirely from a paper (Eisenstein 1850) of G. Eisenstein (1823-1852) – whose work he refers to as the very first work on explicit reciprocity laws in cyclotomic fields – even claiming that the results Hasse will prove in this work will come "entirely through extension and combination of the methods and ideas developed in this work of Eisenstein." [35] It was Artin however, Hasse notes, who brought not only this paper of Eisenstein to his attention, but also the particular formula, which Hasse refers to as the *"Eisensteinsche ausgangspunkt"* (the "Eisenstein starting point"). Finally, when in 1962 Hasse would publish a second paper (Hasse 1961) by the very same title, *Zum expliziten Reziprozitätsgesetz*, he would write that the supplement that he there added was something he found in his journal entry from 16 October 1928, with the notation: *"Einer Anregung Artins zufolge ausgearbeitet"*: "Worked out following a suggestion of Artin."

3.3.5 The Klassenkörperbericht

Class field theory was difficult to understand, even for experts, and certainly for outsiders, and so history repeated itself and it was decided at a meeting of the DMV that a report should be written to gather together, summarize, and systematize the theory. This time Hasse was nominated for the task, and the work would come to be called the *Klassenkörperbericht* (henceforth KKB), or sometimes "Hasse's *Zahlbericht*."

Hasse published the work in three parts, known as Parts I, Ia, and II. The basic idea was that Part I would treat the "class fields side" of the theory, while Part II would cover the "reciprocity laws side". On top of this, Part Ia simply contained detailed proofs which were only sketched in Part I. It was a fortuitous thing that the work was broken down in this way, since, after the appearance of Parts I and Ia in 1926 and 1927, Hasse did not publish Part II until 1930, and therefore had time to react to and incorporate Artin's reciprocity law.

---

states only that, whereas the results of the work had arisen in personal correspondence between the authors, "the younger of them undertook the writing out and exposition." (*"Ausarbeitung und Darstellung übernahm der jüngere von ihnen."*) This, then, was Hasse.

[35] *"Es ist nicht zu viel behauptet, wenn ich sage, daß die im Folgenden bewiesenen Ergebnisse lediglich durch Ausbau und Kombination der in jener Eisensteinschen Arbeit entwickelten Methoden und Gedanken zustande gekommen sind."*

In fact, Artin's law is truly the main theme of Part II, which Hasse opens with the following:

> Since the appearance of the first part of this report, the theory of relative-Abelian number fields has made a stride forward of the utmost significance, which directly concerns the side of the theory planned for this second part, the reciprocity law. Namely, Artin succeeded in giving the general proof for his group theoretic formulation of the reciprocity law, already conjectured in 1923 and proven in special cases. In the following, I name it after him, the Artin Reciprocity Law. (Hasse 1930) [36]

The work is divided into five sections, which Hasse outlines in the introduction as follows: In Section 1 he carefully formulates and proves the Artin reciprocity law, and shows how it leads to an essential completion of the theory of class fields already worked out by Hilbert, Furtwängler, and Takagi. In Section 2 he explains his own theory of norm residues of arbitrary relative-Abelian number fields, as a stepping stone to Section 3, in which he shows how the Artin reciprocity law first merits its name, through its applications to the reciprocity laws of power residues, in their classical formulation.

As for Section 4, Hasse promises work on explicit reciprocity laws, and even says that Henselian methods will be of importance here:

> A farther reaching question, not treated in the Hilbert-Furtwängler-Takagi-Artin theory of the reciprocity law, but rather picking up immediately on the classical works of Gauss, Eisenstein, and Kummer, is that regarding the explicit formula for the reciprocity law, familiar in the simplest case as the Gaussian general reciprocity law along with supplementary theorems for the Legendre symbol for quadratic residues. I have already dedicated a long series of works to the deduction of such explicit formulas for today's current reciprocity laws in algebraic number fields. If the results known up to now do not yet possess the same completeness as do those aforementioned, so shall the attempt first be made here in Section IV, to bring them together into a unified whole. In the further

[36] Seit dem Erscheinen des ersten Teils dieses Berichts hat die Theorie der relativ-Abelschen Zahlkörper einen Fortschritt von der allergrößten Bedeutung gemacht, der gerade die für diesen zweiten Teil in Aussicht genommene Seite der Theorie, das Reziprozitätsgesetz, betrefft. Es gelang nämlich Artin, den allgemeinen Beweis für seine schon 1923 vermutete und in speziellen Fällen bewiesene gruppentheoretische Formulierung des Reziprozitätsgesetzes zu geben, die ich im folgenden nach ihm das Artinsche Reziprozitätsgesetz nenne.

> development of this theory, in which the Henselian number-theoretic methods are of decisive importance, there lies a realm of work of, as it appears to me, extraordinary charm. [37]

All through the discussion Hasse praises in grand terms every part of class field theory that he mentions, but only here, concerning the theory of explicit reciprocity laws, does he make the praise sound anything less than universal, presenting it instead as a personally held opinion. This seems to fit with the account of things that we find in many popular summaries (e.g. (Lang 1970)) of the intertwined subjects of class field theory and reciprocity laws, which seem to make little or no mention of explicit reciprocity laws.

Even Hasse himself, writing at the sober remove of 37 years, had to admit in his *History of Class Field Theory* talk at the Brighton conference in 1967 [38] that the subject was too marginal for discussion at that venue. At the same time, he reminds us of his own special interest in the topic:

> There still remains much to be said about further developments arising from the class field theory delineated up to this point. For instance, what lies particularly close to my heart, the *explicit reciprocity formulae* (determination of the norm symbol $\left(\frac{a,b}{\mathfrak{p}}\right)_n$ for prime divisors $\mathfrak{p}|n$; ... and so on. I must, however, refrain from talking about those subjects here, because that would exceed the frame of this lecture. (Cassels and Fröhlich 1967, p. 276).

As for more popular work, Hasse had this to say at the close of his 1967 talk:

> If I have understood rightly, it was my task here to delineate for the mathematicians of the post-war generation a vivid and lively picture of the great and beautiful edifice of class field theory erected by the pre-war generations. For the

[37] Eine weitergehende, in der Hilbert-Furtwängler-Takagi-Artinschen Theorie des Reziprozitätsgesetzes nicht behandelte, wohl aber unmittelbar an die klassischen Arbeiten von Gauß, Eisenstein und Kummer anknüpfende Fragestellung ist die nach expliziten Formeln zum Reziprozitätsgesetz, wie sie im einfachsten Falle als Gaußsches allgemeines Reziprozitätsgesetz nebst Ergänzungssätzen für das Legendresche Symbol der quadratischen Reste bekannt sind. Der Herleitung solcher expliziten Formeln auch für die heute aktuellen Reziprozitätsgesetze in algebraischen Zahlkörpern habe ich bereits eine größere Reihe von Arbeiten gewidmet. Wenn auch die bisher vorliegenden Resultate noch nicht die gleiche Abgeschlossenheit haben wie die vorher besprochenen, so soll doch nachstehend in Abschnitt IV erstmalig der Versuch gemacht werden, sie zu einem einheitlichen Ganzen zusammenzustellen. In dem weiteren Ausbau dieser Theorie, in der die Henselschen zahlentheoretischen Methoden von entscheidender Bedeutung sind, liegt ein Arbeitsgebiet von, wie mir scheint, ganz eigenartigem Reiz.

[38] (Cassels and Fröhlich 1967)

> sharply profiled lines and individual features of this magnificent edifice seem to me to have lost somewhat of their original splendour and plasticity by the penetration of class field theory with cohomological concepts and methods, which set in so powerfully after the war. (Cassels and Fröhlich 1967, p. 276)

In Hasse's own view, then, although he was once the author of the official "*Bericht*" for class field theory, it was certainly a subject whose mainstream development he had left behind by the end of World War II. We should note that, according to Lang (Lang 1970) p. 176, Hochschild's cohomological work in 1950 showed certain class field theoretic work of Hasse from the 1930s to be unnecessary.

3.4 Political unrest

Hasse stayed in Germany during the Nazi period, unlike so many other mathematicians, who either were Jewish themselves or had Jewish relatives. Artin for one, whose wife was Jewish, emigrated to the United States in 1937.

Also among those who were forced out of their professorships, and for safety's sake left the country altogether, was Richard Courant, who had been director of the new Mathematics Institute at Göttingen. Hasse was called to replace Courant, and, after visiting Göttingen briefly, and returning home to Marburg in disgust at pro-Nazi student demonstrations he had witnessed there, eventually accepted the post. (Reid 1976, p. 162)

From 1934 to 1939 Hasse fulfilled his duties as director at Göttingen. It is clear that Hasse was thus at least "acceptable" to the Nazi party, and Edwards has stated in (Edwards 2008a) that Hasse "made no secret of his strongly nationalistic views and of his approval of many of Hitler's policies." On the other hand, Edwards also notes just as much in defence of Hasse's character, for example:

> ... his relations with his teacher Hensel, who was unambiguously Jewish by Nazi standards, were extremely close, right up to Hensel's death in 1941, and his relations with the Hensel family remained close and warm throughout his life. ... In his years as director of the Mathematics Institute in Göttingen ... he struggled against Nazi functionaries who tried (sometimes successfully) to subvert mathematics to political doctrine. Hasse never published in the journal *Deutsche Mathematik*. [39]

[39] (Edwards 2008a). The journal *Deutsche Mathematik* was founded in 1936 by L. Bieberbach (1886-1982)

In April 1940, Hasse was conscripted to the Berlin Navy Headquarters. (Rohrbach 1998, p. 9) As some measure of the time and involvement that this occupation must have demanded of Hasse, we may note that after graduating two PhD students in 1939 (from Göttingen), Hasse did not sign off on another dissertation until 1950, then at Humboldt University in Berlin. Between 1945 and 1950 this was the unavoidable result of Hasse's placement in the "denazification" program, wherein he was not allowed to teach classes or take students, but from 1939 to 1945 it suggests a possible monopolization of his time and efforts by the German Navy.

In honour of his 75th birthday, the double volume 262-263 of Crelle's journal in 1973 was dedicated to Hasse, and featured an article by Hans Rohrbach – then co-editor of Crelle's Journal with Hasse – on the subject of, "The Logogryph of Euler". In his introduction to this paper on a cryptographic challenge posed by Euler in a 1744 letter to Christian Goldbach, Rohrbach wrote,

> So I take the opportunity for publication where a special volume of Crelle's Journal is dedicated to my friend Helmut Hasse since I know that he, too, is interested in cryptanalysis. Some time ago both of us, for a couple of years, were officially busy with, to be sure, more difficult material of that kind. (Rohrbach 1973, p. 393)

He said nothing more about it. Several years later, however, in a talk about Hasse's role as editor of Crelle's journal, given at a symposium in commemoration of Hasse in Hamburg, 7 February 1981, and reprinted in the journal's 500^{th} volume, Rohrbach spoke more openly, confirming that in his conscription into the Navy Hasse "was to be in charge of a research group, which had to decipher intercepted radio signals with the help of mathematical methods." (Rohrbach 1998, p. 9)

Rohrbach had his PhD from Berlin in 1932, under Issai Schur, and starting as early as 1934 he was assisting Hasse with the editing of Crelle (ibid., p. 10) He then became co-editor with Hasse of the journal in 1952 (retiring from that role only in 1978) a circumstance that would not be inconsistent with their having worked together during the war, as Rohrbach's cryptic remark in (Rohrbach 1973) indicated. In (Rohrbach 1998) however, Rohrbach did not claim to have been involved in the Navy research group headed by Hasse.

---

and T. Vahlen (1869-1945), who had bought into racial theories circulating at the time, which suggested that there was a difference between "German mathematics" and "Jewish mathematics"; as a part of the general madness of the era, only the former was to be allowed in the journal. See (Mehrtens 1987).

3.5 Olga Taussky

The mathematical interests of Olga Taussky (30 August 1906 to 7 October 1995) appear to have been almost hand-crafted to make a researcher ready to contribute to computational algebraic number theory, and indeed she is an important figure in the history of this subject.

Taussky was born in Olmütz, in the Austro-Hungarian Empire, which is now Olomouc, in the Czech Republic. Her father was an industrial chemist, her two sisters went on to be chemists as well, and she too began her studies at the University of Vienna in that subject. (Luchins and McLoughlin 1996) Before long, however, her love of mathematics brought her into those studies where she remained all her life, making great contributions, and achieving a good deal of fame for a mathematician. While perhaps not one of the truly giant names known to all who study mathematics, she was certainly celebrated, not only within the mathematical community, but even publicly: she was, for example, named one of nine "Women of the Year" by the Los Angeles Times in 1963 (ibid.). Numerous memorial articles have been written about her by fellow mathematicians, for example (Bauer 1998; Davis 1997; Hlawka 1997; Kisilevsky 1997; Luchins and McLoughlin 1996; Schneider 1998), and she has written autobiographical accounts as well (Taussky 1977, 1985).

Not just in terms of quality, but also in terms of raw volume, the subject to which Taussky seems to have made the largest contributions is Matrix Theory. She is, for example, credited with having been instrumental in making this into a subject in its own right, rather than merely "a part of algebra which was now largely superseded by the theory of vector spaces" (Schneider 1998).

For example, Davis writes (Davis 1997):

> The field she is most identified with – which might be called "linear algebra and applications" though "real and complex matrix theory" would be preferred by some – did not have autonomous existence in the 1930s, despite the textbook by C.C. MacDuffee. Her stature in that field is the very highest, as was palpable in the standing ovation after her survey talk at the second Raleigh conference in 1982.

Still, Taussky herself stated that number theory began as and always remained her favourite among mathematical subjects. Davis wrote:

> Her first research ... was on algebraic number theory, and she never stopped

> regarding that as her primary field. (Davis 1997)

And in Taussky's own words,

> At the age of about 15 (a pupil of the only Mittelschule for girls in Linz, Upper Austria) I came to realize that science and mathematics were to be my subjects. Slowly this changed to "mainly mathematics," with science still of great interest to this day, and in due course mathematics meant mainly number theory. (Taussky 1977)

Elsewhere she indicates that while the circumstances of life drew her away from the subject for many years, she was always anxious to get back to number theory:

> [For a large part] of my life all I wanted to work in was number theory. But this was frustrated through many circumstances. In fact, it took a long time before I could return to my dream subject. [40]

Her contributions to the area were quite bountiful as well: besides her work in the computational branch which we will be interested in primarily, we note also that one memorial article (Kisilevsky 1997) of six pages was devoted entirely to a review of Taussky's work in class field theory.

In addition to her own work, she played a role in the publication of other important number theoretic works: she was co-editor of the first volume of Hilbert's collected papers, which gathered together all his number theoretic work; she also took the notes on Artin's 1932 class field theory lectures in Göttingen, which were finally published in English in (Cohn 1978), after being circulated by hand for many years (Hlawka 1997; Luchins and McLoughlin 1996).

The story of the path that Taussky followed in life, which led her first to number theory, and then away from it to discover her interests in matrix theory and a couple of other mathematical subjects as well, takes us up to the time of World War II. It was however during the War, and also continuing on afterwards, that Taussky would get involved with electronic computers, and we delay this part of the story until Chapter 5.

Taussky was at the University of Vienna during the time that the last steps in the classical phase of class field theory were being taken, i.e. the last steps up to the principal

[40] From (Taussky 1985), quoted in (Luchins and McLoughlin 1996).

ideal theorem. Artin realized that the principal ideal theorem could be reduced to a purely group theoretic problem, and communicated this idea to Furtwängler, who himself had been working on group theoretic formulations of number theoretic problems at the time (Kisilevsky 1997). Furtwängler succeeded in completing the group theoretic step, and thus proved the principal ideal theorem. His work was published in 1930, in (Furtwängler 1930).

Taussky's doctoral thesis was completed in the year 1930 as well, and was published in *Crelle* in 1932 (Taussky 1932). The title of her thesis, *"Über eine Verschärfung des Hauptidealsatzes"* ("On a Refinement of the Principal Ideal Theorem") reflects the fact that Furtwängler asked her to investigate the finer structure of the principal ideal theorem in the following way, as characterized in (Luchins and McLoughlin 1996): whereas (1) class field theory states that the Galois group of the Hilbert class field H of a number field F is isomorphic to the class group G of F, while (2) Galois theory states that the subfields of H over F correspond to the subgroups of G, and (3) the principal ideal theorem says that *all* ideals of F become principal in H, it is thus a natural question to ask whether the intermediate fields *between* F and H could be characterized by those ideals of F which are *not yet principal* there. This, in essence, was the large question that Taussky was asked to investigate, by considering certain particular, smaller questions.

Namely, Taussky's problem arose in the following way, as explained by Kisilevsky: [41]

> Since an ideal class $c \in C(F)$ of order n would still have order n in any extension of degree prime to n, it was natural that one restricted attention to the p-primary subgroups $C_p = C_p(F)$ of the ideal class group $C(F)$ and to extensions of p-power degree. (Kisilevsky 1997)

Furtwängler had already achieved some results on the case of $p = 2$, and asked Taussky to consider the case of odd primes $p \geq 3$. The results were erratic, as Taussky later would write:

> I did indeed solve [the problem] for 3. While trying to generalize it for prime numbers larger than 3, ... I found that every prime number p behaves differently. (Luchins and McLoughlin 1996)

and again

[41] Kisilevsky was a student at MIT (PhD 1968) of Ankeny, who in turn was a student at Princeton (PhD 1951) of Artin. Ankeny's name will come up again in work with Artin that appears in Zimmer's 1972 survey (Zimmer 1972) of the emerging field of computational algebraic number theory.

> ... the theorems seemed to be of a chaotic nature. The results of my thesis problem made Furtwängler give up class field theory forever after." (Taussky 1977)

Artin even asked her once whether she was still working "on these hopeless questions" (Kisilevsky 1997).

She persevered however, and this research led Taussky immediately into a further work, published in 1934, and done together with Arnold Scholz, [42] which is very interesting to us for its significance in computational algebraic number theory. Apart from our particular interest in it, this work has also been noted by others as well: Hlawka (Hlawka 1997) refers to it as a "very significant paper," and Kisilevsky notes (Kisilevsky 1997) that it provided the first non-trivial examples of finite 3-class towers. Scholz would appear to be a little-known figure, whose work, during his short life, was geared entirely toward computational algebraic number theory.

In the paper of 1934, Scholz and Taussky carried on with the questions Taussky had considered for her doctoral thesis, this time under the assumption that the base field F is imaginary-quadratic, and with $p = 3$ and the group $C_3(F)$ being of the form $(\mathbb{Z}/3^m\mathbb{Z}) \times (\mathbb{Z}/3^n\mathbb{Z})$. Namely, they consider the fields $\mathbb{Q}(\sqrt{-4027})$ and $\mathbb{Q}(\sqrt{-3299})$ which have 3-class groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ resp. (ibid.). A letter from Taussky in Hasse's *Nachlass*, written 29 July 1933, shows that Taussky and Scholz were both in communication with Hasse around this time, and were sending him copies of their work.

The work is entitled "The Principal Ideals of cubic Class Fields of imaginary-quadratic Number Fields," with the subtitle, "their computational Determination and their Influence on the Class Field Tower" (*Die Hauptideale der kubische Klassenkörper imaginär-quadratisch Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperturm*). Indeed, the work features about 7 pages (out of 23 total) filled with computations of examples of such things as minimal polynomials, discriminants, and algebraic representations of the cubes of certain ideals. These pages are filled with numbers, a rare sight in a very theoretical subject ordinarily populated mostly by variables!

A comment in the introduction foreshadows the emphasis Taussky will place on the need

[42] Arnold Scholz (24 December 1904 to 1 February 1942) studied under Issai Schur at the University of Berlin, PhD 1928, dissertation, *"Über die Bildung algebraischen Zahlkörper mit auflösbar Galoisscher Gruppe"* ("On the Construction of algebraic Number Fields with solvable Galois Group"). After his early death at the age of 37, his memorial article (Taussky 1952) was written by Taussky.

for rational methods in a 1953 talk on computational number theory, which we will consider in Chapter 5. Moreover, it is interesting that work of Hasse from 1929 was useful in the computations done in this paper, at least in that this foreshadows later influence of Hasse's work on Taussky's computational research in the 1950s. Namely, Taussky and Scholz write (their emphasis):

> These studies do not require the Artin Reciprocity Law. *It will be decided by means of relations in the field of rational numbers,* which classes become principal in the unramified relative-cubic extension field. For this section the theorems of Hasse on cubic fields (Math. Zeitschrift 31) were essential. [43]

Later, when she wrote his obituary (Taussky 1952), Taussky would seem to attribute the method of computation solely to Scholz:

> Scholz found a method to decide by means of rational numbers alone, whether a class of the ground field would go over into the principal class in an unramified relative-cubic extension field. [44]

The paper of Hasse referred to is entitled *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage* ("Arithmetic Theory of cubic Number Fields on class-field-theoretic Foundations"), and is yet another example of Hasse's interest in tables and computational work. It features a beautiful table organizing facts about such things as prime decompositions, and contributions of primes to discriminants, conductors, and norms of conductors for fields B, Q, and K, where K is a cubic field over $\mathbb{Q}$, B is a Galois extension that is quadratic over K, and Q is that quadratic subfield of B over which B is cyclic-cubic.

In Taussky's obituary for Scholz, she wrote of him that,

> He hoped that, with time, more tables concerned with algebraic number fields would be published. Since then, this was carried out partially by Hasse in the case of cubic number fields. [45]

---

[43] Diese Untersuchungen benützen das Artinsche Reziprozitätsgesetz nicht. *Es wird mit Hilfe von Relationen im Körper der rationalen Zahlen entschieden,* welche Klassen in den relativ unverzweigten kubischen Oberkörpern zur Hauptklasse werden. Für diesen Abschnitt waren die Sätze von Hasse über kubische Körper (Math. Zeitschrift 31) sehr wichtig.

[44] Scholz fand eine Methode, mit Hilfe rationaler Zahlen allein zu entscheiden, ob eine Klasse des Grundkörpers in einem unverzweigten relativ-kubischen Erweiterungskörper in die Hauptklasse übergeht.

[45] Er hoffte, daß mit der Zeit mehr Tabellen, die sich mit algebraischen Zahlkörpern befassen, veröffentlicht würden. Dies wurde seither teilweise von Hasse im Falle kubischer Zahlkörper durchgeführt.

Taussky's reference would seem to be to the paper of Hasse mentioned above.

This work with Scholz demonstrates Taussky's computational number theoretic interests very early in her career, just four years after her doctorate. She will revisit this very same subject again, i.e. her PhD thesis topic and these extensions of it, in a paper presented at an important conference in the history of computational number theory, held near Oxford in 1969. We will return to this in Chapter 7.

Taussky's movements after her doctorate, as recounted in (Hlawka 1997), were as follows: 1931-2, assistant to Courant in Göttingen, where her primary duty was the editing of the collected volume of Hilbert's number theory works; 1932-4 assistant to Hans Hahn and Karl Menger in Vienna; 1934-5 at Bryn Mawr College in Pennsylvania with Emmy Noether; 1935-7 research fellow at Girton College in Cambridge, England; 1937 onward, teaching at Westfield College of the University of London. Here she met John (Jack) Todd, who taught mathematics at another college, and they were married in 1938.

She was on leave of absence from the University of London 1943-6, taking a position in the National Physical Laboratory in Teddington, near London, for work related to the war effort. She served the Ministry of Aircraft Production in the analysis of aircraft designs for their stability properties (Davis 1997), and in particular was assigned to the "Flutter Group" under Robert A. Frazer, working on a boundary value problem for a hyperbolic differential equation arising from flutter at supersonic speed (Luchins and McLoughlin 1996). Taussky wrote that it was here that she became involved in matrix theory:

> It is a curious coincidence that in both Wielandt's case and my own, our interest in matrix theory was generated by our involvement in aerodynamics in WWII. [46]

After the War, Taussky and Todd would sail to the U.S. and would live there for the rest of their lives. We pick up with that story in Chapter 5.

In particular, when we consider Taussky's collaboration with Zassenhaus and Dade in 1959, we will see these researchers computing algebraic number theoretic objects which are represented by matrices; thus, we will see a combination of all those areas of Taussky's expertise which made her so well suited for work in the field of computational algebraic number theory: the research concerned objects associated with algebraic number fields; the

[46] Quoted in (Schneider 1998).

objects being operated upon were integer matrices; the operations were being performed on electronic computers.

3.6 Hans Zassenhaus

Hans Julius Zassenhaus (28 May 1912 to 21 November 1991) coauthored with Michael Pohst the book *Algorithmic Algebraic Number Theory* (Pohst and Zassenhaus 1989), published in 1989, which was a landmark in computational algebraic number theory. We will return to discussion of this book in Chapter 7. Pohst collaborated with Zassenhaus for many years on that book's subject. After the latter's passing in 1991, he wrote a memorial article (Pohst 1994), from which we draw the facts of his life story.

Born in Koblenz-Moselweiß, Germany, Zassenhaus moved with his family to a suburb of Hamburg in 1916. He graduated in 1930 from the Lichtwark High School, and entered the University of Hamburg. There he took classes from Artin and Hecke, among others. He obtained his PhD in 1934 under Artin, for the dissertation, *"Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen"* ("Characterization of finite linear Groups as Permutation Groups"). From 1934 to 1936 he worked as *wissenschaftlicher Hilfsarbeiter* (scientific assistant) in Department of Mathematics at the University of Rostock.

It was during his time at Rostock that Zassenhaus completed the first draft of his book on group theory, (Zassenhaus 1949a). Pohst describes the book as "epoch-making," and says that it "became the leading textbook on that subject for a generation," noting also that the book was "inspired by a course of E. Artin." Zassenhaus himself wrote in a memorial article on Artin (Zassenhaus 1964) that,

> [Artin] influenced decisively the basic organization of the books of van der Waerden on Algebra, Zassenhaus on group theory and Tim O'Meara on quadratic forms, moreover Artin's spirit of abstraction had an admittedly strong influence on the Bourbakists.

It is well known that Emmy Noether shared with Artin the role of inspiring van der Waerden's famous Algebra book, which Corry (Corry 1996) and others have pointed to as emblematic of the rise of the structural view of algebra. Thus, Zassenhaus was instrumental in that generation of mathematicians who were learning the new, abstract algebra from the lectures of Artin, Noether, and others, and were codifying these lectures in new textbooks.

In 1936 Zassenhaus was appointed assistant to Artin at the University of Hamburg. He obtained his *Habilitation* there in 1938 with a work on the theory of Lie rings. He became *Diätendozent* (a *per diem* lecturer) there in 1940, and also volunteered for the navy that year, as an alternative to joining the Nazi party. In this capacity, he worked during the war in a meteorological research group. After the war, he became *außerordentlicher Professor* (assistant professor) at the University of Hamburg (Pohst 1994).

It is hard to find much in Zassenhaus's work before or during the war that should have made him especially predisposed for work on computational algebraic number theory. Certainly he had a strong background in algebra, group theory in particular, which via Galois theory forms one side of the study of number fields. Although he worked closely with Artin, he entered University only in 1930, the same year that the principal ideal theorem was proved, and the initial phase of class field theory was finished. Pohst states that Zassenhaus's first purely number theoretical paper was (Zassenhaus 1949b), published in 1949, and this was on the subject of primes in arithmetic progressions. [47] In fact, Pohst also attests that,

> [Zassenhaus's] tendency to computational algebraic number theory came out for the first time at Caltech during his visit 1959.

This was a collaboration with Taussky and C. Dade, which we will return to in Chapter 6.

Instead, in Zassenhaus we find a mathematician who had very widespread interests, and who seems to have been always ready to embark on research in a new area of mathematics. Although he was already 47 when he first became involved with computer research in 1959, this became a major aspect of his work. As Pohst writes,

> This appreciation of his life would be incomplete without mentioning his efforts to join mathematicians and computer scientists. Being one of the pioneers in symbolic and algebraic computation, he gave a highly integrating stimulus by pointing out the importance of contributions from both parties for the development of methods in computer algebra. In 1987 these efforts were honoured by a special volume of the *Journal of Symbolic Computation*.

Altogether, among areas to which Zassenhaus made important contributions Pohst lists: group theory, nearfields, the theory of orders, representation theory, (computational) algebraic number theory, the geometry of numbers, Lie algebras in mathematical physics,

[47] It was not, however, analytic, but elementary, the purpose of the paper being to prove Dirichlet's theorem by elementary means.

didactics, and the history of mathematics. We would note the area of polynomial factorization as well.

Chapter 4

Setting the stage in the 1940s

It was in the 1940s, largely due to the war, that the development of electronic computers began. Work was done principally in the United States, the U.K., and Germany, and the history has been well studied. [1] Electronic machines like Eckert and Mauchly's UNIVAC, and von Neumann's machine at the Institute for Advanced Studies in Princeton started to be designed and built toward the end of the 1940s, and became operational and began running jobs in the early 1950s. During the war, more primitive electro-mechanical machines (using relays instead of vacuum tubes) had been built.

Histories of computing technology which aim to be comprehensive, e.g. (Williams 1985), always start out by discussing computing devices entirely different from what we think of as computers today: things like *planimeters* from the late nineteenth and early twentieth centuries, which are analogue devices for estimating integrals by tracing graphs with pointers connected to wheels and such; or even earlier, things like a calculating machine constructed in 1623 by Schickard in Tübingen (Zuse 1980); or more rudimentary devices like *Napier's bones*, on which Napier published in his 1617 *Rabdologiæ*.

Even in the history of computing in number theory there is a specialized device from the 1930s. [2] The *photo-electric number sieve* was built by D.H. Lehmer with funding from the Carnegie Institute of Washington, and he published an article on the machine and its use in 1933. [3] The sieve used rotating gears, perhaps giving it an analog character on first

[1] See (Williams 1985) and (Metropolis, Howlett, and Rota 1980), among others.

[2] See also (Shallit, Williams, and Morain 1995).

[3] (Lehmer 1933a)

appearance, but in truth it was of a more digital nature. [4] Digital or not, the machine was wholly different from the stored-program electronic computer that started to appear in the late 1940s and early 1950s. Lehmer used the machine to compute class numbers, and Taussky cited his work in her 1953 survey on computational algebraic number theory [5] which we will discuss in Section 5.3, and we therefore will devote a little space to the machine here, in Section 4.1.

Afterward, we give Section 4.2 to D.H. Lehmer's 1941 *Guide to Tables in the Theory of Numbers* (Lehmer 1941). We may again frame our discussion as guided by Taussky's survey, in which she said that, "A list of table work concerning algebraic number fields – there is not much of it – can be found in Lehmer." [6] Lehmer's guide to tables does seem to stand as a fairly comprehensive review of what table work had been done in number theory (in general, as well as in the algebraic branch in particular) up to the time that electronic computers started to become available. Therefore, in our effort to give a somewhat comprehensive view of the work in our field, we may hope that Lehmer's tables will give us a strong basis on which to build. Since we cannot devote more space to it, we hope also that in the course of these first two sections some image of the importance of D.H. Lehmer, as well as that of his wife Emma Lehmer, in computational number theory will become apparent.

Next, Section 4.3 examines Weyl's 1940 textbook on algebraic number theory, and its importance as a representative of the Kummer-Kronecker-Hensel tradition in this subject. Finally, as promised in Chapter 1, we examine in Section 4.4 Hasse's view of the methodological divides that we have set out to understand, as voiced in statements penned in 1945 and 1949.

We may view all of the material to be covered in this chapter as in a way setting the stage for the birth of computational algebraic number theory as a robust field of research. The sections on the number sieve and the *Guide to Tables* give background for the technological aspect of this program, while the sections on Weyl and Hasse show how certain prominent figures made an attempt to give voice to a side of algebraic number theory which they felt had been unduly neglected, and to call for the widespread adoption of the methods

[4] Merriam-Webster defines an analog mechanism as one in which data are represented by continuously variable physical quantities. Lehmer's sieve kept track of only discrete quantities, namely, (1) the number of hole positions through which each gear had been turned, modulo the number of holes on that gear, and (2) the number of gear teeth turned through by the drive gears.

[5] (Taussky 1953)

[6] (ibid.)

belonging to this side.

4.1 A photo-electric number sieve

The name of Derrick Henry Lehmer (1905 - 1991) – more often known as Dick Lehmer – is well known in mathematics; many, in fact, may remember him as one half of the mathematical duo of D.H. and Emma Lehmer (1906 - 2007). Less well known is his father, Derrick Norman Lehmer (1867 - 1938), who was also a mathematician, and taught at Berkeley starting in 1900. (O'Connor and Robertson 2004)

While Dick was an undergraduate physics student at Berkeley (he later obtained his graduate degrees in mathematics from Brown University), he assisted his father with his project on *factor stencils*, which were a kind of card with punched holes in them that could be laid on top of one another in order to factor large numbers. Derrick Norman Lehmer had long been interested in the problem of factoring, and in the idea of sieves, and shortly after the project on factor stencils he described his vision for an electro-mechanical sieve. As announced in the New York *Herald Tribune* of 12 July 1931, he received a grant of $1,000 from the Carnegie Institution of Washington D.C. for the construction of the machine under his direction, and to be carried out by his son in the capacity of national research fellow. [7]

The machine, described in (Lehmer 1933a), had an array of thirty gears, $G_1, G_2, \ldots, G_{30}$, representing moduli $m_1, m_2, \ldots, m_{30}$ which were primes and powers of primes less than 127. Gear G_i had m_i teeth, and had a hole opposite each tooth, which could be plugged or left open. If an arithmetic problem was solved with respect to each modulus m_i, in general having multiple solutions, then the holes corresponding to the solution residues were left open, while all others were plugged. A light beam then could pass through all the gears only when they were rotated to a position representing a single number which was a solution with respect to all moduli. The light beam would then strike a photoelectric plate, causing the gears to stop rotating. Dick Lehmer emphasized that it was only in then recent times that the sensitive electronics necessary to detect the light beam and shut off the machine had become available.

While the initial motivations for the machine may perhaps have been of an elementary

[7] (unknown 1931), cited in (O'Connor and Robertson 2004).

number theoretic nature, having to do with the factoring of large numbers, and the computing of Fermat primes, the application through which Dick Lehmer exemplified the use of the machine in his 1933 paper, still he wasted no time in applying the machine to a problem in algebraic number theory.

Gauss had noted (in different language, since he did not speak of number fields) that among imaginary quadratic number fields $\mathbb{Q}(\sqrt{-D})$, those with D equal to $1, 2, 3, 7, 11, 19, 43, 67, 163$ had class number equal to 1, and he conjectured that h was equal to 1 for only finitely many D altogether, having checked all cases $D < 3000$. (Lehmer 1933b) Heilbronn proved this to be the case in 1934 (Heilbronn 1934), and together with Linfoot (Heilbronn and Linfoot 1934) demonstrated that in fact there could be at most one $D > 163$ for which h was 1. Gauss's list therefore either was complete already, or lacked just one number, which had to be at least 3000. Finally in 1967 it was proved independently by Alan Baker on the one hand, and by Harold Stark on the other, that in fact Gauss's list was already complete.

In 1933, however, before any of these results had been proved, it was still a time in which it made sense to gather evidence for Gauss's conjecture, by exploring large ranges of values for D, and showing that for none of them was h equal to 1. Lehmer noted that prior to his own work, Dickson had been able to prove that $h > 1$ for $163 < D < 1,500,000$. Using a different method, and applying his photo-electric number sieve, Lehmer was able to extend the range to $163 < D < 5,000,000,000$, the machine processing $100,000$ values of D per second (for just under 14 hours of processing time). (Lehmer 1933b)

This extension of the interval provided data, and must have bolstered the conviction of many that indeed Gauss's conjecture was probably true, but did it yield new insight? Did it illuminate the nature of an algebraic number theoretic object – the class number, in this case – making its outline more sharply delineated, and its functioning easier to grasp? While Lehmer's work was an exciting and innovative use of technology to gain new data and evidence, it seems not to have been of the specific type whose history we intend to explore here, namely, the sort of computational work that Hasse called for in the foreword to KAZ. It did not help the algebraic number theorist to "move more freely" in number fields, in Hasse's words.

We may ask whether the kind of work that Hasse envisioned could even have been possible before the advent of the stored-program electronic computer. Was the machine exploration of algebraic structures (number theoretic or otherwise) possible prior to the invention of machines that permitted operations on arbitrary data structures? The simple geometric

shapes of the parts out of which special-purpose computing devices like planimeters or the Lehmers' photo-electric sieve were apt to have been made seem to lend themselves naturally to geometric problems, and even to periodicity and to discrete systems (as with the gears with holes in them), but it is hard to imagine a machine in which the special shape of the parts would of itself yield answers about things like algebraic numbers or integral bases, which researchers would eventually represent by data structures populated with integers, or rational numbers, as we will see in Section 6.1, in the work of Zassenhaus, Dade, and Taussky in 1959.

4.2 D.H. Lehmer's Guide to Tables, 1941

In order to understand the context in which the early number theoretic work on electronic computers was done, we need to start with a knowledge of what was in existence before that time. Apart from electro-mechanical computers like the one considered in the previous section, even when it comes to earlier and more primitive computation with pencil and paper, we turn again to D.H. Lehmer, who compiled a comprehensive guide, published in 1941, to all the extensive tables of computed number theoretic data that had been published up until that time. (Lehmer 1941)

The 105th issue of the *Bulletin of the National Research Council*, from February 1941, was entitled, "Guide to Tables in the Theory of Numbers." It was managed by the Committee on Mathematical Tables and Aids to Computation in the NRC's Division of Physical Sciences, chaired by Raymond Clare Archibald. [8]

Archibald was then professor at Brown University. Later he would become managing editor of the journal, *Mathematical Tables and other Aids to Computation*, which had its first issue in January 1943, and which would become the journal *Mathematics of Computation* in January 1960. The journal would be an important venue for early computational work. In 1941, Lehmer was at the Department of Mathematics at U.C. Berkeley. Later, he was co-editor with Archibald of *Mathematical Tables*.

The Committee on Mathematical Tables and Aids to Computation was divided into subcommittees concerned with different topics, the theory of numbers being just one, namely, "Subcommittee F", in an alphabetic designation system. Other topics included logarithms,

[8] See (Grier 2001).

hyperbolic and exponential functions, numerical solution of equations, summation of series, statistics, integrals, astronomy, geodesy, navigation, to name a few. Lehmer's report, however, was in fact the first to be published by the Committee. (Lehmer 1941, p. vii)

Among other things, the Report contained a painstaking compilation of errata on existing tables, in which Lehmer not only gathered together existing errata, but also extended these considerably by his own observation. The bibliography was also extraordinarily thorough, each entry being supplemented with a list of libraries (mostly at universities) where the sources in question could be found. Altogether, the report was divided into three parts: I Descriptive Survey, 80 pages; II Bibliography, 42 pages; and III Errata, 37 pages.

Of the purpose of such tables in number theory, Lehmer wrote,

> The theory of numbers is a peculiar subject, being at once a purely deductive and a largely experimental science. Nearly every classical theorem of importance (proved or unproved) has been discovered by experiment, and it is safe to say that man will never cease to experiment with numbers. The results of a great many experiments have been recorded in the form of tables, a large number of which have been published. The theory suggested by these experiments, when once established, has often made desirable the production of further tables of a more fundamental sort, either to facilitate the application of the theory or to make possible further experiments. (ibid., p. 1)

Lehmer generalizes broadly, suggesting that the process of discovery followed by nearly every mathematician begins with experiment, before moving to conjecture and proof. We may wonder, however, whether the experimental phase was diminished with those mathematicians who were known for a more conceptual style of mathematics. For example, at least when seeking a proof, Hilbert claimed that he simply quieted his mind, and tried to see the main "idea" of the proof. (See (Reid 1970).) However, discovering proofs and discovering theorems are very different things, and even Hilbert was guided by data on quadratic extensions when he stated his general class field conjectures. The degree of experimentation may vary from one mathematician to the next, but probably Lehmer is basically right.

Regarding comprehensiveness of the *Guide*, Lehmer claimed that,

> The writer has tried to include practically all tables appearing since 1918, and on the whole has probably erred on the side of inclusion rather than exclusion. (Lehmer 1941, p. 2)

As for tables prior to 1918, Lehmer included a great number of them, and, noting that most of those which he did not include were mentioned already in Dickson's three-volume *History of the Theory of Numbers*, he provided an exact list of the seventy-four such references in Dickson, sorted by subject matter, using the same list of subjects as was employed throughout his own report.

That list of subjects spanned all of number theory, sorted under headings labelled **a** through **q**, many of those headings having several subsections. Algebraic number theory was under heading **p**, and was a short section of just two and a half pages, although, as Lehmer indicated there, many of the other sections contained useful data for algebraic number theory, namely,

- **b2** Sum and number of divisors, and allied functions
- **b4** The quotients of Fermat and Wilson
- **d** The binomial congruence
- **e2** Tables of factors of numbers of special form
- **f2** Primes of special form
- **i2** Quadratic residues and characters and their distribution
- **j** Diophantine equations of the second degree
- **l** Diophantine equations of degree > 2
- **m** Diophantine continued fractions
- **o** Tables related to cyclotomy [9]

Still, useful though these other sections may have been for the researcher in algebraic number theory, they did not represent computation *in* algebraic number theory, which was confined to the references made in section **p**, some of which was redundant with section **o**, tables related to cyclotomy. It is interesting to note that headings **o** and **p** were the only ones missing from Lehmer's tabulation of references in Dickson. All of this attests to

[9] Namely, tables containing data such as: coefficients of the cyclotomic polynomials; multiplication tables for "periods" (as in Kummer); minimal polynomials for periods; representations of cyclotomic polynomials as quadratic forms in other polynomials.

the statement made by Taussky in her 1953 survey of computational problems in algebraic number theory (Taussky 1953): "A list of table work concerning algebraic number theory – *there is not much of it* – can be found in Lehmer" (my emphasis).

What there was, however, was not quite fairly represented by this *Guide*. In fact Lehmer was in charge not just of Subcommittee F on the Theory of Numbers, but also of Subcommittee G on Higher Algebra, and in Section **p** he promised that other tables important for algebraic number theory, though more algebraic than number theoretic, would appear in a future report on the latter subject. [10] These were to include tables of, "irreducible polynomials (mod p), modular systems, Galois field tables, class invariants, singular moduli, etc."

As for section **p** of the 1941 *Guide*, Lehmer began by observing that,

> Algebraic number theory, like the theory of forms, is a rather technical subject. The more extended parts of the theory are so ramified that tables are apt to be little more than mere illustrations of theorems. In fact, many articles on the subject contain numerical illustrations too numerous, too special and too diverse to permit description here. Although these numerical illustrations serve to make more real the abstract subject matter being considered, they cannot fairly claim to be described as useful tables. (Lehmer 1941, p. 75)

His thoughts recall Hasse's remarks from KAZ, written some four years after the publication of this *Guide*, regarding the presence of many scattered numerical examples of number field objects, disappointing for their lack of systematicity.

Lehmer noted furthermore (ibid., p. 75) that, if tables were organized according to the degree of the numbers considered, then many would pertain to quadratic number fields. Again, this claim would be echoed by Hasse's statement in the foreword to KAZ, that it was really only in the quadratic fields that one had the kind of cognitive "control" of the theory that comes from access to numerous examples.

Lehmer went on in section **p** to describe work that fell into five categories (which overlapped in some cases), according to the kind of number field in which computation was taking place. These were the main headings in the listing below. Without repeating Lehmer's description verbatim, I have attempted to summarize the kinds of objects being computed in

[10] A supposedly complete bibliography of Lehmer's work (Brillhart 1992) suggests however that Lehmer never wrote this report.

each work cited. Numbers in the listing below refer to Lehmer's bibliography.

- Quadratic fields
  - Sommer 1: basis, discriminant, the ideal classes, genera, characters, fundamental unit
  - Ince 1: cycles of equivalent ideals, the number of genera, the number of classes in each genus, generic characters, the fundamental unit
  - Schaffstein 1: class number
- The Gaussian field $\mathbb{Q}(i)$
  - Gauss 2: for certain primes p, gives those complex numbers mod p which have each of the 4 different biquadratic characters mod p
  - Gauss 9: indices for certain complex primes $p = a + ib$
  - G.T. Bennett 1: extended the tables in Gauss 9
  - Bellavitis 1: tables of powers of a primitive root for p
  - Voronoi 1: for certain primes p, a table of powers of a primitive root mod p, and a table giving the indices of certain special powers of these primitive roots
  - Glaisher 17: tables of certain sums of powers of "primary" Gaussian numbers
- Cubic fields
  - Reid 1, 2: for certain cubic fields, gives discriminant, class number, a basis, a system of units, and factorization of certain small rational primes in the field
  - Daus 2, 3: the units in certain cubic fields
  - Delone 1, 2: units of certain cubic fields of negative discriminant
  - Zapolskaia 1: tables for *relative* cubic fields
- Quartic fields
  - Delone, Sominskii and Bilevich 1: a list of totally real quartic fields, together with bases

  - Tanner 1, 2: tables of factors of primes of certain form, in the quartic field defined by a primitive 5th root of unity
  - Bickmore and Western 1: similarly, now for the quartic field defined by a primitive 8th root of unity

- Cyclotomic fields

  - Reuschle 2, 3: tables giving the complex factors of certain rational primes p in the cyclotomic field of nth roots of unity, for certain n, and in the subfields generated by the periods

For convenience, I list here the years of these citations, sorted chronologically:

1832	Gauss 2	1902	Zapolskaia 1
1859-60	Reuschle 2	1907	Sommer 1
1875	Reuschle 3	1911	Bickmore and Western 1
1877	Bellavitis 1	1926-27	Delone 1
1885	Glaisher 17	1928	Delone 2
1887	Tanner 1	1928	Schaffstein 1
1893	Tanner 2	1929	Daus 2
1893	G.T. Bennett 1	1934	Ince 1
1894	Voronoi 1	1935	Delone, Sominskii and Bilevich 1
1899	Reid 1	1936	Daus 3
1901	Reid 2		

As for Gauss 9, the actual date of the work is unclear. It seems to have first appeared in an 1876 collection of Gauss's work. Note that the tables of Reuschle and of Sommer are also mentioned by Hasse in KAZ as illustrations, when he calls for further tables of algebraic number theoretic data.

4.3 Weyl 1940

Weyl's *Algebraic Theory of Numbers* of 1940 is an important book in the history of our subject, in that it served as an access point to the theories of Kronecker and Hensel.

Hermann Weyl, who earned his PhD at Göttingen in 1908 under Hilbert's advisement, was eventually to be regarded by Hilbert as having gone somewhat astray, when he became an enthusiastic supporter of Brouwer's philosophy of mathematics. This makes Weyl a challenging and seemingly contradictory character to understand, in that on the one hand he believed in Brouwer's extreme constructivism, while on the other hand the letter from Hasse which we saw on page 86 paints Weyl as a supporter of Hilbert's conceptual approach, which "freed" us from the necessity of explicit computations.

Brouwer's rejection of the Law of the Excluded Middle meant the loss of mainstays of mathematics such as proof by contradiction, and the well-ordering principle of the natural numbers. The "foundations crisis" set off by the set theoretic antinomies, such as the "set of all sets that do not contain themselves" had prompted widespread reexamination of the basic laws of logic involved in mathematical proof, and Brouwer's reaction was radical. At a meeting in Hamburg in 1922, Hilbert expressed his opposition to this point of view:

> "What Weyl and Brouwer do comes to the same thing as to follow in the footsteps of Kronecker! They seek to save mathematics by throwing overboard all that which is troublesome .... They would chop up and mangle the science. If we would follow such a reform as the one they suggest, we would run the risk of losing a great part of our most valuable treasures!" [11]

As for the allusion to Kronecker, there can be no doubts as to Hilbert's attitude toward him and his philosophy. He felt that Kronecker's views were untenable to say the least, and we find this opinion expressed in Hilbert's unpublished lectures, *Probleme der mathematischen Logik*, held in Göttingen, in the Summer Semester, 1920. The translation by Ewald picks up just after Hilbert has presented the basic paradoxes of set theory:

> From the last paradox in particular we can now see that arbitrary definitions and inferences, made in the manner that was hitherto usual, are not allowed. And this leads to the expedient of prohibitions, of dictatorship.
>
> The first, most far-reaching, and most radical dictator in this area was Kronecker.
>
> ....
>
> On the basis of his way of looking at things, Kronecker forbids already the simplest irrational number $\sqrt{2}$; he introduces the concept of the modulus $x^2 - 2$

[11] Hilbert, quoted in (Reid 1970, p. 155).

> in place of this 'inadmissible' concept. ...
>
> His efforts to save at least those things that he needs in algebra become ever more cramped, and his theory of modules ever abstruser.
>
> Kronecker fights against every concept to the extent that it makes statements possible whose correctness is not decidable in a finite number of operations. For example he allows the concept of the irreducibility of an entire rational function (with integral coefficients) only under the condition that a finite process is given for deciding the irreducibility. ....
>
> ... To proceed in this way is to throw the baby out with the bathwater. [12]

Indeed, right in line with the constructive tendencies he demonstrated by following Brouwer, Weyl structured his number theory text around the Kronecker and Hensel versions of the theory of algebraic numbers. In the preface he wrote,

> ... In Chapter II I have axiomatized Kronecker's approach to the problem of divisibility, which has recently been completely neglected in favour of ideals; the reasons for this procedure are given in the text. The ultimate verdict may be that the one outstanding way for any deeper penetration into the subject is the Kummer-Hensel p-adic theory. ... (Weyl 1940, p. iii)

In his Chapter II, Section 11, entitled "Kronecker and Dedekind", Weyl expressed his reasons for preferring Kronecker's theory over Dedekind's, writing,

> As both theories are actually equivalent one can dissent about questions of convenience only. To my judgement the odds are here definitely against Dedekind. His theory suffers from a certain lack of self-sufficiency, in so far as its proofs resort to indeterminates and pivot around the fundamental Lemma II 7, A, tools which are native to Kronecker's set up, alien to Dedekind's. A proof of Theorem II 8, A, so simple by means of forms and their contents, seems nearly impossible without this instrument. Kronecker's criterion of divisibility is one decidable by finite means, while Dedekind's criterion refers to the infinite set of all possible integers λ. This has further awkward consequences. The question whether the number α in κ is divisible by the divisor $(\alpha_1, \ldots, \alpha_r)$ in κ is answered by

[12] Hilbert, translated in (Ewald 2005, pp. 943-944).

> Dedekind in different ways according to whether the question is put in κ or in a finite field K over κ, the answer requiring solvability of the equation
>
> $$\alpha = \alpha_1\Lambda_1 + \cdots + \alpha_r\Lambda_r$$
>
> by integers Λ_i in K in the second, by integers Λ_i in κ in the first case. It is a remote consequence of the theory that both requirements agree, while in Kronecker's theory the embedding field, κ or K, is irrelevant for the definition. (In a joint paper with H. Weber, laying the foundations for an arithmetical theory of the algebraic functions of one variable, Dedekind himself adopted a method closely related to Kronecker's approach; cf. H. Weber, Lehrbuch der Algebra, 2d ed., Braunschweig 1908, vol. 3, 5th book.) [13]

Proceeding then to discuss the relative merits of the Kronecker and Dedekind approaches when one passes to fields of rational functions in several variables, Weyl eventually brought his discussion around to Kummer and Hensel:

> The question naturally arises whether one can algebraize the Puiseux expansions and thus develop a new universal method for the construction of prime divisors. In fact the oldest approach to the theory of algebraic numbers, that of Kummer, follows this line. Kummer did not win through to a perfectly general formulation, to whatever depths he penetrated in his special study of the cyclotomic fields. It was left to Hensel, who was guided by the analogy with the Puiseux expansions, to carry Kummer's approach to the finish by means of his idea of p-adic numbers. The next chapter will be devoted to a careful preparation and development of this method. (Weyl 1940, p. 70)

And indeed, Weyl's Chapter 3 is called "Local Primadic Analysis (Kummer-Hensel)". At 70 pages, it occupies about one third of the book.

Edwards opens his investigation of Kronecker's theory of divisors (Edwards 1990) by attesting to the importance of Weyl's book in making Kronecker's theory known:

> Today most mathematicians who know about Kronecker's theory of divisors know about it from having read Hermann Weyl's lectures on algebraic number

[13] (Weyl 1940, pp. 67-68). The parenthetical reference to the joint paper of Dedekind and Weber is Weyl's.

> theory, and regard it, as Weyl did, as an alternative to Dedekind's theory of ideals. (Edwards 1990, p. v)

Surprisingly, however, he goes on to state that Weyl to some extent missed the point, in failing to observe that Kronecker made the definition of greatest common divisors fundamental, rather than the achievement of factorization into primes. Edwards adds that,

> The reason Kronecker gave greatest common divisors the primary role is simple: they are independent of the ambient field while factorization into primes is not.

If this was the main advantage of Kronecker's theory, then Edwards's assessment of Weyl seems unfair, since Weyl most certainly did observe this, as we saw above when he wrote that, "It is a remote consequence of [Dedekind's] theory that both requirements agree, while in Kronecker's theory the embedding field, κ or K, is irrelevant for the definition." Weyl's statement lacks some precision, in that Kronecker did not work with fields, but his main point stands.

If it was through Weyl that Kronecker's theory was made known, then surely the same book had some impact in popularizing Hensel's approach. Hensel's own book, TAZ, was read by some, and in contrast to Kronecker's notoriously difficult and sketchy *Grundzüge*, is written with great clarity, employs normal modes of expression, and proceeds slowly and methodically. It is named in the very short bibliography of Weyl's book, and might in that way have been brought to some people's attention. It, and Hensel's *Zahlentheorie* (Hensel 1913) after it, would also have been made known through Hasse's *Zahlentheorie* (Hasse 1949), which presented itself as the successor to those two books. [14]

It seems that these books of Hensel, Hasse, and Weyl might thus have stood as references and access points to the early computational tradition in algebraic number theory, and we will therefore be careful to note in Chapter 6 the several ways in which Zassenhaus's computational work of 1969 drew time and again on both (Weyl 1940) and (Hensel 1908). This is one respect in which we may say that there was some causal connection between Zassenhaus's work and that of his predecessors, so that he was not merely *reinventing* computational methods, but actually *reviving* (and modifying) them. These books, and Zassenhaus's use of them, in this way stand as some evidence of continuity in the computational tradition in algebraic number theory.

[14] A favorable 1910 review of TAZ by Dickson (Dickson 1910), appearing in the Bulletin of the American Mathematical Society, might also have helped make the book visible in the American scene.

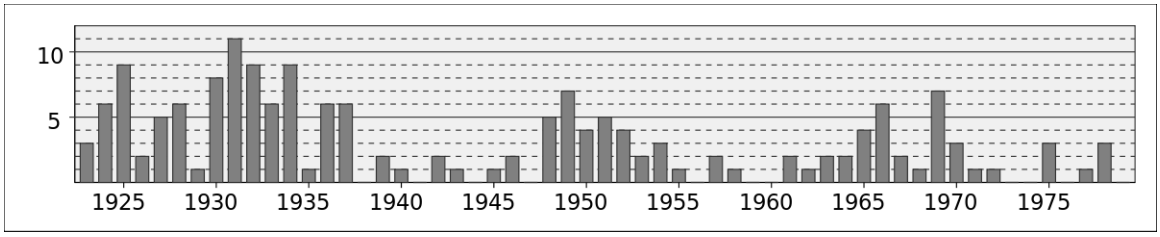

Figure 4.1: Number of papers published by Helmut Hasse each year, from 1923 to 1979. Source: (ibid.)

4.4 Hasse's view

In this section, we attempt to understand Hasse's view of the methodological divides in the subject of algebraic number theory. In the process we will quote at length from the forewords and introductions to his early post-war works *Zahlentheorie*, [15] and *Über die Klassenzahl Abelscher Zahlkörper* (KAZ), in which he made bold statements comparing the divisor-theoretic and ideal-theoretic approaches, and examining what he characterized as the largely unaddressed need for computational treatments of the theory.

These works were published at the beginning of what appears as the second of three overall surges of publishing activity over the course of Hasse's career, as shown in Figure 4.1. KAZ (but not *Zahlentheorie*, since it was completed already in 1938) stands at the beginning of what Hasse's student H.W. Leopoldt identified as a definite phase in Hasse's lifework, which he characterized as beginning with "a return to the roots of algebraic number theory in Kummer" (*Rückbesinnung auf die Wurzeln der algebraischen Zahlentheorie bei Kummer*), and involving, *inter alia*, "problems in the constructive control of concrete fields of certain types", and especially directed toward the subject of Abelian number fields. (Leopoldt 1973, p. 2, p. 15 ff.)

In the quotations below, we will see Hasse calling for a new research program, devoted to the determination of practical means for the computation of essential objects and invariants of number fields such as integral bases, discriminants, systems of fundamental units, and class numbers. He felt the methods should be applicable to number fields beyond mere

[15] By Hasse's own account, (Hasse 1980) p. VI, the manuscript was completed by 1938, but was delayed in publication until 1949, due to "the war and other circumstances".

quadratic ones, the only ones he said were yet fully understood.

In this, we will be tempted to see Hasse promoting the very transition – from computability in principle to computability in practice – that we have set out to examine. For at the same time that he will call for practical computation in algebraic number theory, he will appear to characterize this as the natural continuation of the approach of his mathematical forefathers Hensel and Kronecker. He may be right. We will, however, see him blur the analysis we made in Chapter 1 between the two distinctions, divisors versus ideals on the one hand, and computability versus existence on the other. We therefore must remain critical as to whether Hasse was merely passively carrying on the program he was brought into as a student, or actively giving this program a new focus.

4.4.1 Hasse's *Zahlentheorie*

The foreword

We get a clear summary of Hasse's view of the history of his subject in the foreword to (Hasse 1949), signed in Berlin, February 1949 – at least, this is how he saw things at this point in his career. To begin with, he outlined a dichotomy in the subject which for him seemed to run parallel to, or perhaps even to be coincident with, the one we are presently concerned with, between the computational and existence approaches. We quote from Zimmer's English translation (Hasse 1980):

> There are two quite distinct approaches, the *divisor-theoretic* and the *ideal-theoretic*, to the theory of algebraic numbers. The first, based on the arithmetic researches of Kummer and Kronecker and on the function-theoretic methods of Weierstrass, was developed by Hensel at the turn of the century; it was expanded by the general field theory of Steinitz and the general valuation theory of Kürschák, Ostrowski, and others. The second approach was conceived somewhat earlier by Dedekind, further developed by Hilbert, and was then expanded by the general ideal theory of Emmy Noether, Artin, and others.

He turned then from this purely factual, historical account, to more editorial statements about the relative merits of the two approaches, attributing to his favoured one both an enhanced simplicity and naturality of expression, and the power to reveal "the true significance of class field theory and the general reciprocity law:"

> It seemed at first that the ideal-theoretic approach was superior to the divisor-theoretic, not only because it led to its goal more rapidly and with less effort, but also because of its usefulness in more advanced number theoretic research. For Hilbert and, after him, Furtwängler and Takagi succeeded in constructing on this foundation the imposing structure of class field theory, including the general reciprocity law for algebraic numbers, whereas on Hensel's side no such progress was recorded. More recently however, it turned out, first in the theory of quadratic forms and then especially in the theory of hypercomplex numbers (algebras), not only that the divisor-theoretic or *valuation-theoretic* approach is capable of expressing the arithmetic structural laws more simply and naturally, by making it possible to carry over the well-known connection between local and global relations from function theory to arithmetic, but also that the true significance of class field theory and the general reciprocity law of algebraic numbers are revealed only through this approach. Thus, the scales now tip in favour of the divisor-theoretic approach.

Let us note that the German term which Zimmer translated by "approach" is *Begründungsweise*. A more literal translation, if too awkward, would perhaps be "way of setting the foundations". More than just the "way of looking at things" or "set of methods" that the term "approach" might denote, the German term seems to also include the ontological matter of a "way of saying what things are" as well as the logical matter of a "way of building up the theory from first assumptions". These meanings could possibly suggest that for Hasse there was a struggle to define not just how the subject of algebraic number theory ought to be handled, but what it actually was: what objects it was concerned with, and what theorems it was built up out of.

Hasse went on to discuss the state of the literature in 1949:

> At the present time, the only comprehensive treatments of the divisor-theoretic approach are the two books by Hensel, Theorie der algebraischen Zahlen, I (Leipzig, 1908) and Zahlentheorie (Berlin and Leipzig, 1913). Therefore, it now seems appropriate to give an exposition of the present state of our knowledge of this approach. The present book is intended to fill this frequently expressed desire. The manuscript was completed already in 1938, but the war and other circumstances delayed its appearance until now.

> The book originated from lectures that I had given at the universities of Marburg and Göttingen during the thirties. Its spiritual father, my esteemed teacher Kurt Hensel (1861 - 1941), participated with enthusiasm in its planning. It is a great sorrow to me that he did not live to see it published.

Hasse thus depicted a mathematical context in which his approach had won recent successes and even excited the interest of many, but remained largely untold.

His tone was then in some ways the same, in some ways milder than the tenor of his foreword to KAZ, penned roughly four years earlier. There too, as we consider in Section 4.4.2, he mentioned recent successes of the divisor-theoretic approach, which he believed had "prepared the ground for the return to an organic equilibrium between the two approaches." (Hasse 1952, p. VIII) Yet, there was also an urgency to Hasse's 1945 prose, which seems to have been somewhat quelled by 1949. Perhaps by 1949 he felt his side had gained more of the recognition it deserved.

4.4.2 Hasse's *Über die Klassenzahl abelscher Zahlkörper*

In this section we quote at length from the introductory material to Hasse's 1952 book, *Über die Klassenzahl abelscher Zahlkörper* ("On the Class Number of abelian Number Fields"), which we refer to as KAZ.

The foreword

Hasse began the foreword to KAZ by recounting the basic history of his subject:

> From its first beginnings with Gauss, algebraic number theory developed under the hands of the great masters of this and the last century into a massive edifice, which today stands essentially complete, with general theorems, commanding methodological viewpoints, and deep structural insights. The first phase of this development was summarized by Hilbert, in his celebrated report on the theory of algebraic number fields (hereafter referred to as the *Zahlbericht*). This report presents in its first two parts the general foundations of the theory, and then elaborates in the following three parts on three special types of algebraic number fields, namely quadratic, cyclotomic, and Kummer fields. From today's

> standpoint these last three sections of Hilbert's *Zahlbericht* examine three special cases of the general theory of relative-Abelian number fields. [16]

Thus, Hasse portrays an example of progress in mathematics toward increasing generality, and the tendency to want to understand, or even "explain away" old subjects as being "mere special cases of something more general."

Hasse continued discussing basic history:

> These usher in the second phase of the development, to which Hilbert himself gave the impulse, with his bold conception of the class field concept, and the class field conjectures. In a three-part report (Hasse 1926, 1927, 1930) (hereafter referred to as the *Class Field Bericht*) subsequent to Hilbert's *Zahlbericht*, I have summarized this second phase, the theory of relative-Abelian number fields, in which class field theory is developed in its full generality and applied to the derivation of the general reciprocity theorem. [17]

At this point, Hasse left behind a mere historical account of the development of the theory, and transitioned into what reads as a sort of manifesto for computational algebraic number theory. He began with that crucial motivation for computing, the need to understand the subject, or as he said, "control" it, by seeing and working through numerical examples. In Sections 5.3 and 6.1 we will hear this sentiment echoed again and again by writers such as Olga Taussky and Hans Zassenhaus of survey articles on the new subject of computational number theory in the early era of electronic computers. Hasse proceeded:

---

[16](Hasse 1952, p. V): Die algebraische Zahlentheorie hat sich aus den ersten Ansätzen bei Gauß unter den Händen der großen Meister des vergangenen und dieses Jahrhunderts zu einem gewaltigen Lehrgebäude entwickelt, das heute überreich an allgemeinen Sätzen, beherrschenden methodischen Gesichtspunkten und tiefen strukturellen Einsichten im wesentlichen abgeschlossen dasteht. Die erste Phase dieser Entwicklung hat Hilbert (Hilbert 1897) in seinem berühmten Bericht über die Theorie der algebraischen Zahlkörper zusammenfassend dargestellt. Dieser Bericht bringt in seinen ersten beiden Teilen die allgemeinen Grundlagen der Theorie und geht dann in weiteren drei Teilen auf drei spezielle Typen algebraischer Zahlkörper des näheren ein, nämlich auf die quadratischen Zahlkörper, die Kreiskörper und die Kummerschen Zahlkörper. Vom heutigen Standpunkt ausgesehen führen diese letzten drei Teile des Hilbertschen Zahlberichts Spezialfälle der allgemeinen Theorie der relativ-abelschen Zahlkörper durch.

[17](Hasse 1952, p. V): *Sie leiten die zweite Phase der Entwicklung ein, zu der Hilbert selbst mit seiner kühnen Konzeption des Klassenkörperbegriffs und der Hauptsätze der Klassenkörpertheorie den Anstoß gab. Diese zweite Phase, die Theorie der relativ-abelschen Zahlkörper, in der die Klassenkörpertheorie in voller Allgemeinheit entwickelt und auf die Herleitung des allgemeinsten Reziprozitätsgesetzes angewandt wird, habe ich (Hasse 1926, 1927, 1930) im Anschluß an Hilberts Zahlbericht in einem dreiteiligen Bericht zusammenfassend dargestellt.*

> In this entire development, which has led to general theoretical, structural, methodological, and systematic viewpoints, the need felt by every true number theorist to gain explicit control of the subject by working through numerical examples has, however, been strictly confined to the background. Should one ask a number theorist today for which types of algebraic number field he is in a position to clarify the laws of the general theory through explicit accounting of the general structure invariants of the type of field in question, or even as preparation for that, only to produce, say, an integral basis, the discriminant, a system of fundamental units, and the class number, through a systematic process using structure invariants, the answer, if he is honest, will in general be: only for the quadratic number fields. Only in these fields does every number theorist, as well as many another mathematician, feel so at home that he can do, at will, whatever he wants with the concepts of the general theory, whereas in higher field types even with complete and sovereign control of the general theory such freedom of movement is severely restricted to the minimum. [18]

While later authors would promote computation in number theory by naming such practical motivations as the furnishing of examples for the purpose of formulating new conjectures, or the production of counterexamples in order to refute existing conjectures, few would write so colourfully and metaphorically as Hasse did, with his talk of "feeling at home" and "freedom of movement". Metaphorically, Hasse seemed to paint a picture of "exploring" a given number field by viewing its class number here, then walking there to view its discriminant, and so forth, with no obstructions to movement or vision.

---

[18] (Hasse 1952, pp. V-VI): *Bei dieser ganzen Entwicklung, die von allgemeinen theoretischen strukturellen, methodischen und systematischen Gesichtspunkten geleitet wurde, ist nun aber das jedem echten Zahlentheoretiker eigene Bedürfnis nach expliziter Beherrschung des behandelten Gegenstandes bis zur Durchführung numerischer Beispiele stark in den Hintergrund getreten. Fragt man heute einen Zahlentheoretiker, für welche Typen algebraischer Zahlkörper er in der Lage ist, die Gesetzlichkeiten der allgemeinen Theorie durch explizite Aufstellung der allgemeinen Strukturinvarianten für den betreffenden Körpertypus zu erläutern oder auch als Vorbereitung dazu nur etwa eine Ganzheitsbasis, die Diskriminante, ein Grundeinheitensystem und die Klassenzahl nach einem systematischen Strukturinvarianten Verfahren zugewinnen, so wird, wenn er ehrlich ist, die Antwort im allgemeinen lauten: nur für die quadratischen Zahlkörper. Nur in diesen Körpern fühlt sich heute jeder Zahlentheoretiker und wohl auch mancher andere Mathematiker so zu Hause, daß er in ihnen mit den Begriffen der allgemeinen Theorie nach Belieben schalten und walten kann, während in höheren Körpertypen selbst bei völliger und souveräner Beherrschung der allgemeinen Theorie die Bewegungsfreiheit zum mindesten stark eingeschränkt ist.*

Hasse continued, addressing what he considered a crucial aspect of computational methods, that they should have a broad range of routine applicability. In addition, he believed the computed results should have a certain canonicity:

> Certainly there is no lack of the first beginnings of a corresponding control of number fields other than quadratic ones, or of numerical examples added here and there for the clarification of the general laws. Yet most such beginnings are lacking in uniformity, in systematicity, and above all in the feeling that one should characterize fields of the kind in question not by random means of determination – such as say the coefficients of a generating equation, be they chosen haphazardly or normalized through some kind of reduction condition – but rather through structure invariants, like discriminant, associated class group, conductor, characters; and predominating in the numerical examples are ad hoc tricks and more or less groping guesses, as opposed to systematic calculation methods. Thus, for instance, for a given kind of field, let us say absolute-cyclic number fields, one can use the constructive method of the general theory for the determination of an integral basis; the basis thus obtained, however, will not in general be a distinguished one, formed from structure invariants. [19]

Here the "constructive method of the general theory" would seem to refer to that method of constructing an integral basis which we saw presented in a semi-constructive way in Hilbert, in Section 2.3, and in an entirely constructive way in Hensel, in Section 2.4. Interestingly, Hasse departs here from Hensel not in that he seeks a faster, more practical version of Hensel's construction, but in that he wants a more canonical construction.

We may note here as an aside that, ironically, it was in part the very same rejecting of the arbitrary and questing after the canonical which led Dedekind to abandon a generalization

[19](Hasse 1952, p. VI): *Zwar mangelt es nicht an Ansätzen zu einer entsprechenden Beherrschung auch anderer als quadratischer Zahlkörper und an numerischen Beispielen, die zur Erläuterung allgemeiner Gesetzlichkeiten hier und dort angefügt sind. Jedoch fehlt es den meisten solchen Ansätzen an Einheitlichkeit, an Systematik und vor allem an dem Gefühl dafür, daß man den zu behandelnden Körpertypus nicht durch zufällige Bestimmungsstücke – wie etwa die Koeffizienten einer erzeugenden Gleichung, sei diese willkürlich gewählt oder durch irgendwelche Reduktionsbedingungen normiert –, sondern durch Strukturinvarianten, wie Diskriminante, zugeordnete Klassengruppe, Führer, Charaktere, beschreiben sollte, und in den numerischen Beispielen herrschen ad hoc geschaffene Kunstgriffe und mehr oder weniger tastendes Erraten gegenüber systematischen Berechnungsverfahren vor. So kann man etwa für einen vorgelegten Körpertypus, sagen wir die absolut-zyklischen Zahlkörper, das konstruktive Verfahren der allgemeinen Theorie zur Gewinnung einer Ganzheitsbasis ablaufen lassen, jedoch erhält man auf diese Weise im allgemeinen nicht eine ausgezeichnete, aus Strukturinvarianten Bestimmungsstücken dieses Körpertypus gebildete Ganzheitsbasis.*

of Kummer's theory of ideal numbers along Henselian lines, which he himself had attempted. As we reviewed in Chapter 1, in such a theory the splitting of a rational prime p is governed by the factorization modulo p of the minimal polynomial of an arbitrarily chosen primitive element α for the number field in question. This arbitrariness led Dedekind to remark that this method failed to "reveal the *invariance* that these notions do in fact possess". [20] In Section 2.4 we saw the construction of an integral basis founded on the same choice of an arbitrary primitive integer β for the field in question. Yet whereas Dedekind responded by moving to the infinite sets that are ideals, Hasse simply said we have to try harder, and come up with algorithms that do use "structure invariants". In KAZ Hasse had some success in this direction, and we will see in Section 6.3 how he applied the techniques he developed in KAZ, putting great care into both the construction of singular primary numbers out of fundamental units, and the determination of the most natural and canonical normalizations of these numbers.

Continuing with the foreword to KAZ, Hasse called for computed results that could be presented in such a way as to provide true insight into the theory of number fields. We call special attention to this point here, because in Section 6.3 we will see Hasse again, about 23 years later, demanding this same thing, in a research collaboration with Zassenhaus and a student, Liang. This is perhaps a perfectly ordinary aspect of mathematical practice, i.e. to strive to render objects in just the right form so that the desired insight into their structure becomes possible, but it is nevertheless worth our time to take note of examples of this facet of the art of mathematics when we find them.

As Hasse addressed this point, he began with a somewhat puzzling reference to "North American works", in which his meaning is not obvious, although a good guess seems to be that he was referring to the giant, three-volume *History of the Theory of Numbers*, by L.E. Dickson (Dickson 1919). He proceeded:

> With a "*complete list of all cases*", as is the final goal in similar situations in numerous North American works, the need of deeper-striving number theorists is by no means satisfied. These often amply plain "*complete solutions*" are more often than not lacking in the assimilation of the examined subject into a general theory, and in the meaningful handling of special cases through structure invariants standard in this theory. One will, in a way reminiscent of certain works

[20] Piazza's translation (Piazza 2007, p. 454). Original quotation from (Dedekind 1878, p. 202).

> in the descriptive sciences or ancient history, gather and record all the material, admittedly in the most faithful way, but will neglect to interpret this "Collection, Arrangement, and System" in terms of general points of view, and to separate the essential from the inessential, and the law-like from the random. [21]

Whereas here Hasse drew out the importance of rendering computed examples in the right way, so that insight into the theory would become possible, next he addressed an entirely different aspect of their importance, namely, the understanding that could be gained during the process of computing. He spoke, in fact, not merely of the understanding there was to be gained, but also of the sheer joy he himself found in calculating. He did not neglect to make the standard point either, that it is in examples that mathematicians can perceive new laws.

> Regarding the working through of numerical examples, mentioned repeatedly above, I wish to avoid the misunderstanding here that, as opposed to general theorems, I ascribe to such examples an unwarranted importance. Many number-theoretic textbooks, works, or lectures are peppered throughout with numerical examples, and the general study goes forth entirely through them. Experience teaches that the reader or hearer, if he is not inordinately assiduous, simply falls into these examples, and loses the general thread of the study. He would rather find his own examples and work these through, and rightfully so. For the value of a numerical example of course lies not at all in the perfectly completed and presented calculation and its result, but rather in the activity which is required to work through it. The study of a general theory develops a potential of ability, of mental force, and of power over the treated material. The working through of an example is the touchstone to test whether one has internalized the theory and has superior control over it, and it is the test of the hard-won

[21] (Hasse 1952, p. VI): *Mit einer* complete list of all cases*, wie sie für solche und ähnliche Fälle in zahlreichen nordamerikanischen Arbeiten als Endziel registriert wird, ist das Bedürfnis des tiefer strebenden Zahlentheoretikers durchaus nicht befriedigt. Diesen uns oft reichlich flach erscheinenden* complete solutions *mangelt es meistens an der Eingliederung des betrachteten Gegenstandes in eine allgemeine Theorie und an dem sinnvollen Beherrschtsein des Spezialfalles von den in dieser Theorie maßgebenden Strukturinvarianten. Man wird an den Typus gewisser Arbeiten aus den beschreibenden Naturwissenschaften oder aus der Vorgeschichte erinnert, die zwar getreulichst alles Material sammeln und registrieren, aber versäumen, in diese Sammlung Ordnung und System zu bringen, sie nach allgemeinen Gesichtspunkten zu deuten und das Wesentliche vom Unwesentlichen, das Gesetzliche vom Zufälligen abzuheben.*

> power and strength. The exercise of this ability, the release of this power, the application of this strength creates in those who work the example themselves a complete feeling of joy and satisfaction, but not however in those who find the example already completed. I will only pose the question here, to what extent the same is true quite generally for every kind of mathematical activity, as for the development of mathematical theory; there remains much to be said. In physics, and quite rightly so, alongside the lectures on experimental physics goes a course of practical training, in which the receptive student's learning is secured through his own activity. In number theory an entirely analogous role is played by the working out of numerical examples. Moreover these are in the hands of research mathematicians precisely what experiment is for the physicist, namely one of the best means for discovering new laws. It should be clear now for which reasons I do and do not place value on the explicit control of the general theory through the working of numerical examples; in my own work they appear only then when there is sober rationale for it. [22]

Here Hasse turned from such general remarks back to the history of his subject. He next addressed dichotomies in the methodology of algebraic number theory, and we must

[22](Hasse 1952, pp. VI-VII): *Was die vorstehend mehrfach berührte Durchführung numerischer Beispiele betrifft, so möchte ich hier dem Mißverständnis vorbeugen, daß ich solchen Beispielen gegenüber allgemeinen Sätzen eine unberechtigte Bedeutung beimesse. Manche zahlentheoretischen Lehrbücher, Arbeiten oder Vorträge sind mit numerischen Beispielen geradezu gespickt, und es wird gar an ihnen die allgemeine Untersuchung fortgeführt. Die Erfahrung lehrt, daß der Leser oder Hörer, wenn er nicht übertrieben gewissenhaft ist, diese Beispiele einfach übergeht und dem allgemeinen Faden der Untersuchung nachstrebt. Er wird sich lieber selbst Beispiele suchen und diese durchführen, und das mit Recht. Denn der Sinn eines Zahlenbeispiels liegt doch keinesfalls in der formvollendet mitgeteilten Rechnung und ihrem Ergebnis, sondern in der Aktivität, die zu seiner Durchführung erforderlich ist. Das Studium einer allgemeinen Theorie entwickelt ein Potential von Können, von geistiger Kraft und von Macht über die behandelte Materie. Die Durchführung eines Beispiels ist der Prüfstein dafür, daß man sich dies Theorie innerlich zu eigen gemacht hat und sie souverän beherrscht, ist die Probe auf die gewonnene Kraft und Macht. Die Ausübung diese Könnens, das Spielenlassen dieser Kraft, die Anwendung dieser Macht löst bei dem, der das Beispiel selber rechnet, ein Vollgefühl von Freude und Befriedigung aus, nicht aber auch bei dem, der es fertig vorgesetzt bekommt. Die Frage, inwieweit Entsprechendes ganz allgemein für jede Art mathematischer Betätigung, also auch für das Entwickeln mathematischer Theorien gilt, will ich hier nur aufwerfen: es ließe sich viel dazu sagen. Mit vollem Recht tritt in der Physik neben die Vorlesung über Experimentalphysik das physikalische Praktikum, in dem das rezeptiv Erlernte in eigener Aktivität verfestigt werden soll. Eine ganz entsprechende Rolle hat in der Zahlentheorie die Durchführung numerischer Beispiele. Darüber hinaus sind sie in der Hand des forschenden Mathematikers genau das, was für den Physiker das Experiment ist, nämlich eines der Hauptmittel zur Auffindung neuer Gesetzlichkeiten. Hiernach ist klar, aus welchen Gründen und aus welchen nicht ich Wert auf die explizite Beherrschung der allgemeinen Theorie bis zur Durchführung numerischer Beispiele lege, aber in meiner Arbeit selbst solche nur dort bringe, wo es aus sachlichen Gründen geboten erscheint.*

let him spell these out in his own terms before we attempt to reconcile his view with the one we sketched out in Chapter 1. He would continue to use the phrase "explicit control" (*"explizite Beherrschung"*) to refer to one sort of mathematical practice. This might refer to the understanding one gains through the working of examples, or perhaps to the activity of developing methods to allow such working of examples. In any case, Hasse counterposed it against the general development of theory, i.e. the discovering and proving of new theorems.

After polemicizing against the way in which the viewpoint of Hilbert and of Dedekind "reigned" supreme, even while deviating from Gauss's original intention that "explicit control" of the theory be maintained, Hasse returned again to his colourful and metaphorical characterization of that which was lost in this departure. He continued to use kinesthetic terms – "freedom of movement" and such – to describe the sort of frustration there was in the inability to compute actual examples of the sorts of objects with which the theory of algebraic number fields was constantly concerned. He spoke again of the need to feel "at home" with these objects. This seems to have been a call for a kind of familiarity; and familiarity surely is to be gained through encounter with many examples.

> The sense that the explicit control of the subject in all its details should keep step with the general development of the theory was made known by Gauss, and later above all by Kummer in very pronounced terms. Directly in Kummer are an abundance of investigations along these lines, supplementary to his general theory of ideal numbers. Under the commanding influence exerted by Hilbert on the further development of algebraic number theory, however, this sense is more and more dwindling away. It is typical of Hilbert's approach, aimed entirely at the general and conceptual, at existence and structure, that in his *Zahlbericht* he dimissed in short notes and hints all studies and results of Kummer and others concerned with the explicit control of the subject, in order not to engage himself with them, just as he also systematically and consistently replaced Kummer's methods of proof, which were more computational, constructive, and hence easy to be carried out explicitly, by inference methods that were more conceptual, harder to understand numerically, and scarcely controlable. Also Dedekind, with his heavily conceptual methodology, already deeply advanced into axiomatics, had a vital part in this development, whereas on the other hand the more constructive methods of Kronecker and Hensel carry

on the tradition of Kummer, but against Hilbert's reigning influence gain general acceptance only with difficulty; meanwhile, let it be noted that in recent times decisive successes of this methodology have prepared the ground for the return to an organic equilibrium between the two approaches. We must of course not misjudge or diminish the great merit that Hilbert has earned through his undeviating, thorough upholding of the described viewpoint, in the rise of the theory of algebraic numbers to a state of impressive generality, conceptual clarity and perfect simplicity. His great successes and all that which those coming after him have been able to contribute toward the perfection of the building begun by him speaks for itself. Only in the course of my own participation in the end phase of this development I am ever more clearly and vividly aware that, despite all the dazzling beauty and imposing grandeur, still something essential is missing, with which one can feel at home in the established building. One must most thoroughly get to know its several floors, its several rooms in their special peculiarities and in their relation to the whole, and one must learn to move freely in them. To that end it appears to me, returning from the picture to the subject at hand, to be imperative that the standpoint opposed to Hilbert's as regards explicitness, and numerical detail, must be allowed to come ever more into its natural right. Guided by this point of view, I have already devoted relatively extensive space in the second part of my *Class Field Bericht*, which is concerned with the most general reciprocity law, to explicit formulas for this law, picking up with pre-Hilbertian studies. [23] In the present, larger work, I return to this point of view, with a new subject. [24]

---

[23] Hasse examines, for example, work of Eisenstein (1823-1852), which was in existence long before Hilbert.

[24] (Hasse 1952, pp. VII-VIII): *Der Sinn dafür, daß die explizite Beherrschung des Gegenstandes bis in alle Einzelheiten mit der allgemeinen Fortentwicklung der Theorie Schritt halten sollte, war bei Gauß und später vor allem noch bei Kummer in ganz ausgeprägter Weise vorhanden. Gerade bei Kummer findet sich eine Fülle von in dieser Richtung liegenden ergänzenden Untersuchungen zu seiner allgemeinen Theorie der idealen Zahlen. Unter dem beherrschenden Einfluß, den Hilbert auf die weitere Entwicklung der algebraischen Zahlentheorie ausgeübt hat, ist jedoch dieser Sinn mehr und mehr verlorengegangen. Es ist typisch für Hilberts ganz auf das Allgemeine und Begriffliche, auf Existenz und Struktur gerichtete Einstellung, daß er in seinem Zahlbericht alle mit der expliziten Beherrschung des Gegenstandes sich befassenden Untersuchungen und Ergebnisse von Kummer und anderen durch kurze Hinweise oder Andeutungen abtut, ohne sich mit ihnen im einzelnen zu beschäftigen, wie er ja auch die mehr rechnerischen, konstruktiven und daher der expliziten Durchführung leicht zugänglichen Beweismethoden Kummers systematisch und folgerichtig durch mehr begriffliche, numerisch schwerer zugängliche und kaum kontrollierbare Schlußweisen ersetzt hat. Auch Dedekind mit seiner stark begrifflichen, schon tief ins Axiomatische vorstoßenden Methodik hat an dieser*

Thus, as far as dichotomies are concerned, Hasse spoke of "the standpoint opposed to Hilbert's as regards explicitness and numerical detail". This has nothing to do with divisors versus ideals, and everything to do with maintaining "explicit control" of the theory.

Still, one passage is a bit challenging to interpret:

> ...whereas on the other side the more constructive methods of Kronecker and Hensel carry on the tradition of Kummer, but against Hilbert's reigning influence gain general acceptance only with difficulty; meanwhile, let it be noted that in recent times decisive successes of this methodology have prepared the ground for the return to an organic equilibrium between the two approaches.

We must ask what were "the more constructive methods of Kronecker and Hensel" which "carry on the tradition of Kummer". Did Hasse mean the use of divisors, or simply the constructive character of the work? It seems far more likely that it was the methodology of divisors which "in recent times" had had "decisive successes". Here Hasse could have been referring to the reformulation of class field theory on p-adic foundations, for example, or to the unification of number theory and function theory in general. On the other hand, in what way could mere constructive or computational ideology have had recent "decisive successes"?

Entwicklung entscheidenden Anteil, während auf der anderen Seite die mehr konstruktiven Methoden von Kronecker und Hensel die Kummersche Tradition weiterführen, sich aber gegenüber dem beherrschenden Einfluß Hilberts nur schwer durchsetzen, bis dann allerdings in letzter Zeit entscheidende Erfolge gerade dieser Methodik den Boden für die Rückkehr zu einem organischen Gleichgewicht beider Richtungen bereitet haben. Es soll selbstverständlich nicht das große Verdienst verkannt oder geschmälert werden, das sich Hilbert gerade durch sein unbeirrbares, konsequentes Festhalten an der geschilderten Einstellung um die Aufwärtsentwicklung der Theorie der algebraischen Zahlen zu eindrucksvoller Allgemeinheit, begrifflicher Klarheit und formvollendeter Einfachheit erworben hat. Seine großen Erfolge und all das, was nach ihm Kommende in seinem Geiste und mit einen Methoden zur Vollendung des von ihm begonnenen Bauwerks beitragen konnten sprechen für sich. Nur ist mir im Laufe meiner eigenen Teilnahme an der Endphase dieser Entwicklung immer deutlicher und eindringlicher bewußt geworden, daß bei aller blendenden Schönheit und imponierenden Größe doch noch etwas Wesentliches fehlt, damit man sich in dem errichteten Bau auch so recht zu Hause fühlen kann. Man muß seine einzelnen Stockwerke, seine einzelnen Räume in ihrer besonderen Eigenart und in ihrer Beziehung zum Ganzen genauestens kennenlernen, und man muß lernen, sich in ihnen frei zu bewegen. Dazu erscheint es mir, vom Bilde zum Gegenstand zurückkehrend, geboten, die der Hilbertschen entgegengesetzte Einstellung auf das Explizite und auf das Detail bis zum Numerischen wieder mehr zu ihrem natürlichen Recht kommen zu lassen. Von diesem Gesichtspunkt geleitet, hatte ich schon im zweiten Teil meines Klassenkörperberichts, der sich mit dem allgemeinsten Reziprozitätsgesetz befaßt, den expliziten Formeln zu diesem Gesetz, anknüpfend an vorhilbertsche Untersuchungen, einen verhältnismäßig breiten Raum gegeben. Mit der vorliegenden größeren Arbeit greife ich diesen Gesichtspunkt an einem anderen Gegenstand erneut auf.

Moreover, Hasse's characterization of things forces us to reconsider our own distinction between computability in principle and in practice. At least in Kummer, Hasse saw methods of proof which were "more computational, constructive, and hence easy to be carried out explicitly" whereas we, on the other hand, have made a clear distinction between that which is computational and constructive, and that which is easy to carry out explicitly. In Section 2.4 we examined this through the work of Hensel, in which the methods of proof were surely constructive, although in many cases could never be carried out explicitly in a human lifetime. Might Hasse have meant only that Kummer's methods of proof were easy *in principle* to carry out explicitly? One perspective is, available from today's standpoint, is that the computation of most objects associated with number fields is of such an inherent complexity that computability in principle was the only kind of computability available before the advent of high speed computers.

With his motivating philosophy thus expressed, Hasse went on to indicate the particular subject matter with which he would attempt to enact his ideas in KAZ. He referred to some early table work by Sommer (Sommer 1907), which served for him as a model of the sort of data which we ought to be able to compute for any number field. He also mentioned early table work of Reuschle (Reuschle 1875). Both Sommer and Reuschle were named in Lehmer's *Guide* (Lehmer 1941).

Again, Hasse named two motivations for the computation of examples: the deepening of understanding, and the furtherance of the theory through the discovery of new laws. He did not mention applications.

> I have set myself the goal, if possible, to illuminate the class of absolute abelian number fields, or at least the class of absolute cyclic number fields, in a systematic way using structural invariants, to such a degree that one will then be able to move as freely there as in quadratic number fields. It should serve as touchstone for the reaching of this goal, that using the methods, formulas, and results to be developed here we are able to compute for these fields, by a schematic procedure, exactly the same tables that Sommer (Sommer 1907) gave for quadratic number fields in his well-known textbook. Such tables would form an extremely valuable tool, just as Sommer's tables do already today, for every number theorist who would like to form numerical examples for the already established general laws of algebraic number fields and for possible further such laws, be it in order to

> deepen his or her own inner grasp of the theory, or be it in order to discover by experimentation the trail toward new laws and connections. In this direction there have been until now only the tables of complex numbers calculated by Reuschle (Reuschle 1875) on the basis of Kummer's data, which are however, despite the abundance of numerical material compiled in them, unsatisfying, since they do not contain certain essential things, namely fundamental units, class numbers, and class groups. [25]

Later, as we will note in Chapter 6, in the early 1960s Zassenhaus would articulate a similar program for computational algebraic number theory, in which computing the group of fundamental units, and the class group of a number field were two of his main goals. Hasse proceeds:

> The present work shall develop, as a first contribution toward the indicated broad objective, the foundation for the computation of the class number of absolute Abelian number fields. Moreover it is thought of as a supplement to Hilbert's *Zahlbericht* and my *Class Field Bericht.* [26]

Here it would seem that Hasse wanted to characterize work on the computation of number field objects and invariants as the third chapter in the overall development of the theory of algebraic number fields, the first being the basic work summarized in Hilbert's *Zahlbericht*, and the second being the class field theory summarized in his *Class Field Bericht.*

---

[25](Hasse 1952, p. VIII): *Ich habe mir zum Ziel gesetzt, wenn möglich die Klasse der absolut-abelschen Zahlkörper, zum mindesten aber die Klasse der absolut-zyklischen Zahlkörper in systematischer und strukturinvarianter Weise so weitgehend zu erschließen, daß man sich in ihnen ebenso frei bewegen kann wie in den quadratischen Zahlkörpern. Als Prüfstein für die Erreichung dieses Zieles mag gelten, daß es auf Grund der zu entwickelnden Methoden, Formeln und Ergebnisse gelingt, für diese Körper nach einem schematischen Verfahren ebensolche Tafeln zu berechnen, wie sie Sommer (Sommer 1907) für die quadratischen Zahlkörper seinem bekannten Lehrbuch beigegeben hat. Derartige Tafeln würden für jeden Zahlentheoretiker, der sich für die schon gewonnenen allgemeinen Gesetzlichkeiten aus der algebraischen Zahlentheorie und für etwaige weitere solche Gesetzlichkeiten numerische Beispiele bilden will, sei es um sich die Theorie innerlich nahezubringen, sei es um auf experimentellem Wege neuen Gesetzen und Zusammenhängen auf die Spur zu kommen, ein äußerst wertvolles Handinstrument bilden, so wie es die Sommerschen Tafeln schon heute sind. Bisher liegen in dieser Richtung nur die nach Kummers Angaben berechneten Tafeln komplexer Primzahlen von Reuschle (Reuschle 1875) vor, die aber trotz der Fülle des in ihnen zusammengetragenen Zahlenmaterials unbefriedigend sind, weil sie gerade die wesentlichen Dinge, nämlich Grundeinheiten, Klassenzahl und Klassengruppe, nicht enthalten.*

[26](Hasse 1952, p. IX): *Die vorliegende Arbeit soll als ersten Beitrag zu der genannten umfassenden Zielsetzung die Grundlagen für die systematische Berechnung der Klassenzahl absolut-abelscher Zahlkörper entwickeln. Darüber hinaus ist sie als eine Ergänzung des Hilbertschen Zahlberichts und meines Klassenkörperberichts gedacht.*

It is not clear whether others shared Hasse's view on this point, but at least this seems to show very clearly how Hasse envisioned the overall arc of the development of algebraic number theory: explicit, practical computation was to be the third major phase.

Hasse completed his statement in the following way:

> Besides the view toward the utilization of the general class number formula for the actual computation of the class number, we will aim to report on the results of Kummer and others for the class number of cyclotomic and other kinds of fields, to generalize these results to arbitrary absolute Abelian number fields, and to examine them from the standpoint of general class field theory.
>
> In addition to the actual results on the class number of absolute Abelian number fields, the work contains also a wealth of algebraic and number-theoretic detail attractive in itself, in part in the proofs that have been included, in part, to name a few highlights, in a peculiar generalization of the well-known decomposition of the group determinant of an Abelian group into linear factors, theorems on the ramification behaviour of an absolute Abelian number field over its maximal real subfield, as well as a novel auxiliary to Gauss's Lemma on quadratic residues. Contrary to many statements on the other side, I have always been of the view that classical number theory, with its goals and methodology directed toward the reality of the natural numbers, today is by all means still capable of vital and fruitful further development on its very own grounds, and that one need not look to abstract algebraic fields, or to topology, set theory, or axiomatics in order to find new sustenance for arithmetic activity. As in music one remembers fondly the romantic and post-romantic eras, steeped in heroic and demonic works, and in audacious fantasy, but thinks more deeply on the fountainhead of purer and plainer musicality of the old masters, so it seems to me that also in number theory, which indeed like hardly any other mathematical discipline is ruled by the law of harmony, a return is bidden to that which the great masters who established it had in mind as its true face. The present work endeavours to be a spirited testimony to this view

> of mine, and to point the way toward further studies in the same field. [27]
>
> Göttingen, August 1945

The introduction

Something which is not apparent in the Foreword, but which does emerge later, in the Introduction, is another motivation for the work, which would prove a consistent methodological theme in Hasse; we will see it again in his work on the class field of $\mathbb{Q}(\sqrt{-47})$ in Section 6.3. Namely, Hasse was interested in a kind of methodological purity, in that he wanted not only a method for computing the class number of an algebraic number field, but a *purely arithmetical* method.

This was nothing new in algebraic number theory, whose practitioners had long been troubled by the presence of transcendental methods in what seemed, morally, to be a purely arithmetical subject. For another example from Hasse, consider his statement about Takagi's class field theory:

> There is a further fault of beauty in Takagi's class field theory that was obviated by Chevalley (1940). This is the recourse to analytic means (Dirichlet's L-series) for the proof of the first fundamental inequality $h \leq n$. Chevalley succeeded in proving this inequality in a purely arithmetical manner. (Hasse 1967, p. 276).

[27] (Hasse 1952, p. IX): *Neben den Gesichtspunkt der Ausnutzung der allgemeinen Klassenzahlformel zur wirklichen Berechnung der Klassenzahl wird demgemäß der Gesichtspunkt treten, über die von Kummer und anderen gewonnenen Ergebnisse für die Klassenzahl der Kreiskörper und einiger anderer Körpertypen zu berichten, diese Ergebnisse auf beliebige absolut-abelsche Zahlkörper zu verallgemeinern und sie vom Standpunkt der allgemeinen Klassenkörpertheorie aus zu beleuchten. Neben den eigentlichen Ergebnissen über die Klassenzahl absolut-abelscher Zahlkörper enthält die Arbeit eine Fülle von auch an sich reizvollem algebraischem und zahlentheoretischem Detail, teils in die Beweise eingearbeitet, teils besonders hervorgehoben, so eine eigenartige Verallgemeinerung der bekannten Zerlegung der Gruppendeterminante einer abelschen Gruppe in Linearfaktoren, Sätze über das Verzweigungsverhalten eines absolut-abelschen Zahlkörpers über seinem größten reellen Teilkörper sowie ein neuartiges Seitenstück zum Gaußschen Lemma über quadratische Reste. Entgegen mancher Äußerung von anderer Seite bin ich immer der Auffassung gewesen, daß die klassische Zahlentheorie mit ihrer auf die Wirklichkeit der natürlichen Zahlen gerichteten Zielsetzung und Methodik heute durchaus noch einer lebendigen und fruchtbaren Weiterentwicklung auf dem ihr ureigenen Boden fähig ist, auch ohne daß man in abstrakten algebraischen Gefilden oder in Topologie, Mengenlehre, Axiomatik neue Nahrung für den arithmetischen Betätigungsdrang zu suchen braucht. Wie man sich in der Musik nach der in heroischen und dämonischen Werken und in kühnsten Phantasien schwelgenden romantischen und nachromantischen Epoche heute bei aller Freude an diesem Schaffen doch auch wieder stärker auf den Urquell reiner und schlichter Musikalität der alten Meister besinnt, so scheint mir auch in der Zahlentheorie, die ja wie kaum eine andere mathematische Disziplin von dem Gesetz der Harmonie beherrscht wird, eine Rückbesinnung auf das geboten, was den großen Meistern, die sie begründet haben, als ihr wahres Gesicht vorgeschwebt hat. Die vorliegende Arbeit mag ein lebendiges Zeugnis für diese meine Auffassung sein und weiteren Untersuchungen auf dem betretenen Felde den Weg weisen.*

Or, for example, consider the way in which Hilbert introduced his new proof of the Kronecker-Weber theorem:

> The present note contains a new proof, which requires neither the Kummerian decomposition of the Lagrange resolvent in prime ideals, nor the application of the transcendental methods, foreign to the essence of the theorem, of Dirichlet. [28]

Or again, consider his paper (Hilbert 1894) on the Dirichlet biquadratic number field, in which his purpose was to redevelop Dirichlet's theory, only on a purely arithmetical ground, and without use of Dirichlet's analytic methods. In 1949, Selberg and Zassenhaus independently took great pains to produce elementary proofs of Dirichlet's theorem on primes in arithmetic progressions. Even Euler, having already given a proof of the "little theorem" of Fermat based on a series expansion of $(a+b)^n$, later found a more purely number-theoretic proof, and called this one "more natural". [29] The subject of methodological purity as a motivator in mathematics has been taken up in one part of the collection (Mancosu 2008).

It is in any case important to understand that this methodological concern was part of what drove Hasse. He wrote, in the introduction to KAZ:

> One has always taken the standpoint that this class number formula, admittedly flowing from an analytic source while essentially arithmetic, is a final goal, and that therefore with its deduction all is done. Already the simplest example of the quadratic number field shows however that the formula in the form in which it is initially obtained is hardly or not at all appropriate for the actual arithmetic computation of the class number, for one thing because this computation in particular cases requires unmanageably large numerical calculations, and for another because the formula still contains analytic elements, remnants of its deduction, which are foreign to the numerical calculation methods of number theory. A procedure in which one has to call upon the logarithm table and the trigonometric tables cannot be viewed as a computation which is, in the true sense, arithmetic. Thus one has abandoned the application of the formula to the actual computation of the class number, and in its place offered the fumbling

[28](Hilbert 1896), reprinted in (Hilbert 1981a, p. 53): *Die vorliegende Note enthält einen neuen Beweis, welcher weder die Kummersche Zerlegung der Lagrangeschen Resolvente in Primideale noch die Anwendung der dem Wesen des Satzes fremdartigen transcendenten Methoden von Dirichlet erfordert.*

[29](Euler 1915, p. 510), quoted in (Wussing 1984, p. 51).

guess-and-check process applicable to arbitrary algebraic number fields, which rests on the well-known theorem: In every divisor class of an algebraic number field of degree n, with r_2 pairs of complex-conjugate conjugate fields, and with discriminant d, there is an integral divisor $\mathfrak{a}$ with $N(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{d}$. Here now, one has with great difficulty found a wonderful explicit formula for the class number, and then given up resignedly on its actual application; what a pitiful standpoint for the number theorist concerned with his abilities! For him however, after shedding away those tools foreign to him though until now indispensable for the deduction, begins here first the true problem, namely to put the formula into a form suitable for arithmetic computation. How this problem is to be tackled and to be coped with, I have (Hasse 1940) briefly shown, in the case of the real quadratic number field of prime discriminant. In continuation thereon, my student Bergström (Bergström 1944) has been successful in extending this method to all real quadratic number fields. Moreover I can at this time give the solution to this problem also for the real cyclic cubic and biquadratic number fields, as I will present in another place (Hasse 1950a). [30]

[30](Hasse 1952, pp. 1-2): *Man hat sich bisher immer auf den Standpunkt gestellt, daß diese zwar aus analytischer Quelle fließende, aber doch wesentlich arithmetische Klassenzahlformel ein Endziel ist und daß daher mit ihrer Herleitung alles getan sei. Schon das einfache Beispiel der quadratischen Zahlkörper zeigt jedoch, daß die Formel in der zunächst erhaltenen Gestalt für die tatsächliche arithmetische Berechnung der Klassenzahl wenig oder gar nicht geeignet ist, einmal weil diese Berechnung in gegebenen Fällen unverhältnismäßig große numerische Rechnungen erfordern würde, und dann weil die Formel noch von ihrer Ableitung herrührende analytische Elemente enthält, die den numerischen Rechenmethoden der Zahlentheorie fremd sind. Ein Verfahren, bei dem man die Logarithmentafel und trigonometrische Tafeln heranzuziehen hat, kann nicht als eine im eigentlichen Sinne arithmetische Berechnung der Klassenzahl angesehen werden. Daher hat man auf die Anwendung der Formel zur wirklichen Berechnung der Klassenzahl verzichtet und statt dessen das für beliebige algebraische Zahlkörper anwendbare tastende Probierverfahren empfohlen, das sich auf den bekannten Satz stützt: In jeder Divisorenklasse eines algebraischen Zahlkörpers vom Grade n, mit r_2 Paaren konjugiert-komplexer Konjugierter und mit dem Diskriminantenbeitrag d, kommt ein ganzer Divisor $\mathfrak{a}$ mit $N(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{d}$ vor. Da hat man nun mit viel Mühe eine wunderschöne explizite Formel für die Klassenzahl gewonnen und verzichtet dann resigniert auf ihre wirkliche Anwendung; welch ein trauriger Standpunkt für den sich seiner Kraft bewußten Zahlentheoretiker! Für ihn beginnt doch hier, nach Abstreifen des ihm fremdartigen, zur Herleitung bisher unentbehrlichen Rüstzeuges, erst die eigentliche Aufgabe, nämlich die Formel in eine der arithmetischen Rechnung zugängliche Gestalt zu setzen. Wie diese Aufgabe anzupacken und zu bewältigen ist, habe ich (Hasse 1940) kürzlich am Beispiel der reell-quadratischen Zahlkörper von Primzahldiskriminante Zeigen können. Im Anschluß daran ist es meinem Schüler Bergström (Bergström 1944) gelungen, diese Methode auf alle reell=quadratischen Zahlkörper auszudehnen. Darüber hinaus konnte ich die Lösung jener Aufgabe vorerst einmal auch für die reellen zyklischen kubischen und biquadratischen Zahlkörper geben, was ich an anderer Stelle darlegen werde (Hasse 1950a).*

Chapter 5

Taussky-Hasse correspondence in the 1950s

Having considered now the program that Hasse sketched in KAZ for the making practical of the computation in principle that his mathematical forefathers had espoused, we must ask what he or others did about it. Was the work carried out? By whom? When, why, and how? In this chapter we focus on one particular researcher, Olga Taussky, who contributed to a research program like the one Hasse had in mind, and who we may view as having provided a link between Hasse and Zassenhaus, given her interactions with the former, and her role in the beginning of the latter's involvement in the subject.

In Section 3.5 we saw the emphasis Taussky and Scholz placed on "rational methods", and in Section 5.3 we will see Taussky return to this key point again, in a survey talk she gave in 1953 on the emerging field of computational algebraic number theory. We consider there how the image of algebraic number theory in Kronecker – in which one simply works with polynomials modulo other polynomials – had resurfaced now that researchers wanted to represent algebraic numbers in data structures inside a computer.

When we left off with Taussky's story in Chapter 3, she had been appointed to a teaching position at Westfield College of the University of London in 1937, and had been on war leave from 1943 to 1946 to work in an aerodynamics group.

Besides introducing her to matrix theory, the war work brought Taussky into computers. Davis writes (Davis 1997) that, "The Todds' war work coincided with the start of the great

expansion of number-crunching technique." [1] The expertise the duo gained in this work must have made them attractive to the U.S. National Bureau of Standards (NBS), which was involved in such computation-heavy tasks as operations research for the U.S. Air Force, and to von Neumann as well, for, as noted in (Luchins and McLoughlin 1996), the Todds crossed the Atlantic in September 1947, headed for the NBS's National Applied Mathematics Laboratory, where they would work under John H. Curtiss, [2] and along the way they stopped first at the IAS, working briefly in the Electronic Computer Project of von Neumann. They appear thus to have been, for a little while, touring about as a pair of computer experts, at a time when there were only one or two dozen computers in the world.

Hasse's *Nachlass* [3] contains many letters between him and Taussky, [4] but only a few of them are from the 1930s. We noted one in Section 3.5 already, pertaining to Taussky's work with Scholz. In another, from 1937, Hasse talked about how busy he was with work on his *Zahlentheorie*, which, he wrote, "indeed is based on entirely different foundations, and will be very extensive."

One letter especially foreshadows their later collaboration in the 1950s. It was sent by Taussky on 27 October 1936, from Girton College, Cambridge, and shows that Hasse had circulated a proposal for the computation of tables of class numbers. Taussky raised a few points regarding the practicality of the computations and the notion Hasse had evidently put forth that untrained human computers could be employed to carry out the work. Given that the two would about fifteen years later find themselves once again discussing the practicalities of employing an "untrained labourer" – this time an electronic machine – for the computation of class numbers and other number theoretic quantities, the letter appears ironic indeed.

It seems that correspondence between Taussky and Hasse resumed in or shortly before June 1949, after a hiatus of perhaps as many as 10 years [5], due most likely to the disruption caused by the war. It was just a couple of months before the Todds would make their

[1] By this time, Olga Taussky was married to fellow mathematician Jack Todd.

[2] Later, Curtiss would be editor of the Proceedings of the 1953 Symposium in Applied Mathematics (Curtiss 1956), in which Taussky's survey on computational algebraic number theory (Taussky 1953) would appear.

[3] I.e. the papers and notebooks left behind after he died.

[4] Helmut Hasse and Olga Taussky. Correspondence. Cod. Ms. H. Hasse 1:1696. Niedersächsische Staats- und Universitätsbibliothek Göttingen.

[5] Many letters are missing from the *Nachlass*, so the absence there of any letters between 1939 and 1948 is not conclusive.

permanent move to the States, and both Taussky's return to number theory and her use of computers for pure mathematical research would begin. We therefore take advantage of excerpts from their letters to give us insight into their professional relationship, and in particular to see how their interactions were important in the history of computational algebraic number theory.

Among the things we will see in the sections below are the following: discussion between Hasse and Taussky of two important works of Hasse in the subject of computational algebraic number theory, namely KAZ and another work (Hasse 1950a) which would play a part in his collaboration with Zassenhaus and Liang in the late 1960s; discussion of Taussky's 1953 survey talk (Taussky 1953) on the emerging subject; in-depth discussion of a number theoretic job which Hasse asked Taussky to run on NBS computers; intimations of specifically *algebraic* number theoretic computations which both Hasse and Taussky seem at first independently and later together to have considered.

In general the letters contain more than is reproduced here. In quotations, ellipses "..." standing alone as paragraphs have been used to indicate that one or more paragraphs from the original letters have been omitted.

In her position at the U.S. National Bureau of Standards, first in Washington D.C. and later in Los Angeles, Taussky had access to two of the earliest electronic computers anywhere in the world. In D.C. she could use the SEAC (Standards Eastern Automatic Computer) and in L.A. she could use the SWAC (Standards Western Automatic Computer). We note that the Lehmers used the SWAC as well, and at the same 1953 conference at which Taussky gave her survey on work in computational algebraic number theory, Emma Lehmer presented work on Fermat's Last Theorem, which she had carried out on this machine (Lehmer 1956).

The SEAC and the SWAC were planned in late 1948 resp. January 1949, and were completed and fully operational by April 1950 resp. July 1950. Their construction had been urged by George Dantzig (1914 - 2005), the expert in operations research, when the U.S. Air Force wanted the NBS to help it with some of its operations research problems. The NBS was waiting for the completion of both the UNIVAC by Eckert and Mauchly, and the IAS machine by von Neumann. Both of these machines would be highly powerful, but their completion was taking too long, and Dantzig impatiently insisted that some very simple machines be built in the interim. The USAF agreed to fund this project, and the SEAC and the SWAC were built. (Williams 1985, pp. 367-371)

Eckert and Mauchly, we note, are also well known as two of the main engineers behind the ENIAC. That the SEAC and SWAC predated even their UNIVAC, in this era of acronym-named behemoth machines, should illustrate clearly just how early in the electronic computer era Taussky had access to machines. The SEAC was in fact the first fully operational stored-program electronic computer in the U.S. (only some test runs had been done on the BINAC nine months earlier). As for the SWAC, when it became operational in July 1950 it was the fastest machine in the world, only to be surpassed in speed by von Neumann's IAS machine a year later. (Williams 1985)

As for the simplicity of the SEAC and SWAC that would allow their rapid design and construction, part of this had to do with their hardware, and part to do with the machines' logic and operational capabilities. The latter is of interest to us here, in that it helps us to imagine what it meant to translate problems in algebraic number theory onto these machines. The SEAC had just seven basic instructions : addition, subtraction, multiplication, division, comparison, input, and output. On the SWAC there were eight basic instructions: addition, subtraction, multiplication (both single and double length), comparison, input, output, and something called "data extraction". Notably, division is not listed. (ibid.)

The SWAC had been constructed specifically for the NBS's Institute for Numerical Analysis (INA), and was used by the INA until this Institute was disbanded by the NBS in 1954. At that time, the SWAC was brought to UCLA, and was used there until late 1967. (ibid.)

Meanwhile in Germany, where Hasse was, it took longer for machines to become available. Konrad Zuse (1910 - 1995) had begun to sketch designs for mechanical computing machines in 1934, while a civil engineering student in Berlin. During the war he was relieved from military service in order to work as an engineer in the aircraft industry. He built his first fully operational computing machine, the Z3, in 1941. He too, like Taussky, was involved in flutter calculations, i.e. the attempt to figure out aerodynamic conditions leading to flutter, which technically is a rapid periodic vibration that results from the natural frequencies of elements like wings being subjected to fluid flow:

> The work done with this machine during 1941-1943 included solution of linear equations up to third order, solution of quadratic equations, and evaluation of determinants with complex elements for aircraft flutter calculations. (Zuse 1980, p. 618)

It is not clear whether Zuse referred to the Z3 or the Z4 here.

Other special purpose machines were designed by Zuse during the war, for purposes such as control of missile construction processes. A collaborator, Helmut Schreyer, built computers which were purely electronic, while Zuse's machines were mechanical or electromechanical (i.e. using relays). It seems the two submitted a proposal to the German government to build an electronic computer with as many as 2000 vacuum tubes, but the idea was not supported. (Zuse 1980, p. 619) Even this would have been a smaller machine than the 18,000-tube ENIAC on the other side of the Atlantic.

Zuse writes that after the war he and colleagues could not continue developing computers until 1950. Then, sponsorship came from optical industries, land surveying authorities, and universities. Zuse states that it was only through the universities that there was any government funding. Zuse's factory was eventually purchased by the Siemens corporation.

In Chapter 6 we will find Hasse using a computer called the TR 4 at the University of Hamburg, for work published in 1964, 'TR' standing for *Telefunken Rechenautomaton*. The Telefunken company produced radio and vacuum tube equipment during the war, and was a joint venture of Siemens and the electrical equipment company AEG founded by Emil Rathenau, father of German statesman Walter Rathenau.

If Zuse and others had to wait until 1950 to resume work, whereas computer development in the U.S. and the U.K. continued unabated after the war, it is not hard to believe that Hasse would have had to wait longer than mathematicians in those countries to have a machine available to him. It was perhaps under these circumstances that he wrote to Taussky about number theoretic computations which he hoped she would run on the SEAC. Indeed, it is noted in (Williams 1985, p. 225) that Zuse continued producing the relatively primitive relay-based machines up into the mid-1950s, and only began designing a vacuum-tube-based machine in 1956, delivering it in 1958.

5.1 Reestablishing contact

The Hasse *Nachlass* contains a letter from Taussky to Hasse, dated 1 June 1949, the text of which seems to suggest that Hasse had been the first to write, yet his letter, though many of his are present in the collection, is absent. Taussky began her letter by thanking Hasse for off prints of "three of [his] newer works" which she had received "a few days ago" and in which she was "naturally very interested". She asked him whether he might not also be

able to send her "the two first parts of the work in the *Mathematische Nachrichten,*" since, she said, "I cannot easily obtain these here."

It is clear from Hasse's bibliography that the three-part work of which he sent Taussky the third must have been "Existence and Multiplicity of Abelian Algebras with given Galois Group over a Subfield of the Ground Field" [6] It could not be any earlier work, since this appeared in the first volume of the *Mathematische Nachrichten*, in 1948.

Taussky went on to write that she had been, "already for many years no longer at Westfield College." She proceeded,

> I had for a few years a position in aerodynamics. Last year we were both in the U.S.A. and we intend to return to the same positions in late summer. My address is then from approximately mid-August onward: Division 11.0, National Bureau of Standards, Washington 25, D.C., U.S.A.

At the time of writing, her address was in Surrey, England.

It is thus clear that the mailing from Hasse containing the off prints indicated, in one way or another, that he still believed her to be at Westfield College. Since it was a mailing, one would therefore expect that he sent it to an old address which he had for her there. Perhaps it was then forwarded to her, and her mention of having received it only "a few days ago" was meant to address the delay this would have introduced.

In any case, Taussky's mention of her aerodynamics post would seem to indicate that their earlier period of correspondence must have ended no later than 1943, when Taussky took the job, unless perhaps for reasons of British national security she had simply been unable to discuss her work with him, while he resided behind the German enemy lines.

It seems odd that after years of silence Hasse would suddenly send unrequested off prints of his recent work to Taussky, yet if there had been any prior contact between them one would expect that she would already have discussed with him her work in the recent years of her life. Perhaps it was simply that in the reestablished peacetime, Hasse was gradually setting about resuming contacts broken by the war, and in early 1949 found the time to reach out to Taussky. We cannot be sure.

---

[6] *"Existenz und Mannigfaltigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers"*, parts I, II, and III, (Hasse 1948).

In the remainder of the letter, Taussky expressed how happy she was to finally be able to get back to number theory and algebra, and indicated that in her employment at the NBS she had been encouraged to apply computing to number theoretic or group theoretic problems:

> Fortunately I can now return to number theory and algebra, although through the many difficulties which we had for years, and my aerodynamic activities I am thus back somewhat sore. It is useless to lament the lost years. Hopefully it will now really be better. At the moment I am interested especially in the relations between classes of ideals and classes of matrices.
>
> In the U.S.A. my husband will again work on the application of ‘‘high-speed automatic digital computing machines’’ [7] and I have been encouraged to study number theoretic or group theoretic problems in this respect. [8]

Finally, she promised to send Hasse some off prints in a couple of days, and bid him to write whether they could send him anything from there, before signing off, *"Mit bestem Dank und freundlichen Grüssen".*

It does indeed seem that this letter, and the mailing from Hasse which must have preceded it, were a reestablishment of contact, for Hasse replied three weeks later, writing,

> I rejoiced over such friendly lines of yours, in remembrance of long gone old times; accept my best thanks for these. ... How nice that you can now once again work on algebra and number theory. I too was so happy, when in 1945 I could again apply myself to these ‘‘pure’’ things. [9]

---

[7] Taussky herself put the English phrase in quotes.

[8] *Glücklicherweise kann ich jetzt wieder Zahlentheorie und Algebra betreiben, aber durch die vielen Schwierigkeiten, die wir jahrelang hatten und meine aerodynamische Tätigkeit bin ich da arg zurück. Es ist nutzlos die verlorenen Jahre zu betrauern. Hoffentlich wird es jetzt wirklich besser sein. Im Augenblick interessiere ich mich besonders für die Beziehungen zwischen Klassen von Idealen und Klassen von Matrizen. Mein Mann wird in U S A wieder an der Anwendung von* "highspeed automatic digital computing machines" *arbeiten und ich bin ermutigt worden zahlentheoretische oder gruppentheoretische Probleme auch in dieser Hinsicht zu studieren.*

[9] *Über Ihre so freundlichen Zeilen habe ich mich in Erinnerung an längst vergangene alte Zeiten von Herzen gefreut; nehmen Sie meinen besten Dank dafür. ... Wie schön, dass Sie jetzt wieder Algebra und*

He also expressed his best wishes toward Jack Todd, and seemed concerned about possibly having lost the latter's esteem, perhaps through his involvement in the German war effort, although his language was cryptic:

> Again heartfelt thanks and friendly greetings, also to your husband, who hopefully out of the rumours in the time of our deepest misfortune has not formed an altogether disagreeable impression of me. [10]

In fact, at least as late as 1963, some mathematicians expressed animosity toward Hasse, refusing to attend his memorial talk for Emil Artin at the number theory conference in Boulder, Colorado of that year, "because of [Hasse's] cooperation with the Nazis while he was head of the Mathematics Institute in Göttingen". Taussky, however, who was at the conference in Boulder, did attend Hasse's talk. (Schneider 1998, p. 18) It is even related in (Rohrbach 1998, p. 12) that during the conference, on 25 August, the day of Hasse's 65th birthday, Jack and Olga treated Hasse to a picnic at the Boulder Canyon.

There came next a letter from Taussky to Hasse, but with no date. It was a short handwritten note, on a small slip of University of London, King's College letterhead – Jack Todd's college at the University – though there was a strike through the letter head. It was written by Taussky, and in German. Right at the end however, after Taussky signed, was added simply, "All good wishes. John Todd."

5.2 Number theory on the computer in the early 1950s

From this point onward, while all letters from Hasse remained in German, Taussky's letters were in English, which, as she explained to Hasse, was so that she could have her letters typed. She was now at the NBS in Washington.

Between late 1949 and early 1955, their letters were focused on the topic of number theoretic computation on NBS machines. They moved on to other topics after this time; in addition, from 1949 to 1950 they were concerned with the obituary of Arnold Scholz, Taussky's collaborator from the 1930s, who died in February 1942. Scholz's sister had

---

Zahlentheorie arbeiten können. Auch ich war so froh, als ich mich 1945 wieder diesen "reinen" Dingen zuwenden konnte.

[10] *Nochmals herzlichen Dank und freundliche Grüsse, auch an Ihren Mann, der hoffentlich aus der Unterredung in der Zeit unseres tiefsten Unglücks keinen allzu ungünstigen Eindruck von mir mitgenommen hat.*

contacted Hasse seeking a proper handling of her brother's mathematical *Nachlass*, and in response Hasse asked Taussky to write Scholz's obituary, and even asked her whether she could complete an unfinished article Scholz had begun for a mathematical encyclopedia.

Regarding number theoretic computation on NBS machines, there was in particular a job related to Fermat's last theorem which Hasse asked Taussky to run, and we learn a lot about the practicalities of such research in this era by reading their letters. Also, there was discussion about potential computational jobs relating to class numbers, but unfortunately several letters are missing, and we do not get to see exactly what was discussed.

Taussky's first letter to Hasse after her move to the NBS was dated 5 December 1949. Hasse had mailed her a month or so earlier, evidently describing a computation he hoped she could run, although the letter is missing. Through the letters that we do have, we are able to reconstruct at least some image of what the computation involved, and this will emerge gradually through the excerpts that we examine below. After responding on a few other matters, Taussky addressed the computation ideas:

> ...
>
> Now the longer questions; I have not had time so far to study your proof sheets from the point of view of high-speed computing machinery, but I have been thinking seriously of tackling your other problem arising out of the Fermat conjecture. I would like to do it, but have to put more thoughts into it, as the domain $\ell < 100$ is far too large for the machinery which I have at my disposal here unless I can think of some trick for abbreviating the work. This I am doing now in conjunction with looking for more extensive tables than the canon arithmeticus. There are some useful tables mentioned in Lehmer's book. I hope to write to you again soon about my success in this matter, but would like to know in any case what smaller domain would still appear useful to you. By about spring time I hope to have available an electronic machine when this problem could be dealt with easily, I think.
>
> ...

Already we see how practical considerations of computing time could bear on the work, and how one might rely on existing tables, be they Jacobi's very old *Canon Arithmeticus*

(Jacobi 1839a), filled with the powers of primitive roots mod primes and powers of primes less than 1000, or any other work named in "Lehmer's book", by which Taussky must surely have meant his *Guide to Tables* (Lehmer 1941).

Beyond this, Taussky mentioned a few other things of interest to us. She thanked Hasse for proof sheets of his article which she referred to as "Arithmetische Bestimmung..." and which must have been *"Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern"* [11], which was published shortly thereafter, in 1950.

This is a larger work of Hasse's, at 95 pages, and was closely allied with KAZ. The two deal with similar problems of computing class numbers, and Hasse would apply methods from both works in his computational investigations in (Hasse 1964), which we will consider closely in Section 6.3. In his 1962 survey of early work in computational algebraic number theory (Cohn 1962), Harvey Cohn's remarks would suggest the importance of (Hasse 1950a) to people working in the field at that time. Namely, in reference to Reuschle's tables (Reuschle 1875), Cohn wrote,

> Yet no progress has been made since 1875, [12] although a general revival of computational interest seems clear from current literature [16].

and his endnote [16] read,

> For many illustrations of modern advanced computational techniques, see H. Hasse, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, *Abh. Deutsch. Akad. Wiss. Berlin. Math.-Nat. Kl.*, 1950.

It would seem that the reference was to this work, (Hasse 1950a), when Taussky wrote, "I have not had time so far to study your proof sheets from the point of view of high-speed computing machinery," suggesting that already at this time Hasse had expressed a hope to do some kind of machine computation on a problem handled in this manuscript, or anyway related to the results therein. Unfortunately, from Taussky's vague remark we cannot tell which problem or problems he had in mind in particular.

---

[11] "Arithmetic Determination of Fundamental Unit and Class Number in cyclic cubic and biquadratic Number Fields" (Hasse 1950a).

[12] I.e., since the work of Reuschle.

Finally, the letter shows that Hasse had asked whether Taussky owned a copy of Weyl's number theory (Weyl 1940), to which she replied that she was unable to locate one. Later, in a letter from November 1950, we see that Hasse sent her a copy of the book. Evidently, he felt it was something that she should read. We recall the significance of Weyl's book, as we considered it in Section 4.3.

Hasse's reply to Taussky's letter was written just six days later, on 11 December 1949:

> ...
>
> It is very kind of you that you will follow up on my suggestion on the tables for the Fermat conjecture. I have also become clear in the meanwhile that with ordinary computing machinery one cannot deal with the entire domain of prime numbers ℓ under 100. If already in spring you will have an electronic machine at hand, it is hardly worth your while to tackle a smaller domain until then with ordinary machines. In any case I am set at ease by your assurance that with the electronic machines it ''could be dealt with easily''. I therefore await your further communications on this with anticipation. This matter is somewhat close to my heart. [13]
>
> ...

The next letter from Taussky was dated 17 Mar 1950. She mentioned a letter of Hasse from 15 February, but it is not present in the *Nachlass*. On the computations, she wrote the following. Her remarks are hard to follow, insofar as we have missed the original description of the problem, but the nature of the problem comes to greater light as the letters proceed.

> ...
>
> I had just meant to write to you anyhow. I hope that your numerical problem will soon be tackled now, but it is a time-consuming problem

[13] *Es ist sehr nett von Ihnen dass Sie meiner Anregung über die Tabellen zur Fermatschen Vermutung nachgehen wollen. Mir ist auch inzwischen klar geworden, dass man mit gewöhnlichen Rechenmaschinen den Bereich der Primzahlen l unter 100 nicht wird erledigen können. Wenn Sie nun schon im nächsten Frühjahr Elektronenmaschinen zur Hand haben werden lohnt es sich wohl kaum, bis dahin noch mit den gewöhnlichen Maschinen einen kleineren Bereich in Angriff zu nehmen. Jedenfalls beruhigt mich Ihre Versicherung, dass es mit den Elektronenmaschinen* "could be dealt with easily". *Ich sehe dann also Ihren weiteren Mitteilungen hierüber mit Erwartung entgegen. Die Sache liegt mir einigermassen am Herzen.*

> even for a very fast machine. Since it involves such very straightforward computation it is not easy to simplify when ‘‘putting it on the machine.’’ I intend to instruct the machine to stop working on a number p if one of the 2 conditions you mention is not fulfilled. This will save a little time. Would it be alright for your purposes if I also arranged that the machine stops to work on a number ℓ if a p is found which satisfies both a) and b)? After all, you only want to know that at least one such p exists, you don't really need to know all of them. Let me know about this as soon as possible, please.
>
> ...

She also mentioned that she was working on the Scholz obituary, and she was thankful that she had been asked to complete Scholz's incomplete encyclopedia article, but wanted to see the existing part to decide whether she felt competent to complete it. Also she was worried about having enough time: "I am very busy in my present job as consultant– although I enjoy it tremendously."

Hasse replied eight days later, on 25 March 1950:

> It cheers me greatly to hear that it will now soon be my number theoretic problem's turn. However your proposal to stop the machine as soon as it has found a p with the two properties a) and b) would compromise the value of the results materially. For a basis for the conjectural frequency of occurrence of these p ought to be gained. Unless it causes more trouble, I would therefore be thankful if from the beginning this wider scope be planned, if need be under sacrifice of the extent of the range of the prime number ℓ to be studied. [14]
>
> ...

Around this time the NBS sent the Todds to visit the Los Angeles branch, and Taussky

[14] *Es freut mich sehr zu hören, dass meine zahlentheoretische Aufgabe nun bald dran ist. Allerdings würde Ihr Vorschlag, die Maschine stoppen zulassen, sobald sie ein p mit den beiden Eigenschaften a) und b) gefunden hat, den Wert der Ergebnisse erheblich beeinträchtigen. Denn es soll ja gerade eine Grundlage über die vermutliche Häufigkeit des Auftretens dieser p gewonnen werden. Selbst wenn es mehr Mühe macht, wäre ich doch denkbar, wenn von vornherein dieser weitere Rahmen zugrundegelegt würde, nötigenfalls unter Opfer des Umfangs der zu bearbeitenden Primzahlen ℓ.*

found time to reply to Hasse on 28 June 1950, writing on letterhead from the NBS's Institute for Numerical Analysis at UCLA.

> Dear Professor Hasse,
>
> Your letter of March 25 reached me a long time ago. I delayed answering until I had some mathematical news to tell you. Unfortunately, this is not yet the case. Your problem has been prepared for the high speed machine, but in the mean time we were sent to visit the Institute in Los Angeles. I had hoped that work on the problem might be carried out in my absence, but I have heard nothing about it. I shall try to speed things up when I return to Washington.
>
> I was also too busy with other work to study Scholz' manuscript sufficiently to come to a decision regarding ability to complete it.
>
> I am really only writing to apologize for all the delays. I have still not completed the Scholz obituary notice, but I have now received all information about his personal life from his sister.
>
> With best regards, also to your family, from both of us.
>
> Yours sincerely,
>
> Olga T. Todd

She wrote again on 21 November 1950, thanking him for the copy of Weyl's number theory which he had sent in the meanwhile, and also reporting some results. Here we see again an example of real use of the kind of tables which were the subject of Lehmer's *Guide*, and of the "Mathematical Tables" journal. We also see the real limitations of those tables:

> ...
>
> I have been very busy and have not been able to do much concerning the jobs I promised you. Only for the Fermat problem a little progress can be reported. The problem has been set up for the big machine (I had the help of Dr. J.C.P. Miller from England for it) and correct results are coming out. However, I based the computation on the knowledge of a primitive root and tables for these exist only up to $p = 25000$. I could send you results for all $\ell < 100$ and $p < 25000$, but for larger p

> we shall have to wait and compute the primitive roots first which is not too difficult since usually very small ones can be found.
>
> ...

Where Taussky mentioned the "jobs," plural, that she had promised, and wrote that, "Only for the Fermat problem a little progress can be reported," it sounds as though she and Hasse had discussed *several* problems for which they would like to run jobs on the NBS machine. For while she also had the tasks of the Scholz obituary and encyclopedia article before her, it seems a bit odd to refer to these as "jobs", in the same context as the computing job that she was discussing. Moreover, in her previous letter she made no "promise" regarding Scholz, but on the contrary had not yet come to a decision. All this makes it appear that by this time Hasse and Taussky were already discussing more computing problems than just the Fermat one.

A week later, on 28 November 1950, Hasse replied:

> You have my heartfelt thanks for your friendly letter with the beautiful news that already results are there for the question on the Fermat-Problem. I am very curious about it, and would be very thankful to you, if you could send me the results for all $\ell < 100$ and $p < 25000$, if it causes you no great trouble. [15]
>
> ...

and he went on to discuss other matters.

Taussky replied on 15 December 1950:

> Best thanks for your letter. I am sending you herewith the results you wanted as far as we have computed them. I hope they are correct. They have not been checked so far and I must point out above all, that consecutive residues $> 10,000$ have been ignored by the machine so far, so that some of the exceptional larger p's may have to be omitted. We are computing primitive roots in the meantime.

[15] *Haben Sie recht herzlichen Dank für Ihren freundlichen Brief mit der schönen Nachricht, dass bereits Ergebnisse zu der Frage über das Fermat-Problem vorliegen. Ich bin sehr gespannt darauf und wäre Ihnen sehr dankbar, wenn Sie mir die Resultate für alle* $\ell < 100$ *und* $p < 25000$ *schon jetzt zusenden könnten, sofern Ihnen das keine grosse Mühe macht.*

with a handwritten postscript:

> p.s. The work for $\ell = 13$ is incomplete so far.

Next came another letter from Taussky, dated 26 January 1951. She thanked Hasse for a letter of 24 January, but unfortunately it, along with every other letter from Hasse to Taussky written in 1951, is absent from the *Nachlass*.

In this letter, Taussky described in detail the meaning of the entries in a table of computed results which she would soon send to Hasse. While we cannot see the letter from Hasse in which he originally described the problem, here we get some valuable hints as to what exactly the problem was. For one thing, Taussky wrote that the tables concerned "the Legendre-Sophie Germain criterion". Furthermore, her description of the table gives us some idea of what was being computed:

> Best thanks for your letter of January 24. I can give you more detailed tables concerning the Legendre-Sophie Germain criterion. In fact I shall send you very soon a microfilm with the complete results. You can read it with a magnifying glass, unless you have a projector. This table is to be understood as follows: The first entry on the left is ℓ, the second is p, the third is either (1) a blank or (2) one member of the first pair of consecutive ℓ-th power residues -- if there is such a pair -- or (3) the number ℓ if it is an ℓ-th power residuum; in this case the number p is also tested for consecutive ℓ-th power residues in the next line. In the case (3) the number p therefore is treated twice, e.g., $\ell = 17, p = 6257$. What I had called ''exceptional'' p's in my previous communication were the p's for which blanks turn up.
>
> The fourth entry gives the index of the number in the third entry with respect to the primitive root and is therefore not of interest to you. Altogether we arranged for the machine to print so many details in order to make occasional checks.

Although it is now mostly clear what the computations must have been, we will wait to spell out our best guess until we have considered one more letter from Taussky, in which she will clarify a couple more details.

As for what it might have been that was referred to as "the Legendre-Sophie Germain criterion", one candidate certainly presents itself. Let us recall that, traditionally, efforts to prove Fermat's last theorem, i.e. the statement that for $n \geq 3$ there are no solutions in positive integers to the equation $x^n + y^n = z^n$, were first reduced to the case in which n was a prime p, and secondly were split into "Case I", in which the exponent p did not divide xyz, and "Case II", in which it did.

In these terms, Sophie Germain (1776-1831) proved in 1823 that if both p and $2p + 1$ are prime, then Case I of Fermat's last theorem is true for the exponent p. A.M. Legendre (1752-1833) extended the result to say that instead of merely considering $2p + 1$, one could consider $cp+1$ for any $c = 2, 4, 8, 10, 14, 16$; he showed that if *any* of these numbers is prime, then Case I is true for exponent p. (Kleiner 2012, p. 49)

If indeed this is the criterion that Hasse and Taussky were working on, then it would seem that their efforts were directed at nothing so obvious as simply checking for many values of p whether any of the permitted $cp + 1$ were also prime. This alone would not explain the table that Taussky described.

Since the last letter we have considered was from January 1951, it should be noted at this point that in late 1950 and early 1951 Taussky was busy organizing and participating in a symposium as a part of the semicentennial celebration of the National Bureau of Standards, for which she, "contributed number theory problems (and their solutions) for the computers" (Luchins and McLoughlin 1996). Bauer has even written (Bauer 1998) that this was "the first symposium on Numerical Algebra". Facts such as these help to demonstrate the leading role played by Taussky in the earliest days of number theory and algebra on electronic computers. They also explain a bit more about what kept her so busy in these days.

A letter next came from Taussky on 22 June 1951, this time giving a clear indication of just how unfortunately "low priority" number theory jobs were on the machines she had at her disposal:

> ...
>
> The background theory concerning my previous computation is, of course, extremely interesting, but I am rather pessimistic about the range of work you are now asking for. In our absence at Los Angeles no work was carried out; when we returned we asked to resume the primitive root

> calculations. We are still very much interested in number-theoretical problems, even if we have to wait for spare moments to put them on.
>
> However, it takes long enough to compute primitive roots and your problem seems to need them for all known prime numbers. Further, you want the precise number of pairs of consecutive residues. That is a lot more than originally required. How can we obtain this number without testing all (or at least more than half the residues)?
>
> Actually, your original inquiry concerned _only_ those prime numbers p for which the machine printed nothing at all. I must admit that originally I tried to arrange the work so that the machine would only print these numbers. Later, it was decided to print out more, for checking purposes mainly. To investigate consecutive residues for those p which had ℓ as an ℓ-th power residue was already a ''Fleissaufgabe;'' [16] but to investigate ℓ for those p which had a pair of consecutive residues is much more work so we did not do it.
>
> Of course, we can investigate all 4 possibilities, but this is already a lot more work even for the range covered up to now.
>
> I wonder if you could make any suggestions how to abbreviate the length of the computations or otherwise suggest what portion of information would still be useful to you. $\ell = 60$ seems already out of the question. I know that this will disappoint you, and I am very sorry about it.

At this point Taussky switched topic. She had opened the letter by thanking Hasse, "for your very interesting letter" (which, again, we do not have). Apart from the "background theory" on Taussky's previous computation, which she called "extremely interesting" above, she was also interested in some other problems which Hasse had begun to discuss, in algebraic number theory. She proceeded,

> I am very interested in your problems in algebraic number theory. I have just been considering starting the machine on class numbers.

[16] I.e. a problem that would require great diligence or industriousness.

> The problem your friend is interested in is rather attractive too; I am glad we could help him a little, even if the result was disappointing.
>
> A young man who is employed here as an engineer to look after the machine but who has great interest in number theory has computed the 3rd Wilson prime, i.e., $p^2 \mid [(p-1)! + 1]$; it is 563. There is no other up to 10,000. The two other ones are 5, 13.
>
> [signs off]
>
> P. S.
>
> When reading through this letter again I feel you may think me uncooperative regarding your problem of whose importance you have certainly convinced me. This is not the case. The trouble is that this particular problem necessitates an unusual expenditure of time (= money). Apart from the mathematicians' time the current expense of running the machine is \$1 per _minute_. [17]

Where Taussky referred to, "your problems in algebraic number theory" it sounds as though she was using the modifier "algebraic" to make a contrast with the work they had been doing up to this point. On the one hand, this seems odd given the place of Fermat's last theorem, at least as a motivator, in the history of algebraic number theory. On the other hand, in light of the focus on class numbers and fundamental units in the problems that Hasse and Taussky would discuss in later letters (to be reviewed below), we find a way to understand such a distinction: Algebraic number theory was a *tool* that was applied to the elementary number theoretic problem of Fermat's last theorem; class numbers and fundamental units, however, are innately algebraic number theoretic objects. In attempting to compute these, one would be directly addressing the sort of computational program that Hasse envisioned in KAZ. As would be revealed in the survey she presented in 1953, and which we consider in depth in Section 5.3, Taussky shared a vision with Hasse of a field of research defined specifically by the computation of the objects associated with algebraic number fields. Perhaps the interesting "problems in algebraic number theory" that Hasse had mentioned in his prior letter belonged to this domain, especially considering Taussky's

[17] In 2012 dollars, this would be roughly \$500 per hour.

subsequent remark, that she had, "just been considering starting the machine on class numbers."

In any case, it is now an appropriate point at which to piece together the information we have about the computations on the Fermat problem. Altogether, the following seems to be the most likely reconstruction of the task: For each prime $\ell < 100$, consider all primes $p < 25000$ for which ℓ divides $p-1$ (so that ℓ^{th} power residues mod p are interesting, *every* residue mod p being an ℓ^{th} power otherwise). For each such p, determine (a) whether ℓ is an ℓ^{th} power mod p, and/or (b) whether there exist any consecutive residues c, $c+1$ mod p both of which are ℓ^{th} powers mod p. A prime p is called "exceptional" with respect to ℓ if neither of the two conditions (a), (b) is satisfied.

The most obvious way to handle this task is to obtain for each prime p a primitive residue r, so that the ℓ^{th} powers mod p are precisely the $r^{a\ell}$ mod p for $a = 1, 2, \ldots, (p-1)/\ell$, and indeed, Taussky wrote in the letter of 21 November 1950 that she, "based the computation on the knowledge of a primitive root". She had found tables of these for p up to 25000, and when she later began setting the computer to find primitive residues for $p > 25000$, this evidently was by brute force search, since she wrote that the problem was "not too difficult since usually very small ones can be found".

In this case, the table Taussky described in the letter of 26 January 1951, would have been for $\ell = 79$ as in Table 5.1, provided she used the primitive root 3 mod 79 as we have done here. (The one named in the *Canon Arithmeticus* is 29.) We have also added "***" on those lines on which ℓ was found to be an ℓ^{th} power mod p.

While we have chosen to show the table here for $\ell = 79$ since it is short enough to fit on a page (there are only 36 primes $p < 25000$ for which 79 divides $p-1$), this example is not indicative of the fact that the "exceptional" primes, i.e. those for which nothing is printed in the third column, do in general merit their name: for smaller values of ℓ only a few p are exceptional, and these are always among the smallest p. For example, for $\ell = 3$ only $p = 7, 13$ out of 1371 primes are exceptional; for $\ell = 5$ only $p = 11, 41, 71, 101$ out of 689 primes; for $\ell = 7$ only $p = 29, 71, 113, 491$ out of 452 primes.

On modern equipment (2.4 GHz processor, 12 GB RAM), coding the task in the most simple-minded way, the entire problem for all $\ell < 100$ and $p < 25000$ was completed on the MAPLE 15 computer algebra system in under 65 seconds. The code that we used is reproduced in Appendix C.

How the data on these tables were to serve Hasse and Taussky in discovering something

ℓ	p	result	index	
79	317			
79	1423	643	948	
79	2213			
79	2371	464	790	
79	2687			
79	3319	1527	1106	
79	3793	1068	1264	
79	4583			
79	5531	550	4898	
79	5689	528	1027	
79	6163	79	5135	***
79	6163	78	4108	
79	6637	1370	4424	
79	7901			
79	8059	2765	5372	
79	8849			
79	9007	1094	6004	
79	9323			
79	10271			
79	10429	79	8848	***
79	10429	2414	3476	
79	10903	478	3634	
79	12641	486	3397	
79	12799	2418	4266	
79	14221	4845	9480	
79	14537			
79	15643	398	474	
79	15959			
79	16433			
79	17539	1	0	
79	18013	2328	12008	
79	18329	5395	12482	
79	18803	1919	3002	
79	19751	79	4661	***
79	20857	1	0	
79	21647			
79	22279	5502	10270	
79	23227	549	15484	

Table 5.1: Data pertaining to the Legendre-Sophie-Germain criterion for $\ell = 79$, following Hasse and Taussky, using primitive root 3 mod 79.

about the Legendre-Sophie-Germain criterion remains a mystery.

In Taussky's next letter, written 30 November 1951, she thanked Hasse for a letter of 5 November, and wrote:

> ...
>
> I am sorry that I did not reply to your earlier letter. The main reason is that I have no progress to report at all. Our machine has been overloaded with work although it is kept going continuously day and night -- apart from repair and testing intervals. People come from universities and research centers far away to run their problems on the machine and, of course, pay for the services -- so I have to wait. We hope to have another machine available in the not too distant future.
>
> Nevertheless I would be very glad to hear what routine problems you propose in connection with class numbers and units. It is necessary to think these problems out a long time before coding them for the machine.
>
> ...

This truly gives us a picture of the scarcity of machines, and the interest shown in them by researchers in general, in late 1951. Also, again Hasse seems to have at least mentioned potential computing jobs on class numbers and units, if not yet described them in detail, and Taussky continued to express keen interest in them.

We find a little insight into the nature of the work on class numbers and units which Hasse had mentioned, in the next letter we have from him, dated 22 January 1952. He speaks of a letter from Taussky sent on 31 December 1951, but it is not present in the *Nachlass*. Hasse wrote,

> I bid you excuse me that I only today answer your friendly letter of 31.12. The reason for this delay lies in the next to last paragraph of your letter, in which you asked which routine problems I can propose in connection with class numbers and units.
>
> Matters now stand so that the works of my student Leopoldt in this realm have not yet reached _the_ conclusion, which is necessary for

> the tackling of numerical calculation. For the computation of the fundamental units of an arbitrary Abelian number field we have up to now been able to develop no useable general algorithm. My purpose, to allow the calculation of class number tables for absolute Abelian number fields, stands or falls with the development of such an algorithm. Perhaps we will be there in a year. Today I can only propose to undertake the cyclic cubic and eventually also the cyclic biquadratic number fields. For these I have in my work, ''Arithmetische Bestimmung von Grundeinheit und Klassenzahl'' in the Abhandlungen der Deutschen Akademie der Wissenschaften, Jahrg.1948,2 appearing 1950, calculated fundamental unit and class number for all conductors under 100. In this work are also elaborate specifications as to how the calculation is to be set about. A look at the tables there on pages 91 - 94 shows that in this realm only trivial class numbers arise. I hold very desirable the extension of these tables to higher conductors, let us say at first to 200, or if the machine allows it, even farther. [18]

Here then was a very clear statement as to Hasse's purposes. He wanted to make possible the computation of class number tables for absolute Abelian number fields. As a prerequisite for this he needed to be able to compute fundamental units of an arbitrary Abelian number field, and he had his student H.W. Leopoldt working on this.

There came next a break of five months, and then on 25 July 1952 Taussky wrote to

[18] *Entschuldigen Sie bitte, dass ich Ihren freundlichen Brief vom 31.12. erst heute beantworte. Der Grund für diese Verzögerung liegt im zweitletzen Absatz Ihres Briefes, in dem Sie fragten, welche Routineprobleme ich im Zusammenhang mit Klassenzahl u.Einheiten vorschlagen könne.*

Die Sache liegt nun so, dass die Arbeiten meines Schülers Leopoldt auf diesem Gebiet doch noch nicht _den_ Abschluss erreicht haben, der zur Inangriffnahme numerischer Rechnungen erforderlich ist. Für die Berechnung der Grundeinheiten eines beliebigen abelschen Zahlkörpers haben wir bisher kein brauchbares allgemeines Verfahren entwickeln können. Meine Absicht, Klassenzahl-Tafeln für absolut abelsche Zahlkörper rechnen zu lassen, steht und fällt mit der Entwicklung eines solchen Verfahrens. Vielleicht sind wir in einem Jahr damit schon weiter. Heute kann ich nur vorschlagen, die zyklisch kubischen und ev.auch die zyklisch biquadratischen Zahlkörper vorzunehmen. Für diese habe ich in meiner Arbeit "Arithmetische Bestimmung von Grundeinheit und Klassenzahl" aus den Abhandlungen der Deutschen Akademie der Wissenschaften, Jahrg.1948,2 erschienen 1950, Grundeinheit und Klassenzahl für alle Führer unter 100 ausgerechnet. In dieser Arbeit finden sich auch ausführliche Angaben, wie die Rechnung anzusetzen ist. Ein Blick auf die dortigen Tabellen S.91-94 zeigt, dass in diesem Bereich nur triviale Klassenzahlen vorkommen. Ich halte eine Ausdehnung dieser Tabellen auf höhere Führer, sagen wir zunächst einmal bis 200, oder wenn die Maschine es zulässt, auch weiter, für sehr erwünscht.

mention a few things, among them thanks for a copy of KAZ which Hasse had sent her. We note that the book was published in the same year, so it appears that Hasse wasted little time in sending Taussky a copy. She seems to have valued it highly, and as we will see in Section 5.4, her praise of the book was not empty talk: Taussky actually made use of the book, even at a remove of twelve years, as a letter of 1964 will show. At time of receipt she wrote:

> ...
>
> Your book on the class numbers just arrived and I am writing to thank you very much for sending it. This certainly is a most valuable book to own.
>
> I am sorry I did not write for quite a long time. I have not done any work at all in connection with our machine as it was being used by others. It is, however, becoming freer now and I hope to use it for number theory again soon. I shall communicate to you if I have any success.
>
> ...

Hasse's reply, written just four days later on 29 July 1952, showed that in fact the computations Taussky referred to were, finally, on class numbers. Among other things, he wrote:

> ...
>
> It would be very nice if you could soon address the planned class number calculation for Abelian number fields. I am at any time ready to advise you in detail. [19]
>
> ...

Once again, it does sound as though at this time it was only through Taussky that Hasse had access to a machine. At least, the level of interest he displayed in these computational problems suggests that if he had had his own machine available he would simply have used

[19] *Es wäre sehr schön, wenn Sie bald an die geplanten Klassenzahlrechnungen für abelsche Zahlkörper herangehen könnten. Ich bin jederzeit bereit Sie im Detail zu beraten.*

it. This accords with what we know of the state of technology in the early 1950s, when still just a few machines were available anywhere in the world, and Zuse would not make vacuum-tube-based machines available in Germany until 1958 (cf. p. 143).

From the correspondence present in the *Nachlass* it is not clear whether the class number calculations were ever actually carried out. There came next a gap of about a year and a half, and the next letter we have is from Taussky, writing on 23 November 1953. As for the Fermat problem, it would not be discussed again until July 1954, as we will review below. At that time, Taussky would write only to mention an interaction with Vandiver on Fermat, and she would recall to Hasse their own collaboration as work "which we had to abandon a few years ago because of the expense".

Over the summer of 1953, Taussky had presented a talk entitled "Some Computational Problems in Algebraic Number Theory" at the Sixth Symposium in Applied Mathematics of the American Mathematical Society, held at the Santa Monica City College, August 26 - 28, and cosponsored by the National Bureau of Standards, where Taussky was still employed. We take an in depth look at her talk in Section 5.3. In her letter of 23 November 1953, she enclosed a copy of the talk, and asked Hasse's opinion of it:

> Dear Professor Hasse,
>
> I am sending you enclosed the manuscript of a lecture I gave last summer. It is to be published. If you can spare the time to read it I would be most grateful for your comments. The lecture was to report mainly on recent work and on my own work, so it was rather difficult!
>
> I hope you and your family are all flourishing.
>
> With kind regards from both of us.
>
> Sincerely yours,
>
> Olga T. Todd

In his reply two weeks later on 8 December 1953, Hasse expressed a favourable impression. He opened,

> With great interest I have read your report on selected computational problems in algebraic number theory. You have really brought it together very nicely. I have actually only very small factual remarks

to make. [20]

It sounds thus as though Hasse approved quite highly of the picture Taussky painted of the field of computational algebraic number theory, naming no areas of research which he felt she had omitted, nor any she included which he felt did not belong. This is an important point for us to notice. Questions of the transmission of certain points of view about what sorts of mathematical activities were valuable are very much the same as questions of the extent to which various mathematicians shared common inner visions as to which questions, problems, and methods various fields of research consisted of. If Hasse agreed with Taussky's idea of what belonged to this field of research, then it would seem that they believed the same sorts of research to be important, at least within this field.

Something of Hasse's meticulousness, and his art for mathematical presentation, comes through in the comments that he did make about Taussky's survey. For one,

> When you at the end of this section write that the analytic class number formula is indeed complicated but yet very useful, one wonders what indeed the use is.

at which point he went on to suggest what he thought she probably had in mind. At another point he wrote,

> On page 7 at the end of Row 4 I would add a ''probably'' to the categorical Feststellung on Lehmer (24).

and it would seem that this regarded Taussky's mention of Lehmer's 1933 work on the class number 1 problem using the photo-electric number sieve, which we discussed in Section 4.1. In the final edition of the talk, she wrote:

> ... for $m > 163$ at most one further m is possible such that the field $F(\sqrt{m})$ has class number unity. It is still an open question whether there is a further m. Work by Lehmer [26] indicates that probably no further m exists.

That Hasse insisted on the use of "probably" shows that he was careful about what claims one could make on the basis of numerical evidence.

---

[20] *Mit grossem Interesse habe ich Ihren Bericht über einige Rechenprobleme in der algebraischen Zahlentheorie gelesen. Sie haben das wirklich sehr schön zusammengestellt. Ich habe eigentlich nur ganz kleine sachliche Bemerkungen dazu zu machen.*

In closing his reply to Taussky, Hasse brought up recent work of Redei on the problem of the structure of the 2-power class group of a quadratic number field, and the necessary and sufficient conditions for the Norm -1 of the fundamental unit. He asked whether she had read it. We note that while the work of Redei was not among those originally named in the bibliography to Taussky's 1953 talk, she did add it before the 1956 publication of the Symposium proceedings.

In another letter several months later, dated 4 May 1954, Hasse wrote solely to urge Taussky to consider the work of Redei, and in particular to consider carrying out computational work on the basis of it. This letter is gratifying in our search for evidence of any influence Hasse may have had, or may have tried to have, on Taussky's selection of problems. As we seek signs of continuity in the computational tradition in algebraic number theory, really one of the strongest forms of evidence we can find is written documentation of one mathematician naming for another some problems which he or she thought were worth working on, and suggesting that the other do so. In the letter of 4 May, we find Hasse making just such statements:

> Certainly you too will have noticed the two very beautiful works of L. Redei in the Acta math.scient.Hungar.4 (1953), in which the questions of the 2-power invariants of the class group of quadratic number fields, and of the solvability of the Pell equation with -1 finally are solved. In reading through these works, a point on p. 39 attracted my attention, where Redei says that with his methods one could compute a solvability table of this Pell equation up to 100,000, whereas the Patz table appearing some time ago goes only to 10,000. Since you are always on the lookout for new potential activities for the electronic computing machine, I would permit myself to make you aware of this point. By his remarks, Redei has certainly not thought of an electronic computing machine, but rather of computation of an earlier kind. For an electronic computing machine the computation up to 100,000 must by my estimate be a mere bagatelle. On the other hand, it would be very interesting to carry it out and publish, since it is indeed concerned with a question which is of fundamental significance, and stands in close relation to other phenomena in quadratic

number fields. Perhaps you could investigate anyway, whether on the basis of the two works of Redei one could not for all the questions I - IV considered by Redei construct with relatively little trouble a table in the range up to $100,000$. [21]

Two months later, Taussky's reply did not address the matter of Redei. She wrote instead, on 7 July 1954, to tell Hasse of her recent interaction with Vandiver, in connection with the Fermat problem.

...

Recently my attention was turned again to the study of consecutive ℓ-th power residues, the study of which we had to abandon a few years ago because of the expense. This time it was through Vandiver who had heard from E. Lehmer about the computations I made for you. Vandiver wants me to study the primes p such that

$$ax^n + by^n + 1 \equiv 0 \mod p$$

has no solutions.

It seems that the computations we made here contradict an unpublished table by Beeger, see Vandiver's article on the Fermat problem in the Amer. Math. Monthly, 1946, p. 565, Theorem VII.

I told Vandiver that I made the computations at your suggestion, but gave no further details.

...

[21] *Sicher werden Sie auch die sehr schönen beiden Arbeiten von L.Redei in den Acta math.scient.Hungar.4 (1953) bemerkt haben, in denen die Fragen nach den 2-Potenzinvarianten der Klassengruppen quadratischer Zahlkörper und nach der Lösbarkeit der Pellschen Gleichung mit -1 endgültig gelöst werden. Beim Durchlesen dieser Arbeiten fiel mir nun eine Stelle auf S.39 auf, wo Redei sagt, dass man mit seinen Methoden leicht eine Lösbarkeitstafel dieser Pellschen Gleichung bis zu 100.000 berechnen könne, während die vor einiger Zeit erschienene Patzsche Tafel doch nur bis 10.000 geht. Da Sie immer auf Ausschau nach neuen Betätigungsmöglichkeiten der Elektronenrechenmaschine sind, wollte ich mir erlauben Sie auf diese Stelle hinzuweisen. Redei hat bei seiner Bemerkung sicherlich nicht an eine Elektronenrechenmaschine gedacht, sondern an Rechnen früherer Art. Für eine Elektronenrechenmaschine müsste aber meiner Schätzung nach die Rechnung bis 100.000 eigentlich nur eine Bagatelle sein. Andererseits wäre es doch sehr interessant, sie wirklich durchzuführen und zu veröffentlichen, weil es sich ja um eine Frage handelt, die von grundsätzlicher Bedeutung ist und zu anderen Erscheinungen im quadratischen Zahlkörper in enger Beziehung steht. Vielleicht sehen Sie sich überhaupt die beiden Redeischen Arbeiten einmal daraufhin an, ob man nicht sogar für die sämtlichen von Redei behandelten Fragen I-IV mit verhältnismässig geringer Mühe eine Tafel im Zahlraum bis 100.000 herstellen könnte.*

She spoke also of a rumour of progress on the Fermat problem in Japan. In his response of 13 July 1954, besides responding to Taussky's main points, Hasse also again urged the work on Redei's ideas:

> ...
> [The works of Redei] are really very interesting, and I think as well that they would give occasion for numerical researches.
>
> I will also obtain the works of Lehmer and Vandiver on the Fermat problem. As for what the rumour from Japan concerns, I can tell you a bit more. At the moment we have Mr. Kuroda here. He recounted just upon his arrival, that his friend Morishima held a lecture in the Tokyo Academy, in which he proved that the first class number factor (real subfield) is not divisible by the prime number, from which then the correctness of the Fermat conjecture would follow. Kuroda himself is very sceptical whether this proof is actually sound. He has not yet presented a precise version, as Morishima wants to revise his manuscript before it goes to press. The lecture itself gave only a short sketch of the proof ideas. Details were not worked through. Thus it remains to wait and see whether the final manuscript of Morishima in preparation will hold water.
>
> It interests me very much, that you are now inspired by Vandiver to computations once again on the problem on which a few years ago you carried out computations on my advice. Anything that you figure out here would very much interest me, in particular more about the contradiction you briefly mentioned between those computations with an unpublished table of Beeger. [22]
> ...

[22] *... [the works of Redei] sind wirklich recht interessant, und ich glaube auch, dass sie Anlass zu numerischen Untersuchungen geben werden.*

Die Arbeiten von Lehmer und Vandiver über das Fermatsche Problem will ich mir gleich beschaffen. Was das Gerücht aus Japan betrifft so kann ich Ihnen etwas Genaueres sagen. Wir haben ja im Augenblick gerade Herrn Kuroda hier. Er erzählte gleich bei seiner Ankunft, sein Freund Morishima habe in der Tokioer Akademie einen Vortrag gehalten, in dem er bewiesen habe, dass der 1.Klassenzahlfaktor (reeller Teilkörper) nicht durch die Primzahl teilbar sei, woraus ja dann die Richtigkeit der Fermatschen Vermutung folgen würde. Kuroda selbst ist sehr skeptisch, ob dieser Beweis wirklich stichhaltig ist. Eine genaue Version hat ihm bisher nicht vorgelegen, denn Morishima wollte sein Manuskript vor dem Druck erst noch überarbeiten. Der Vortrag selbst gab nur eine kurze Skizze des Beweisgedankens. Einzelheiten wurden nicht durchgeführt. So bleibt also abzuwarten, ob das in Vorbereitung befindliche endgültige Manuskript von Morishima hieb-und stichfest ist.

When Taussky wrote back on 1 March 1955, she and Jack were on a year's leave at the AEC (Atomic Energy Commission) Computing Facility at the Courant Institute in New York. Regarding computation, Taussky wrote only a little:

> ...
>
> We arrived here in New York a few weeks ago and are enjoying our stay very much. During my last weeks in Washington I wrote down some first results on the generalized normal basis in algebraic number fields I wrote to you last year about. I hope to send you a copy of the paper soon. I got at last a photocopy of the paper by Redei you kindly told me about, but have not yet had time to dig out the computational problem in it. Also, I think you mentioned that there were two papers on the same subject by Redei in the same number and I have yet to search for the second one, so it all takes a long time.
>
> ...

5.3 A survey talk, 1953

Olga Taussky gave a talk at the Sixth Symposium in Applied Mathematics, entitled "Some Computational Problems in Algebraic Number Theory." The conference took place in 1953, and the theme was Numerical Analysis. As we saw in Section 5.2, Taussky sought Hasse's comments on her talk before sending it to print, in the Proceedings of the Symposium. [23]

Although Taussky's subject might seem to have been out of place given the theme of the Symposium, she was not alone, another talk on number theory having been given by Emma Lehmer, regarding computer investigations recently carried out by herself and D.H. Lehmer on the SWAC. [24] The common element was the involvement of a computer. Numerical analysis was the original application for which computers had been funded during the war, and so in an era in which there might have been few other venues welcoming talks on

---

Es interessiert mich sehr, dass Sie nun von Seiten Vandivers erneut zu Rechnungen über das Problem angeregt wurden, an dem Sie auf meinen Rat vor einigen Jahren Rechnungen ausführen liessen. Alles, was Sie dabei herausbekommen, wird mich sehr interessieren, insbesondere auch Näheres über den von Ihnen angedeuteten Widerspruch Ihrer damaligen Rechnungen mit einer nichtpublizierten Tafel von Beeger.

[23](Taussky 1953)

[24]See Corry (Corry 2008a,b) on the work of the Lehmers.

computer work, the Symposium seems to have been suitable enough. In addition, we may recall that Taussky had close ties to numerical analysis, both through her own involvement in the field during the war, and through her husband Jack Todd, who specialized in the subject. Finally, it seems plausible that the organizers of the conference would have welcomed the chance to promote the involvement of computers in mathematics generally, by inviting talks which demonstrated their applicability to areas of mathematics not immediately associated with physics, engineering, operations research, etc.

Close to ten years later, when Todd edited the volume (Todd 1962) based on a course funded by the National Science Foundation to promote interest in numerical analysis, Taussky's talk was published again, this time appearing, essentially unaltered, as the second half a chapter co-authored with Harvey Cohn and called, simply, "Number Theory".

The title of Taussky's talk was unassuming, in no way purporting to define a field of research, and yet her choice of topics was consistent with (if more limited than) the view of CANT that eventually would emerge through the statements and publications of practitioners like Zassenhaus, Zimmer, Pohst, and Cohen[25]. Whether or not she meant to be definitive, in 1953 her survey made a very early statement as to which problems a computational branch of algebraic number theory could be centred around.

After a brief introduction, she discussed five topics: integral bases, factorization of rational primes in number fields, units, ideal classes and class numbers, and principal idealization, [26] devoting anywhere from a paragraph to a couple of pages to each, in this short talk. While the last of her topics would be presented in Zimmer's definitive survey of computational algebraic number theory in 1972[27] as a somewhat specialized question belonging under his heading of "class numbers and class fields", all five of Taussky's topics do appear in his survey, and the first four are major headings. Zassenhaus too would eventually articulate his four main goals of computing integral bases, groups of units, class groups, and Galois groups, in which there is significant overlap with Taussky's list. As we have seen, Hasse discussed the computation of similar objects in the foreword to KAZ. We thus find a good deal of consistency in the mental images of this field of work held by these participants.

Speaking to an audience likely composed mainly of non-experts in number theory,

[25]Cohen 1993, 2000; Pohst and Zassenhaus 1989; Pohst 1994; Zimmer 1972.

[26]By this phrase Taussky meant the phenomenon of a non-principal ideal in a base field becoming principal in an extension field.

[27]Zimmer 1972.

Taussky opened her talk with a brief statement motivating the study of algebraic number fields itself, the basic idea of which was that many number theoretic theorems for the rational field could be fully understood only in the wider setting of general algebraic number fields. To motivate the *computational* branch in particular, she said that

> Progress in [algebraic number theory] is particularly hindered by the greatly increased difficulties of numerical examples, compared to the rational field.[28]

This, then, was Taussky's stated reason for doing computation in algebraic number theory, in 1953: to produce numerical examples, in service of the advancement of the theory.

Purely chronologically the report seems to be significant, August 1953 appearing quite early both in the electronic computer era, and as regards published statements on the subject of computational algebraic number theory. The Association for Computing Machinery (ACM) had already formed in 1947, but the first issue of its journal did not yet appear until four months after this symposium, in January 1954. Hasse's definitive statement in KAZ had been published the year before, in 1952, but in German and under a title not explicitly indicative of computation.

Regarding table work, Taussky only pointed to Lehmer (Lehmer 1941), and observed that in algebraic number theory, not much had been done. This does not mean however that between 1941 and 1953 no additional table work had appeared. On the contrary, named in (Zimmer 1972) are many works from these years containing small to medium sized tables. In fact we need look no farther than Hasse. The 190-page KAZ ends with 30 pages of tables containing data on all Abelian number fields of conductor at most 100, along with 19 pages of diagrams (the so-called "Hasse diagrams", which Hasse had been using already for 20 years by this time).

Taussky characterized her report as brief, and added that, "only problems concerning the most fundamental concepts are mentioned". By contrast, she added that, "Many other problems have come up," and here cited just one example, the 1953 collaboration of Artin, von Neumann, and Goldstein [29] in which a conjecture of Kummer from 1846 was investigated by computing numerical data on the IAS machine. She did not discuss this work, but merely referred to it in passing. Her point seems to have been that many investigations were being

[28]Taussky 1953, p. 187.

[29]The work (Neumann and Goldstine 1953) is discussed briefly in (Aspray 1990, pp. 160-161) It was published in April of 1953, just four months before the Symposium.

conducted on computers, which did not fit neatly under her main headings for problems in algebraic number theory.

Two matters essential to computational mathematics were confronted by Taussky in her survey, albeit only in passing: (1) the need for rational methods, and (2) the question of the "routineness" of methods, i.e. the extent to which they are generally applicable to a broad class of problems. We consider these themes in some depth now.

5.3.1 Rational methods

In her section on the factorization of rational primes in number fields, Taussky wrote (her emphasis):

> Like many other computations in algebraic number theory, the splitting of rational primes can be treated by *rational* methods only. This fact is very important if computation by automatic computing machinery is considered. Only the knowledge of the irreducible polynomial $f(x)$, a zero of which generates the field in question, is needed. (Taussky 1953, p. 188)

We recall (Section 3.5, p. 101) how she and Scholz had similarly emphasized in 1934 that they would decide "by means of relations in the field of rational numbers" which ideal classes became principal in certain extension fields. In her talk, Taussky recalled her collaboration with Scholz as well, noting that "for this problem also a rational method was found to succeed".

It is not a difficult concept which Taussky was discussing in her survey, but the fact that she needed to point it out tells us something about this moment in time. Even if Taussky's audience contained very few number theorists, still she would speak as if to address the popular, received view of algebraic number theory at the time, a view in which algebraic numbers were entities in their own right. In the computational view, on the other hand, they were to be replaced by their minimal polynomials, or else by other data structures representable on the computer.

In these few words of Taussky, we hear a brief recapitulation of Kronecker's view of algebraic number theory, as opposed to Dedekind's. For Dedekind, Hilbert, and all who followed their line of thought, including Hensel eventually, there were things called algebraic numbers to be talked about, thought about, added and multiplied together. For Kronecker

there were only multivariate polynomials whose arithmetic was to be reduced modulo certain fixed polynomials, and his vision turned out to describe quite well the work of the computational algebraic number theorist that Taussky referred to in her talk. The mathematician sitting before a keyboard and a screen, she seemed to suggest, sees primarily a polynomial, secondarily a field and a generating element. The latter must be held in mind, but only the polynomial would be represented in a data structure in the machine's circuits. That data structure was populated with integers, and the "rational methods" that Taussky referred to were the machine operations that would be performed on those integers.

In the remainder of the talk, Taussky used the term *rational methods* as a kind of technical term: when she said that rational methods were available for a given problem, she meant that it was possible to compute something for this problem. For example, she wrote at the top of page 191,

> A treatment by rational methods is also possible for the [ideal] classes, at least in many cases [21-23]. If the field admits an integral base which consists of the powers of a single number, then there is a 1 to 1 correspondence between the ideal classes and the classes of n by n matrices $S^{-1}AS$, where A is a fixed matrix with $f(A) = 0$. The elements a_{ik}, s_{ik} in $A = (a_{ik})$, $S = (s_{ik})$ are rational integers, and S runs through all matrices with $|S| = \pm 1$.

Note that she was careful to point out that the elements in the matrices were rational integers. For it was through this that the problem was finally grounded in objects which could be represented in and operated upon by a computer.

In the collaboration between Taussky, Zassenhaus, and Dade which we consider in Section 6.1, we will see still more new terminology like "rational methods" being tried out by these pioneers. They will speak of such things as the "computational equivalents" of various algebraic number theoretic objects, these being the data structures that represent those objects, and with which it is possible to compute.

5.3.2 Routine methods

In her section on ideal classes and class numbers, Taussky mentioned KAZ, which had been published the year before, in 1952. As we saw in Section 5.2, Hasse had personally sent her a copy shortly after its publication. She wrote simply,

> Recently a book by Hasse (Hasse 1952) appeared which is concerned with the class number in these fields and their largest real subfields. It contains many new theorems and tables. (Taussky 1953, p. 189)

She did not discuss the programmatic statements in the foreword. In fact, in contrast to Hasse, Taussky was consistently descriptive, not normative: nowhere in her report did she speak about how things *should have been*, but only about how things *were*. We know that Taussky used the results in KAZ in her computational work (see p. 175), but it is not clear whether she agreed with the picture that Hasse portrayed in his foreword.

In one way at least, her attitude was more relaxed than Hasse's, in that she gave ample room for computational methods that might work only in a few cases, rather than being "routine", or generally applicable. We see this in her final comment after discussing the very routine methods of Hasse in (Hasse 1950a):

> A routine method for finding a unit in cyclic cubic fields which together with its conjugates generates all the units was given by Hasse (ibid.). ... Hasse has a routine method for finding the class numbers in cyclic cubic fields, but it is rather complicated. If no routine method is aimed at, the work is sometimes simpler. (Taussky 1953, p. 188)

She thus made the now obvious statement that generally it is easier to find a way to compute certain specific objects of interest, than to give a general method to compute all objects of a certain kind: for example, to compute an integral basis for a given field, rather than to give a generally applicable algorithm for computing integral bases.

Her attitude was thus in contrast to that expressed by Hasse, who called for generally applicable methods to compute number field invariants:

> Yet most such beginnings are lacking in uniformity, in systematicity, and above all in the feeling that one should characterize fields of the kind in question not by random means of determination – such as say the coefficients of a generating equation, be they chosen haphazardly or normalized through some kind of reduction condition – but rather through structure invariants, like discriminant, associated class group, conductor, characters; and predominating in the numerical examples are ad hoc tricks and more or less groping guesses, as opposed to systematic calculation methods. (Hasse 1952, p. VI)

5.3.3 On generalization in number theory

Finally, we return to the point with which Taussky opened her survey talk, since it gives us occasion to visit once again the role of generalization in number theory. She wrote:

> It is frequently claimed that many facts in ordinary number theory can be fully understood only through their generalization to algebraic number fields. A typical fact is the exceptional role played by the prime number 2 in many cases. However, in number fields one proves with ease that all numbers $1-\zeta$ play an exceptional role when ζ is a root of unity. (Taussky 1953, p. 187)

To clarify what Taussky meant, let us write ζ_p for a primitive p^{th} root of unity, where p is any positive rational prime. Then in particular $\zeta_2 = -1$, and Taussky was saying that the exceptional behaviour of 2 in $\mathbb{Q}$ is just the exceptional behaviour of $1-\zeta_2$ in $\mathbb{Q}(\zeta_2)$, a mere special case of the exceptional behaviour of $1-\zeta_p$ in $\mathbb{Q}(\zeta_p)$ generally.

Taussky echoed the same sentiment about the reciprocity law, which surely many had expressed before her as well:

> Another example is the quadratic law of reciprocity for which a really illuminating proof is found only by using number fields. (ibid., p. 187)

Hecke for one had spoken on this when he wrote,

> The development of algebraic number theory has now actually shown that the content of the quadratic reciprocity law only becomes understandable if one passes to general algebraic numbers and that a proof appropriate to the nature of the problem can be best carried out with these higher methods. However, it must be said of the elementary proofs that they possess rather the character of supplementary verification. [30]

And surely one could find any number of statements to the same effect in the literature of algebraic number theory.

---

[30] English translation from (Hecke 1981, p. 53), original from (Hecke 1923, p. 59), quoted in (Lemmermeyer 2000, p. v): *Die Entwicklung der algebraischen Zahlentheorie hat nun wirklich gezeigt, daß der Inhalt des quadratischen Reziprozitätsgesetzes erst verständlich wird, wenn man zu den allgemeinen algebraischen Zahlen übergeht, und daß ein dem Wesen des Problems angemessener Beweis sich am besten mit diesen höheren Hilfsmitteln führen läßt, während man von den elementaren Beweisen sagen muß, daß sie vielmehr den Charakter einer nachträglichen Verifikation besitzen.*

5.4 Letters from the 1960s and 70s

After our last noted letter from March 1955, correspondence between Taussky and Hasse continued on at about the same steady rate, but the topic of discussion turned away from computer usage and instead toward some of Taussky's ideas on matrices which she wanted to discuss with Hasse. While interesting, these letters no longer pertain directly to our topic, and in this last section we simply note a few scattered points from the letters sent in the 1960s and 70s, which we find relevant.

We begin with a letter from Taussky to Hasse, dated 10 Feb 1961, on Caltech letterhead. In 1957 Caltech had invited both Olga and Jack to take teaching positions there, and it is said that the invitation may have had its beginnings when Olga was invited in 1955 to a number theory conference at the campus (Luchins and McLoughlin 1996). They took the jobs, and Olga worked there from 1957 until her retirement in 1977. She originally signed on as a "research associate", a position which did not require any teaching, but she voluntarily taught one course or seminar each year, and she also supervised PhD theses, thirteen in all. [31] In 1971, after the administration recognized someone other than Taussky as the first female professor at Caltech, a title which for all intents and purposes belonged to the former, she brought the matter to their attention, and at last her title was promoted to Professor (Davis 1997).

Taussky wrote of a collaboration with Zassenhaus and her student Dade, which, according to Pohst's memorial article (Pohst 1994), was the very research episode that brought Zassenhaus into computational algebraic number theory. Her enthusiastic mention of the work, and her promise to send a copy shows that she knew it would be of interest to Hasse. She wrote:

> I had completely realized that you were too busy to spend more time on the classes of matrices for the time being. I am very happy about your interest and will certainly inform you if I get more ideas. In the mean time Zassenhaus and Dade, a very gifted young man, and I have completed a first investigation of the semigroup of ideal classes in an order of an algebraic number field. A resumé of this will appear soon and I shall send it immediately.

[31] These details come from reminiscences of Caltech colleague Tom Apostol, published in (Luchins and McLoughlin 1996).

We will continue with the story of this research in Section 6.1.

On 27 Jan 1964, Taussky wrote seeking clarification of a passage in KAZ. It would appear that she and Dade were using it as a reference book for some computational work of their own:

> Dear Professor Hasse,
>
> I would be very grateful if you could give me some advice concerning your book on class numbers of Abelian fields:
>
> On page 54 in footnote 2) you introduce the quantity p. This is also connected with the regulatrix Σ. Mr. Dade and I have some computations concerning p, but we wonder if this is already included in your computations in an indirect way. Our computations concern the real subfield of the field generated by ζ, $\zeta^p = 1$, p prime. I got interested in this in connection with some problem on integral unimodular circulants.

and there was a postscript:

> I think there is much information concerning this on your pages 27-30, but I cannot quite sort it out.

We have already seen that KAZ was cited by Taussky in her 1953 survey. It would be cited again by Zimmer's definitive survey of 1971, which we discuss in Chapter 7. It adds a different kind of evidence for the real importance of this work, however, to see proof that a mathematician such as Taussky actually made real, working use of the book.

In a letter of 9 Dec 1968, Taussky mentioned several things which show that at this time three of our protagonists were still active in computational number theory, and still actively discussing their results with each other. Taussky had revived the computational work on which she had collaborated in the 1930s with Scholz; Hasse and a student were computing tables of data relating to class groups; Zassenhaus and Taussky were interested in Hasse's work and wanted to see the tables:

> You will be interested to hear that I made some progress on the old problems of my thesis and the problems I used to work on with A. Scholz. I hope to write some of it up for the Krull number.

> H. Zassenhaus tells me that your pupil, Gudrun Bayer, has made some tables on the class groups of quadratic fields. Are copies available?

The "Krull number" she referred to was surely the upcoming dual volume 239/240 of *Crelle*, dedicated to Wolfgang Krull for his 70th birthday, in which a paper of hers, "A remark concerning Hilbert's Theorem 94" (Taussky 1969) did appear. Hasse was at this time still editor of *Crelle*, together with Rohrbach.

Hasse had a student by the name of Ochoa whom he put in contact with Taussky so that he might seek her expertise. In a letter of 25 Mar 1971 to Ochoa carbon copied to Hasse, Taussky's remarks demonstrated further the relevance of the sorts of tables in Lehmer's survey of 1941, to a working computational number theorist. The tables of Ince that she mentioned were named in Lehmer's report. [32] We even learn of a specific result which these tables helped Taussky to find:

> ...
>
> In the meantime I want to make some remarks concerning your example for the field generated by $\sqrt{1297}$. ... In order to work out examples you may find the tables by Ince published in the British Association Mathematical Tables IV very useful. I use these tables frequently. In particular they helped me to find my theorem that the transposed matrix class corresponds to the inverse ideal class.
>
> ...

In closing we note that it is evident from their letters and other sources that over the course of their long association Hasse and Taussky became not just colleagues, but friends, something which is not always visible in Hasse's correspondence with the many mathematicians with whom he was in contact. On 21 April 1971 there was a letter from Taussky which makes it clear that Hasse had recently stayed with the Todds on a visit. While the salutations in their letters had begun in Germany as the very formal "Sehr geehrter Herr Professor!" and "Sehr verehrte, liebe Frau Taussky-Todd", and had remained formal for decades afterward, by the 70s their friendship seemed to have matured, and they began to address each other on a first name basis even in writing.

[32] (Ince 1934)

5.5 Coda

In 1977, the year of Taussky's emeritization at Caltech,[33] a volume (Zassenhaus 1977) edited by Zassenhaus was published in honour of three researchers all of whom had been influences on Zassenhaus (and at least one of whom had influenced each of the other contributing authors), one of them being Olga Taussky. The collection opens with a short biographical sketch of each of the three honorees (the other two being Henry B. Mann and Arnold E. Ross), and Taussky's is autobiographical. As we finish this chapter, devoted to her role in our story, we note in closing just a few points from these remarks of Taussky's own, at the end of her long and fruitful career.

Taussky states at one point that,

> Several scholars of immense power came to Caltech during my stay and worked with me a great deal. After years of frequent isolation from mathematicians working in my line, or sometimes from mathematicians altogether, sometimes in positions with hard duties, this was most beneficial for me. These were particularly in number theory Zassenhaus, Dade, and A. Froehlich. (ibid., p. xxxix)

giving Zassenhaus and Dade (who we will consider in Section 6.1) positions of honour. Later she indicates her involvement with computers in number theory, recalling Arnold Scholz, and the tables of Ince.

> Of my other number theory students – L. Foster, D. Davis, and D. Maurer – the first two based their investigations on tables obtained by computers. I myself have been much interested in computational number theory, a subject in which my co-author A. Scholz – mentioned earlier – was a master. For my work on integral 2×2 matrices the tables of E.L. Ince on class groups and units in real quadratic fields are a wonderful help. (ibid., p. xl)

We note in addition, as we prepare to move to our next chapter, in which we will focus on Zassenhaus, that the latter is mentioned no fewer than four times in Taussky's four-and-a-half-page autobiographical sketch. Surely the two had ample influence on each other's lives and work, and accordingly we will begin Chapter 6 with their 1959 collaboration along with the above-mentioned Dade.

[33] Luchins and McLoughlin 1996, p. 845.

Chapter 6

Zassenhaus's work in the 1960s

Zassenhaus remained at the University of Hamburg until 1948. He then took a position at the University of Glasgow, which he held for only one year, before taking a post that lasted for ten years (1949 to 1959), at McGill, in Montreal. During the last year however, Zassenhaus was a visiting professor at Caltech, and this is where his interest in computers began: in 1958, when he was 46.

It is unclear whether Zassenhaus went to Caltech with the plan already in mind to work on computational algebraic number theory with Olga Taussky. His first paper ever coauthored with her (it is on a different subject), was received for publication on 18 December 1958, after his year in California had already begun. Meanwhile, Pohst writes of the year-long stay only that,

> [Zassenhaus's] tendency to computational algebraic number theory came out for the first time at Caltech during his visit 1959. (Pohst 1994, p. 7)

In Section 6.1 we review the number theoretic experiments he carried out that year at Caltech together with Taussky and C. Dade, along with some published reflections on the significance of those experiments, coauthored by Dade and Zassenhaus. Here we will see how these researchers chose data structures with which to represent algebraic numbers and ideals, and how they developed a basic battery of methods to perform arithmetic operations on these objects, and to decide relations like when two algebraic numbers or two ideals are equal. This appears to be a very early case of representing objects associated with algebraic number fields by data structures in a computer.

Of the research program that emerged from this experience, Pohst writes,

> Programmatically Zassenhaus declared the development of methods for the efficient computation of the following four invariants of an algebraic number field F as the most important tasks: (i) the Galois group, (ii) an integral basis, (iii) the unit group, (iv) the class group. (Pohst 1994, p. 8)

Similarly, we saw (p. 125) that in 1945 Hasse felt we should be able to compute at least, "an integral basis, the discriminant, a system of fundamental units, and the class number". In Section 5.3 we saw that in 1953 Taussky identified integral bases, factorization of rational primes in number fields, units, ideal classes, and class numbers as major subjects for the field. In fact even Hilbert wrote, for example, at the very end of §6 of the *Zahlbericht* on units of a field,

> The above proof of Theorem 47 also shows that it is possible to determine a fundamental set of units by means of a finite number of rational operations. A more detailed investigation of the problem of finding the simplest way to calculate the units leads to the theory of continued fraction algorithms, where the wider question of the periodicity of such developments is of particular interest. [1]

showing that he was at least interested in the problem, even if he did not decide that the *Zahlbericht* had room for a section on it. The program articulated by Zassenhaus was thus well in accord with images of the field that earlier proponents had expressed.

Over the next several years Zassenhaus began producing results pertaining to his four main goals, and ultimately, as Pohst writes, "he made considerable contributions for all four tasks". According to Pohst's brief survey, the earliest publications of Zassenhaus contributing solutions to these problems – partial or complete – appeared in print in the years listed in Table 6.1. Typically work begins one or more years before publication, and, in the case of the integral basis, Zassenhaus already presented his work at a conference which met in June 1965, as we will review in Section 6.2.

Meanwhile, in the first half of the decade, he continued to explore his interest in computer-aided experimentation, and even education, in number theory. After his year visiting at Caltech, Zassenhaus took up a position in the department of mathematics at Notre Dame which he would hold from 1959 to 1964. We find some evidence of his continuing interest in computing in that by 1963 he was appointed Director of the Computer

[1] Quoted from Adamson's English translation (Hilbert 1998) of the *Zahlbericht*.

Galois group	1967
Integral basis	1967
Unit group	1972
Class group	1985

Table 6.1: Years of Zassenhaus's earliest published contributions to his computational algebraic number theory program, by subject.

Center at the university. The chair of the mathematics department at that time was Arnold E. Ross, who would move to Ohio State University in 1963, preceding Zassenhaus by a year, and would initiate the latter's move to a research professorship there in 1964. (Pohst 1994, p. 2)

As Zassenhaus would explain in a speech in honour of Ross in 1976 (Zassenhaus 1977, pp. xxvii-xxxiii), Ross entered the University of Odessa at the age of sixteen, as a part of a new program for mathematically talented youth in Russia, and as a result was inspired in his own career to initiate similar programs in the U.S. Ross launched such a program at Notre Dame, and began another at OSU immediately after moving there. In particular, his belief was that,

> ... a course in elementary number theory is particularly suitable to test and develop the talents of a young gifted person. (ibid.),

and accordingly, over the summer of 1964, he enlisted Zassenhaus to run an eight-week course in experimental number theory at OSU, for gifted high school students.

In the subsequent fall semester, Zassenhaus tried offering this same course to university students enrolled at OSU. His description of the computing facilities that they used shows a vivid picture of the sort of technology that might have been available to a university professor in 1964:

> The course met 3 hours per week, 2 hours devoted to theoretical preparation and exercises, 1 hour to experimentation. The room in which the lecture was held was located near a console, through which the parameters and commands stamped into punched-cards were entered, and which, over an approximately 4 kilometre long telephone cable, controlled the IBM 7094 situated in the OSU Computation Center via the IBM 1410. The computer system with its 20,000

> random access kernel words was freed up entirely for our purposes, during the experimentation hour. The output of the computation was always relayed back to the console in less than 10 minutes after acceptance of the data, and there printed out. Most of the time my assistant returned with the numerical result before I had finished explaining the method applied. Eventually we used a projection apparatus with light pointer for display of the results, but for the most part each student received a copy of the computer's output. [2]

Further comments reveal something of the state of the art of programming and algorithms at the time:

> For the success of the experiments it was necessary to use very powerful computer programs, which on the one hand provided the students with sufficient freedom in setting parameters and choosing problems, and which on the other hand would return usable answers in less than 10 minutes. H. Brown used for the subroutines only Internsprache (integer programming!); in order to *combine* the subroutines, however, he employed the symbolic language of the OSU Computation Center, Scatran, an extension of Fortran. For the rapid determination of prime numbers in given intervals (up to say 10^9) the sieve method of Eratosthenes proves most efficient among all well-known methods, making use of the high speed of register operations, to great advantage. [3]

---

[2](Zassenhaus 1967, pp. 104-105): *Der Kursus wurde 3 Stunden wöchentlich gegeben, 2 Stunden dienten der theoretischen Vorbereitung und Verarbeitung, 1 Stunde dem Experimentieren. Der Raum, in dem die Vorlesung gehalten wurde, befand sich in der Nähe einer Datenkontrollstelle, an der die auf Lochkarten gestanzten Parameter und Bestimmungswerte aufgenommen und auf zirka 4 Kilometer langem Telefonkabel der im OSU-Rechenzentrum gelegenen IBM 7094 via IBM 1410 zugeleitet wurden. Die Rechenanlage mit ihren 20,000 frei verfügbaren Kernworten wurde während der Experimentierstunde ganz für unsere Zwecke freigestellt. Der Rechenausstoß wurde durchweg weniger als 10 Minuten nach Annahme der Daten der Datenkontrollstelle übermittelt und dort ausgedruckt. Mein Assistent kam meistens mit der Zahlenausbeute noch eher zurück als ich mit der Erklärung der angewandten Methodik zu Ende gelangt war. Gelegentlich verwendeten wir zur Darstellung der Resultate einen Projektionsapparat mit Lichtzeiger, meistens jedoch erhielt jeder Kursusteilnehmer eine Kopie der Rechenausbeute.*

[3](ibid., pp. 105-106) *Für das Gelingen der Experimente war es notwendig, sehr durchschlagkräftige Rechenprogramme zu verwenden, die einerseits den Studenten genügend Freiheit in der Parameter- und Problemwahl ließen, andererseits in weniger als 10 Minuten verwertbare Antworten ergaben. H. Brown verwendete für die Teilroutinen nur Internsprache (ganzzahliges Programmieren!), jedoch bediente er sich zur Verbindung der Teilroutinen der symbolischen Sprache des OSU-Rechenzentrums, Scatran, die eine Weiterentwicklung von Fortran darstellt. Für das schnelle Auffinden von Primzahlen in gegebenen Intervallen (bis etwa 10^9) stellte sich die Siebmethode des Eratosthenes unter allen bekannten Methoden als am wirksamsten heraus, wobei von der hohen Geschwindigkeit der Registeroperationen mit Vorteil Gebrauch gemacht wurde.*

Zassenhaus published an article describing the OSU experimental number theory course in the proceedings of the same June 1965 conference in Oberwolfach at which he presented his first algorithm for computing an integral basis. In the article he indicated that he had planned a second course, this time on experimental *algebraic* number theory. It is not clear however whether this second course ever took place.

It must be noted that, apart from the administrative challenges that likely were involved in setting up such a course, Zassenhaus also faced the judgement of his peers as he put an increasing amount of his time and effort into computation in an era when this went against the mainstream. Pohst writes (my emphasis) that,

> The constructive point of view was most precisely described in the preface of [Zassenhaus's] joint book with [Pohst]. [4] "History shows that in the long run, number theory always followed the cyclic movement from theory to construction to experiment to conjecture to theory." When that book first appeared in 1989 this point of view was already well adopted. *But when he did research under this guideline Bourbakism was still predominant and computations of all kinds were tabooed.* Zassenhaus stated definitely: "As experience has shown, the new encyclopedia has a similar effect in teaching as Euclid had in his time. It puts the cart before the horse, demanding that the student engage in formal arguments before he has the necessary experience with the fundamentals in an inductive way." [5]

Zassenhaus's statement he believed that computation of examples played an important part in building understanding of the subject. As for Pohst's "cycle" of number theory, involving construction, experiment, conjecture, and theory, we know that such a view, in which experiment played an important part, had been around at least since Gauss, who discovered many of his theorems by experiment. While "conceptualists" like Hilbert may have de-emphasized the role of experiment in published results, it seems likely that they too were led to their results in this way. The rare abstract thinker meanwhile may need no guidance at all from examples and experiments. [6]

As his publication histogram shows, Zassenhaus was very productive in the period from

[4] Pohst refers to (Pohst and Zassenhaus 1989).

[5] (Pohst 1994, p. 4). The phrase "the new encyclopedia" refers to the books of Bourbaki.

[6] Consider for example Grothendieck; see (Jackson 2004).

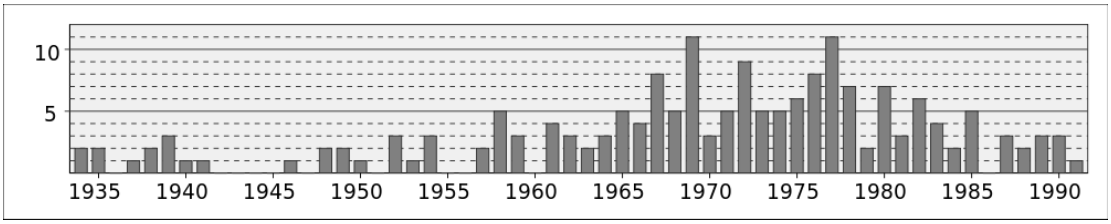

Figure 6.1: Number of papers published by Hans Zassenhaus each year, from 1934 to 1991. Source: (Pohst 1994)

the mid to late '60s on which we will focus. Apart from the two works mentioned already in this introduction – namely, his 1959 "initiation" into the field of computational number theory, and his 1965 integral basis algorithm – we will cover in this chapter the research of 1968 in which Zassenhaus employed Hensel's p-adic methods in practical computation in a big way. In Section 6.3 we review Zassenhaus's work with his student Liang on a problem posed by Hasse, which they solved by a p-adic Newton iteration much like we saw in Section 2.4. In Section 6.4 we consider Zassenhaus's application of ideas from Hensel's p-adic polynomial factorization algorithm which we also saw in Section 2.4, now to the problem of factoring polynomials over $\mathbb{Z}$.

In Section 6.2, by considering the way in which the background on computing integral bases known to Zassenhaus seems to have grown between 1965 and 1971, we will be led to conjecture that specifically during these years Zassenhaus might have delved heavily into the literature of his predecessors such as Hensel and Weyl. His focus on Henselian p-adic methods in 1968 would be consistent with this.

6.1 Algebraic numbers in the computer – 1959 at Caltech

In Section 5.4, we noted a letter sent from Taussky to Hasse in February 1961, in which Taussky discussed her recent work with Zassenhaus and Dade, and promised to send Hasse a copy of the summary of this work, which would soon be published. The summary report appeared on four pages in the Bulletin of the American Mathematical Society in 1961, and was coauthored by all three collaborators. The subsequent larger publication describing all the details of the work filled 34 pages in the *Mathematische Annalen* in 1962, and again was coauthored by all three.

The opening statements of the paper in the *Annalen* explain both why it was entirely natural for someone with Taussky's background to be involved in this research, given its relation to integer matrices and to computers, and also precisely why these researchers found that computers should be brought in:

> The study of fractional ideals of orders of algebraic number fields and their equivalence is closely related to the study of matrices with rational integral elements and their similarities under unimodular transformations.
>
> Such a study should at some stage proceed to the inspection of actual numerical examples. However, quite simple questions, such as the problem of the arithmetical equivalence of two ideals with the same order (see below), require a large number of computational steps. Therefore this task calls for the use of automatic highspeed computers.[7]

A third and final publication on the subject was written by Zassenhaus and Dade alone, [8] and was concerned not with the mathematical results the three had found, but rather with reflections on the role of the computer in their work. They presented it at the Fifteenth Symposium in Applied Mathematics of the American Mathematical Society, held in the spring of 1962, and cited funding from the Office of Naval Research at Caltech. Given that this was Zassenhaus's first foray into computer-aided research, and that he thereafter demonstrated such a profound affinity for computing, the thoughts he and Dade published here should provide us with significant insight into the beginnings of this affinity.

Unfortunately there is no statement as to who exactly did the computer programming – Zassenhaus, Dade, or Taussky – but it seems that Zassenhaus for one must have spent some time with the machine, given his later role as head of the computing center at Notre Dame, and considering the nature of his experimental number theory course at Ohio State.

The stated objectives of the Symposium help to characterize the meaning of computers to mathematicians at this time, as well. There were in fact two separate meetings of this Fifteenth Symposium, the first in Chicago, from April 12 to 14, and the second in Atlantic City, from April 16 to 19. The first was on the subject of "Experimental Arithmetic," and the objective was,

---

[7](Dade, Taussky, and Zassenhaus 1962, p. 31).

[8](Dade and Zassenhaus 1963).

> to examine ways in which the arithmetical potential of modern high-speed computers can furnish experience which sheds light on outstanding problems in mathematics and other sciences. (Metropolis et al. 1963, p. ix)

The second meeting was on the subject of "Interactions between Mathematical Research and High-Speed Computing," and the objective was,

> to enable mathematicians to become familiar with the potentialities of computers of types currently available and with the problems involved in the proper and effective exploitation of these computers. (ibid., p. ix)

Among the four editors of the Proceedings was John Todd. Also submitting papers were Harvey Cohn, and D.H. Lehmer, among others.

The objectives of the Symposium show that in 1962 computers were still new enough that those mathematicians using them were expected to come back with reports of what it was like to use the machines, and with reflections on how they thought such machines could be useful in general. Dade and Zassenhaus were no exception, beginning their talk with discussion of three ways in which they believed high speed computing could influence mathematical research.

Their first suggestion was that, "numerical computation can furnish numerous examples of mathematical objects, which sometimes suggest new conjectures." (Dade and Zassenhaus 1963, p. 87) Interestingly, of the two examples of this phenomenon which they cited, one was Gauss's conjecture of the prime number theorem, and the other concerned the very same tables of Patz that Hasse had mentioned to Taussky in connection with the work of Redei. Dade and Zassenhaus echoed Hasse's call for ways to get a handle on the abstract objects of algebraic number theory:

> In dealing with more abstract structures it is often convenient to have at hand a few numerical examples – enough to set the mind to work, but not so many as to drive out imagination. [9]

The second sort of influence they named was that the challenges involved in computing numerical examples were interesting in their own right. However, Dade and Zassenhaus put an interesting spin on this, pointing in particular to the way in which a necessary retreat from

[9] (Dade and Zassenhaus 1963, p. 87)

incomputable objects to computable ones may force the mathematician to pay attention to a new sort of object which would not otherwise have been considered, but which could turn out to be worth studying.

Thirdly they noted the idea of disproving conjectures by computing counterexamples. Their own work would provide examples of the first two types of influence of computers, but not this third type.

We turn now at last to the nature of the work done by Taussky, Zassenhaus, and Dade, although we will focus not so much on the mathematics involved, as on the way in which the mathematical objects were represented in and operated upon by the computer.

The goal was to study the semigroup formed by the classes of ideals in an order of a number field. Let us review the meanings of these terms here. To begin with, a semigroup is just like a group, except that some elements may fail to have inverses. Thus, there need only be an associative binary operation, and an identity element for this operation.

An order in a number field E may be thought of as a generalization of the ring of integers $\mathcal{O}_E$ of E. It is any subring of $\mathcal{O}_E$ whose additive group possesses a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ of precisely n elements, where n is the degree of E. Thus, an order O is an n-dimensional $\mathbb{Z}$-module contained in $\mathcal{O}_E$ whose basis $\omega_1, \ldots, \omega_n$ might fail to span all of $\mathcal{O}_E$ over $\mathbb{Z}$. For example, an integral basis for the field $\mathbb{Q}(\sqrt{-47})$ is $\left\{1, \frac{1+\sqrt{-47}}{2}\right\}$, whereas $\left\{2, 1+\sqrt{-47}\right\}$ is a basis for an order properly contained in the ring of integers.

Fractional ideals of an order O of a number field E, also called fractional O-ideals, need only be closed under multiplication by elements in O, not in all of $\mathcal{O}_E$. Thus, a finitely generated additive subgroup $\mathfrak{a} \subseteq E$ is an O-ideal if $\omega\alpha \in \mathfrak{a}$ for all $\alpha \in \mathfrak{a}$ and all $\omega \in O$, but not necessarily for all $\omega \in \mathcal{O}_E$.

If for an order O of a number field E we form equivalence classes of fractional O-ideals in the same way that they are ordinarily formed in $\mathcal{O}_E$, namely by defining two ideals $\mathfrak{a}$ and $\mathfrak{b}$ to be equivalent just when there is a nonzero integer $\alpha \in \mathcal{O}_E$ such that $\mathfrak{a} = \alpha\mathfrak{b}$, then the classes so defined form not a group, but a semigroup, in which the class of O is the identity element.

When preparing to study examples of these semigroups at Caltech, however, Taussky, Zassenhaus, and Dade realized that no way was known to compute the equivalence relation on ideals. This meant for one thing that the multiplication table of the class semigroup could not be computed, since, given ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_k$ representing each class, one would need to decide to which of these ideals $\mathfrak{a}_i$ a given product, such as $\mathfrak{a}_1\mathfrak{a}_2$ was equivalent.

It was at this point that the researchers took a step of the kind named by Zassenhaus and Dade as the second way in which high speed computing could influence mathematical research: Since they did not know how to compute this equivalence relation, they decided to replace it by a weaker relation, which they could compute. Namely, they defined ideals $\mathfrak{a}$ and $\mathfrak{b}$ to be "weakly equivalent", written $\mathfrak{a} \sim \mathfrak{b}$, when there were O-ideals $\mathfrak{c}$ and $\mathfrak{d}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ and $\mathfrak{a}\mathfrak{d} = \mathfrak{b}$.

In proceeding to show how their weak equivalence relation on ideals could be effectively computed, Zassenhaus and Dade went on to give what reads like a basic manual for performing arithmetic on number field elements and ideals. The only work they cited in this entire section of the paper was (Weyl 1940), to which they referred only for the basic theory of lattices, and the techniques they discussed here are not present there. It seems likely then that they invented these techniques themselves.

We observe that although the reference to Weyl was casual, or even just because of this, it is significant. Presumably Zassenhaus, the senior author, would at least have approved of this reference, if not decided himself to make it. Since the reference was meant to direct the reader toward the well worked out theory of lattices, the message was clear: Zassenhaus thought of Weyl as the go-to source for a very basic part of algebraic number theory. He could have chosen other books instead. This means for one thing that he was well aware of the Kronecker and Hensel versions of algebraic number theory, on which Weyl put so much emphasis. Moreover, it suggests that his attitudes may have been aligned with Weyl's, i.e. he may have favoured those versions of the theory, if the book was for him a favourite.

Zassenhaus and Dade introduced language to countenance the difference between merely discussing number field objects in the abstract, and actually computing with them. To begin with, they referred to the data structure that would represent an object such as an ideal or an element of the number field as its "computational equivalent". The objects would be called "known" or "given" when the integers in these data structures were known.

In particular, they began by fixing a basis $\omega_1, \ldots, \omega_n$ of the number field E, and noting that for a given ideal $\mathfrak{a}$ of an order O of E there is a unique "reduced basis" $\alpha_1, \ldots, \alpha_n$ of

$\mathfrak{a}$ satisfying:

$$\begin{aligned}
\alpha_1 &= \frac{a_{11}\omega_1}{a}, \\
\alpha_2 &= \frac{a_{21}\omega_1 + a_{22}\omega_2}{a}, \\
&\vdots \\
\alpha_n &= \frac{a_{n1}\omega_1 + a_{n2}\omega_2 + \cdots + a_{nn}\omega_n}{a}
\end{aligned}$$

with the a's relatively prime nonnegative rational integers, and satisfying certain inequalities. They referred to the triangular matrix of integers (a_{ij}) together with the least common denominator a as the "computational equivalent" of the ideal $\mathfrak{a}$, and said that $\mathfrak{a}$ was "given" when these integers were known.

Next, elements $\lambda \in E$ were given a similar treatment. They wrote,

> Any element $\lambda \in E$ has an expression of the form:
>
> $$\lambda = \frac{\ell_1\omega_1 + \cdots + \ell_n\omega_n}{\ell}$$
>
> where $\ell, \ell_1, \ldots, \ell_n$ are rational integers. We say that "λ is known" if the integers $\ell, \ell_1, \ldots, \ell_n$, which make up its computational equivalent, are known.

The next step was to say how the product of two known elements λ, μ of E could be computed, and they showed that this was possible provided we knew the "structural constants of E with respect to the basis $\omega_1, \ldots, \omega_n$." These "structural constants" were defined as follows:

> These are the rational integers z_{ijk} $(i, j, k = 1, \ldots, n)$ defined by:
>
> $$\omega_i\omega_j = \sum_{k=1}^{n} z_{ijk}\omega_k, \qquad i, j = 1, \ldots, n.$$

Whether this term, "structural constants" was in any kind of common use at this time is not clear. We may note at least that when in a 1965 talk Zassenhaus would go over essentially the same matter, he would not use this term, at that time giving these coefficients no special name at all.

It was shown next how to decide whether a given lattice was an ideal of O or not, and then, given two known ideals, how to compute both their product, and their quotient.

Whereas the way to compute the product of ideals was stated in just a few words, it took a little over a page to show how to compute the quotient.

From these ingredients, a process was put together with which to decide whether two given ideals were equivalent or not, by the weak equivalence relation introduced above.

In the remainder of the paper Zassenhaus and Dade went on to show an example of the sort of output their "7090 at UCLA's Western Data Processing Center" produced, and to discuss a conjecture which they together with Taussky formulated on the basis of such examples, and proved. The main point of interest to us, however, is that here in this work, these researchers developed the basics of computational arithmetic with number field elements and ideals. In summary, they provided:

- a computational equivalent of an element λ;
- a computational equivalent of an ideal $\mathfrak{a}$;
- a way to decide "=" on elements;
- a way to decide "=" on ideals;
- a way to compute the product of two elements;
- a way to compute the product of two ideals;
- a way to compute the quotient of two ideals;
- a way to decide whether a lattice is an ideal;
- a way to decide whether two ideals are weakly equivalent in the sense defined above.

With this, these researchers had the beginnings of a general battery of data structures and procedures with which to carry out computational studies in algebraic number theory. If their citations were diligent, then it would seem that these techniques were entirely of their own invention. Inspection of the survey later conducted by Zimmer (Zimmer 1972) suggests that this may have been the first time in history when algebraic number theoretic objects such as number field elements and ideals were represented and computed with, by data structures on an electronic computer.

6.2 Integral bases etc. in the mid 1960s

We leap forward now to the middle of the decade. In his experimental number theory course at Ohio State, Zassenhaus was showing his students how to apply computers to numerous problems in number theory, some of them even relating to algebraic number theory, such as the question of whether the class number of real quadratic number fields is infinitely often equal to unity, or such as investigation of units in real quadratic number fields. Meanwhile, he was developing an algorithm to compute an integral basis for a number field. Whereas the operations and predicates which we saw Zassenhaus and Dade computing in their 1962 Symposium talk constituted rudiments of algebraic number theoretic computation, now the former was attacking a more challenging problem.

Zassenhaus had occasion to present both his work on the integral basis, and also his experiments in education, at a conference on numerical problems in approximation theory (*Tagung über Numerische Probleme in der Approximationstheorie*), which met at Oberwolfach, 22 to 25 June 1965. Other notable computationalists Gröbner and Jack Todd both presented papers as well. The proceedings were published in (Collatz, Meinardus, and Unger 1967). In this section we review some of this work, which occupied Zassenhaus in the mid 1960s.

6.2.1 Number theoretic experiments in education

In the Oberwolfach talk on his OSU experimental number theory course, Zassenhaus listed the many problems that he investigated with his students. We present the list here in order to give an idea of the scope of problems that Zassenhaus was attacking on the computer, and which were already suitably well under control that they could be presented as course work.

1. Solution of linear Diophantine equations
2. Prime numbers
   (a) Number of prime numbers up to a given upper bound
   (b) Prime numbers in given intervals
   (c) Number of twin primes in given intervals
3. Prime numbers in progressions

(a) arithmetic progressions

(b) are there more prime numbers of the form $4k+1$ than prime numbers of the form $4k+3$?

(c) related questions

(d) prime numbers in higher polynomials

(e) Mersenne and Fermat primes

4. Primitive residues

(a) existence

(b) Gaussian algorithm for generation of primitive residues modulo a given prime number

(c) how often is a given integer a primitive residue?

(d) generalization to quadratic number fields

5. Finite fields

6. Separation of quadratic residues and nonresidues

7. Continued fraction expansions

(a) rational numbers

(b) higher real irrational numbers

(c) real quadratic irrationalities

8. Units in real quadratic number fields

As a result of this course, moreover, some of the students went on to work with Zassenhaus on more difficult and unsolved problems. He wrote,

> With satisfaction I discovered that every auditor of my lecture went on in the winter quarter of the academic year 1964/65 to attend a course I announced on algebraic number theory, in which the conceptual standpoint was brought much more strongly to the fore than in the previous course. During the lecture, they were prepared for the yet unsolved experimental problems, and three of

> my auditors participated in an extensive project toward the programming of a fundamental "root-calculus" whose completion will later make it possible to hold a course on experimental algebraic number theory.
>
> Another auditor (J. Sonn) and I found a new constructive approach, based on a geometric Monte Carlo method, to the theorem on the existence of a primitive element for finite separable field extensions. [10]

His work on this "root-calculus", and his concurrent work on an algorithm for computing integral bases, seem to characterize the stage of Zassenhaus's approach to computational algebraic number theory in 1964-65 as having been no longer *rudimentary* – as it was during the 1959 work with Taussky and Dade – but still somewhat *preparatory*, i.e. still concerned with fundamental algorithms on which others would be built. The "root-calculus", at least, was meant to permit a course on experimental algebraic number theory. As for the computation of the integral basis, while indeed somewhat fundamental, this was also one of Zassenhaus's four main goals for computational algebraic number theory, so in this sense he was making headway into his main program.

It seems that some time between his talk at Oberwolfach and the publication of the proceedings, which did not appear until 1967, Zassenhaus sent a similar article to Hasse. The Oberwolfach paper was called "*Zahlentheoretische Experimente im Unterricht*", whereas Hasse's reply of 11 February 1966 referred to a different paper of Zassenhaus, which appeared in a different publication (Zassenhaus 1966). Hasse wrote,

> I wish to thank you heartily for the sending of your article *"Experimentelle Mathematik in Forschung und Unterricht"*. You have really unearthed and developed very beautiful problems there. I was especially interested in the fast algorithm for finding a primitive root, and the generalization of the Artin conjecture on

[10] (Zassenhaus 1967, pp. 107-108) *Mit Genugtuung stellte ich fest, daß alle Hörer meiner Vorlesung im Winterquartal des akademischen Jahres 1964/65 einen von mir angekündigten Kursus über algebraische Zahlentheorie belegten, in dem die begrifflichen Gesichtspunkte viel stärker im Mittelpunkt als in dem vorherigen Kursus standen. Sie wurden während der Vorlesung der noch ungelösten experimentellen Aufgaben gewärtig und drei meiner Hörer nahmen an einem umfangreichen Projekt zur Programmierung eines grundlegenden "Wurzelkalküles" teil, dessen Fertigstellung später die Abhaltung eines Kurses über experimentelle algebraische Zahlentheorie ermöglichen wird.*

Ein anderer Hörer (J. Sonn) und ich fanden einen neuen konstruktiven, auf einer geometrischen Monte Carlo Methode beruhenden Zugang zu dem Satze über die Existenz eines primitiven Elementes für endlich separable Körpererweiterungen.

primitive roots. [11]

Once again, Zassenhaus and Hasse were sharing an interest in number theoretic algorithms. Another letter from Hasse later that year, on 17 November 1966, showed more sharing of computational results:

> Perhaps you will be interested in the enclosed material: text, tables, and programming instructions for a work, which will soon appear in the Mathematische Nachrichten. I have not called for further calculations of this kind. Mr. Benz will elaborate for you if necessary. [12]

6.2.2 The ORDMAX algorithm – 1965

In a second talk at the Oberwolfach meeting in 1965, Zassenhaus presented an algorithm for computing an integral basis for a number field, which worked by starting with a basis for some order in that number field, and then successively augmenting the basis to span larger and larger orders, until finally the maximal order, i.e. the ring of algebraic integers, was spanned. The algorithm thus fully embraced the point of view from which the ring of integers is just another order – the largest of them. It is true that the algorithm given by Hensel, which we reviewed in Section 2.4, starts by considering the power basis $1, \beta, \ldots, \beta^{\lambda-1}$ with β integral, which is a basis for an order contained in the ring of integers; but Hensel seems not to have thought of the procedure in terms of enlarging orders.

We have abundant evidence that orders were indeed an important topic for Zassenhaus. As we saw in Section 6.1, the work with Taussky and Dade was concerned with orders, namely with the generalization of results about certain objects associated with the maximal order in a number field – namely the class group – to the corresponding objects associated with number field orders in general.

Several years later, in May 1972, a "Conference on Orders, Group Rings, and Related Topics" would be held at the Ohio State University, in honour of Zassenhaus. In the foreword to the published proceedings, Arnold E. Ross wrote:

---

[11] *Ich möchte mich recht herzlich für die Zusendung Ihres Aufsatzes "Experimentelle Mathematik in Forschung und Unterricht" bedanken. Sie haben da wirklich sehr schöne Probleme ausgegraben und entwickelt. Besonders hat mich das schnelle Verfahren zur Auffindung einer Primitivwurzel und die Verallgemeinerung der Artinschen Vermutung über Primitivwurzeln interessiert.*

[12] *Vielleicht interessiert Sie das beiliegende Material: Text, Tabelle und Programmierungsanleitung für eine Arbeit, die demnächst in den Mathematischen Nachrichten erscheinen wird. Weitere numerische Rechnungen dieser Art sind von mir nicht in Auftrag gegeben. Herr Benz wird Ihnen nötigenfalls Erläuterungen geben.*

> It gives me great pleasure to extend my warm good wishes and those of my colleagues to our distinguished colleague Professor Hans Zassenhaus upon the occasion of his sixtieth birthday.
>
> Professor Zassenhaus has contributed important ideas and methods to many and diverse branches of mathematics. Among these the range of ideas concerned with Orders, Group Rings and Related Topics have held his attention for many years. His fundamental contributions to these fields have been known, appreciated and used very widely. It was thought appropriate to mark Professor Zassenhaus' sixtieth birthday by bringing together a group of fellow mathematicians who share his interest in Orders and Group Rings for a discussion of the progress to date and the prospects for the future of this difficult and important field of mathematical endeavor. [13]

Zassenhaus's own contribution to the volume was the third version of his integral basis algorithm, whose first version we are presently concerned with.

In fact, Zassenhaus characterized his algorithm as solving not the problem of computing an integral basis for a number field, but rather the problem of embedding a given order in a maximal order, and it was from this point of view that the algorithm got its name, "ORDMAX".

The reviewer for *Mathematical Reviews* of Zassenhaus's paper on ORDMAX was none other than Olga Taussky, and in her review she summarized the approach succinctly:

> An order $\mathfrak{o}$ in an algebraic number field of degree n is a subring of integers with n base elements and containing 1. If its discriminant differs from the discriminant of the field then $\mathfrak{o}$ is not the maximal order. The latter can then be found by replacing the base elements in such a way that the discriminant loses some of its square factors.

By way of motivation, Zassenhaus noted in his Oberwolfach talk that his algorithm would be faster and less specialized than an existing algorithm of Berwick, for the computation of integral bases. We therefore begin by reviewing the latter, in the first subsection below. We then go on to study Zassenhaus's algorithm itself.

[13](Dold and Eckmann 1973)

6.2.3 Berwick's algorithm

W.E.H. Berwick (1888 - 1944), a Cambridge-trained mathematician, published thirteen papers and one monograph. Hawkins writes that, "A penchant for problems involving numerical computation is reflected throughout his publications," (Hawkins 2008) but adds that "Its strong numerical orientation, however, kept his work outside the mainstream of developments in algebraic number theory," reconfirming our image of the unfavourable popular opinion of numerics in this era.

Berwick's monograph (Berwick 1927), aptly titled *Integral Bases*, is a work of about a hundred pages, in which he developed a method by which integral bases could be computed. As he wrote in the book's preface, the method was widely but not universally applicable:

> Failing cases exist but the approximations given are sufficient to cover nearly any numerical equation not specially constructed to defy them. (ibid.)

Later, in (Zassenhaus 1972), Zassenhaus would explain precisely to which cases Berwick's method was applicable. His characterization is roundabout, but perhaps worth repeating here. In general, he described the problem as the task of embedding an order Λ with finite $\mathbb{Z}$-basis $b_1, b_2, \ldots, b_n$ into a maximal order, where Λ is given by the same sort of "structural constants" that Zassenhaus and Dade defined in their 1959 work, i.e., by data which say how to multiply ring elements in terms of their representations over the basis of b_i. In particular, he would give n-by-n matrices $L^{(h)}$ for $h = 1, \ldots, n$ such that for any elements

$$x = \sum_{i=1}^{n} x_i b_i$$

$$y = \sum_{i=1}^{n} y_i b_i,$$

if we write $xy = z$, and

$$z = \sum_{i=1}^{n} z_i b_i,$$

then we have

$$z_i = \sum_{h=1}^{n} \sum_{j=1}^{n} x_h L_{ij}^{(h)} y_j.$$

In Berwick's case, Zassenhaus described $\Lambda = [1, b_1, \ldots, b_{n-1}]$ as the order connected with a monic separable polynomial

$$P(t) = t^n + a_1 t^{n-1} + \cdots + a_n$$

over $\mathbb{Z}[t]$ in the following way. To begin with, we define a matrix $A = (a_{ij})$ associated with P by

$$a_{ij} = \begin{cases} \delta_{i,k-1} & \text{if} \quad 1 \leq i < n \\ -a_{n-k} & \text{if} \quad i = n \end{cases}$$

where $\delta_{i,j}$ is the Kronecker δ symbol. Then define $L^{(h)} = A^{h-1}$ for $h = 1, \ldots, n-1$, thereby specifying Λ via the rule for multiplication of elements in terms of their representation over the basis of Λ.

Reviewing the state of the art in computing integral bases at the time of his own work, Berwick estimated that quadratic, cubic, quartic, and cyclotomic fields had been handled but that little else had been done.

> A quadratic field can always be defined by the equation $\theta^2 - m = 0$, where m is an integer divisible by no square factor, and then an integral basis is known to be
>
> $$\mathfrak{o} = \left(1, \frac{1}{2} + \frac{1}{2}\theta\right) \quad \text{or} \quad (1, \theta)$$
>
> according as
>
> $$m \equiv 1 \pmod 4 \quad \text{or} \quad m \equiv 2, 3 \pmod 4 .$$
>
> Methods of finding an integral basis of a cubic field are due independently to G.B. Mathews and G.T. Woronoj. An integral basis of a cyclotomic field has been obtained by Kummer, while Hilbert's detailed investigations of quadratico-quadratic fields include a discussion of the algebraic integers therein. Little appears to have been done beyond these cases. (Berwick 1927, p. 1)

Berwick's method, in basic form, is reminiscent of the construction of the integral basis in Hilbert and in Hensel which we saw in Chapter 2 – Hensel's more so, in that Berwick's construction involved actual tests of integrality. For the field $\mathbb{Q}(\theta)$ (which Berwick denoted by "$[\theta]$"), where θ satisfied the irreducible polynomial

$$\theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \cdots + a_n = 0,$$

Berwick constructed an integral basis of the form

$$\mathfrak{o} = \left(1, \frac{\psi_1(\theta)}{\Delta_1}, \frac{\psi_2(\theta)}{\Delta_2}, \ldots, \frac{\psi_{n-1}(\theta)}{\Delta_{n-1}}\right),$$

where the ψ_r were degree-r polynomials in θ,

$$\psi_r(\theta) = \theta^r + a_{r1}\theta^{r-1} + \cdots + a_{rr}$$

and the Δ_r were certain factors of the discriminant $D(\theta)$ of θ. Berwick would consider the primes p that divided the discriminant $D(\theta)$ one at a time. For each term

$$\frac{\psi_r(\theta)}{\Delta_r} = \frac{\theta^r + a_{r1}\theta^{r-1} + \cdots + a_{rr}}{\Delta_r}$$

in the basis, he would write $\Delta_r = p^{\mu_r}\delta_r$ with $(p, \delta_r) = 1$, would let c_{rs} be the reduced residue of a_{rs} mod p^{μ_r}, and would ask whether

$$\frac{\theta^r + c_{r1}\theta^{r-1} + \cdots + c_{rr}}{p^{\mu_r}}$$

was integral or not. He wrote,

> ... an integral basis can be immediately constructed when all complex integers [of the above form] have been determined for each prime p dividing $D(\theta)$. (Berwick 1927, p. 2)

6.2.4 Zassenhaus's algorithm

Starting in 1962, a student named Joseph Liang (b. 1936), was affiliated with the Ohio State University, as Teaching Assistant from 1962 to 1965, as "Scientific Programmer" from 1965 to 1966, then as Research Associate 1966 to 1969. Some time during this period he began to work with Zassenhaus, and would complete his PhD with him in 1969, with a dissertation entitled *On Interrelations of Arithmetical Invariants in Algebraic Number Fields*, the subject matter of which we consider more closely in Section 6.3. Liang helped with the writing of the ORDMAX program, and later he would use the program in his doctoral thesis. [14]

In 1971 Zassenhaus would recall, after stating a theorem on which his algorithm was based,

> On this basis a program (ORDMAX) of computing the maximal order for a given commutative order R was written by my Columbus collaborators (headed by H. Kempfert and J. Liang) in 1966-68. It yielded the discriminant of a maximal order and its Z-basis (minimal basis of $2R$) in between 2 and 3 minutes for $n \leq 6$ and single precision on the IBM 7090. (Zassenhaus 1972, p. 394)

[14] (Liang 1969)

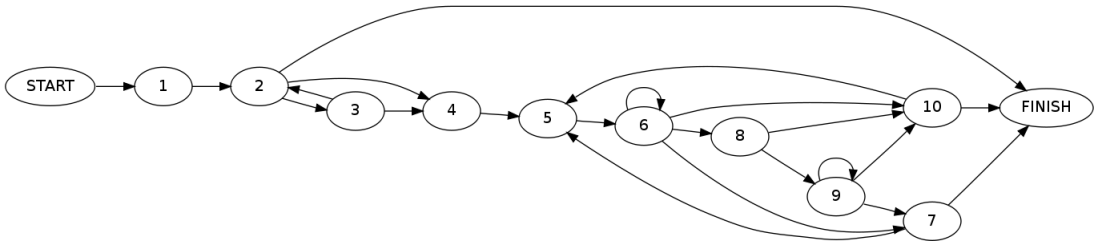

Figure 6.2: Flow chart for Zassenhaus's ORDMAX algorithm.

Here n denotes the order of the basis. Thus, Zassenhaus was able to handle easily a problem on a scale that would have been prohibitive for the integral basis algorithm of Hensel that we reviewed in Section 2.4. There, with $n = 6$, if the discriminant d were as large as 100 (and it could very easily be much larger), then Hensel would already have one trillion checks to perform.

We review now the structure of the ORDMAX algorithm in some detail, if only since this algorithm seems not to be covered in other sources. For ORDMAX to be abandoned in modern treatments is perfectly sensible, since this original version of the algorithm was superseded by later versions, principally the second, which we study in Section 6.2.5. For the sake of history however, we study the first version here.

Zassenhaus laid out the algorithm in 10 steps, for which the "go to" statements resulted in the connectivity diagrammed in Figure 6.2. In broad outline, and referring to Figure 6.2, the basic flow of the algorithm to embed an order $\mathfrak{o}$ in a maximal order is as follows. Step 1 is an initialization. At 2, if the discriminant $d(\mathfrak{o})$ of $\mathfrak{o}$ is squarefree, then we finish immediately. If $\mathfrak{o}$ is not commutative, then we go to 3, replace $\mathfrak{o}$ by another order, and go back to 2. There is now a second chance for the discriminant to be squarefree, and for an early exit.

Otherwise, we move on to 4 and then to 5, initializing the set of primes whose squares divide the discriminant. We will handle these one by one, returning to 5 each time we are ready to handle the next prime.

All of the real work takes place in 6 and 9. Each of these has the potential to send us on to 7 or 10, where we will decide whether to finish, or to go back to 5, for the next prime. As for 8, it either sends us on to 10, or initializes the process that takes place in 9.

In fact steps 3, 8, and 9 are needed only if $\mathfrak{o}$ may be non-commutative, and step 9 is quite complex. In the case of number fields, $\mathfrak{o}$ must be commutative, so Zassenhaus's algorithm may be simplified considerably for express application to the problem of computing an integral basis for a number field.

It is noteworthy, however, that as a footnote to step 9, at a point at which we must determine whether a certain polynomial $M(x)$ is reducible or not, Zassenhaus provides a way to check for reducibility. Namely, he says that we must consider the greatest common divisor of $M(x)$ with each of the polynomials

$$x^{|F_k|^\nu} - x$$

for $1 \leq \nu \leq \frac{1}{2} \deg M$, and ask whether any of these GCDs has degree strictly between 0 and the degree of M. Here F_k is the Galois field of order p^k.

This basic idea of investigating the factors of a polynomial over a finite field $\mathbb{F}_q$, $q = p^k$, by computing its GCD with polynomials of the form $x^{q^\nu} - x$ has a long history. According to von zur Gathen (von zur Gathen 2006) the idea goes all the way back to Gauss, but was obscured since it was intended for the eighth section of the *Disquisitiones Arithmeticae*, which was published only posthumously in 1863, long after the book appeared in 1801. [15] As we saw in Section 2.4, this is precisely the same reason why Gauss's statement of "Hensel's lemma" did not appear in 1801.

Zassenhaus himself did not know exactly where the idea came from. When he finally published with David G. Cantor a polynomial factorization algorithm based on the idea (Cantor and Zassenhaus 1981), they wrote that it "appears to be a 'folk method'", and referred to Knuth's *Art of Computer Programming*, where it is noted that the technique, "was known to several people in 1960 ... but there seem to be no references to it in the 'open literature.'" (Knuth 1981, p. 430)

Two years after Zassenhaus's presentation at Oberwolfach, and in the same year 1967 in which those proceedings were published, Berlekamp gave a polynomial factorization algorithm based on related but somewhat different ideas. In his 1969 paper on polynomial factorization using Hensel's lemma, which is the subject of our Section 6.4, Zassenhaus refined one step of Berlekamp's procedure again using this same core idea which came up already in his 1965 talk. [16]

[15] See (Frei 2007) on Gauss's unpublished Section 8.

[16] See (Zassenhaus 1969, p. 305). Here Zassenhaus cited Berlekamp's publications in Bell Labs technical

6.2.5 "Round 2"

Pohst wrote in 1994 (Pohst 1994) that,

> Basically, all methods for solving [the problem of computing an integral basis] are based on ideas of Zassenhaus. ... Already in [a paper from 1967] he developed an algorithm for the computation of a maximal order, which subsequently became known as ROUND-TWO. It is still the core part of all methods applied in practice. Variants of it are implemented in several computer algebra systems.

Today, eighteen years later, the same still seems to be true. The computer algebra system MAGMA, for example, still uses the Round 2 algorithm for some cases, while deploying a variant called Round 4 on other cases. [17]

The "Round n" naming scheme for these algorithms originated in an odd way. In the paper (Zassenhaus 1972) in which Zassenhaus introduced what came to be known as the Round 2 algorithm, he gave revisions and improvements of the ORDMAX algorithm (which, by this token, could reasonably be called the "Round 1" algorithm). The paper was presented at a symposium at the University of Montreal, called "Applications of Number Theory to Numerical Analysis", which met 9-14 September 1971.

In the introductory section Zassenhaus mused briefly on the way in which, after taking some time away from a problem, a researcher can sometimes return to it, and in this "second round" come up with new ideas. This is the only reason for the name. It has nothing to do with the algorithm itself, but only these casual and incidental remarks of Zassenhaus. Somehow the name stuck. He wrote,

> A close scrutiny of the [ORDMAX] program did not only show that the efficiency of many computational steps could be greatly improved, but it also lead to a number of mathematical questions the solution of which was likely to lead to great improvements in principle.
>
> This sort of review sets in motion the *second round of the program*. There are likely to be many 'second rounds'. The 'last round' would be the successful demonstration of the optimality of the computational methods used by the program in some well defined and pertinent sense.

---

reports (Berlekamp 1967b, 1968a,b). A version of (Berlekamp 1967b) was published in (Berlekamp 1967a), and many of the ideas were collected in the more readily accessible (Berlekamp 1970).

[17] See `http://magma.maths.usyd.edu.au/magma/overview/2/16/6/`.

> The way research progresses today it is more likely that each subsequent 'second round' will produce extensions of the task which had to be mastered initially. Thus at the present 'second round' I discovered that with little additional efforts the new ORD MAX program can be so written that all maximal orders containing a given Z-order of the same rank will be found. This is significant in case the initial Z-order Λ is non-commutative. In case Λ is commutative, there is only one maximal order of the same rank containing Λ (see §2). (Zassenhaus 1972, p. 394)

By 1971, six years after the original presentation of ORDMAX in Oberwolfach, Zassenhaus seems to have delved more deeply into the literature on computation of integral bases, now having more works beyond Berwick's to cite. In particular, (Weyl 1940) was now cited, and methods of Hensel came up repeatedly. Therefore it seems likely that between 1965 and 1971 Zassenhaus was revisiting the old literature on this subject. This would also be consistent with his focus on Henselian p-adic methods in 1968.

Of Berwick's algorithm, Zassenhaus wrote that it was,

> strictly local in analogy to Puiseux's development in algebraic geometry, i.e. in the spirit of the Hensel method. (Zassenhaus 1972, p. 393)

He named further a method of Weyl, [18] but mentioned only the existence of it, and said nothing more about it. Consulting Weyl, we note that it appears to be essentially a p-adic lifting method. Furthermore, among citations of his own prior work, Zassenhaus named *"Über eine Verallgemeinerung des Henselschen Lemmas"* ("On a Generalization of the Hensel Lemma"), from 1954. Hensel's ideas, and p-adic methods generally, thus had a visible presence in this work of Zassenhaus.

Meanwhile, on the side of applications, Zassenhaus cited the PhD thesis of a Gurnam Kaur at the University of Punjab (he did not give the date of the thesis), who applied both the Berwick and the Weyl methods to compute the discriminants of "about 100" algebraic number fields of degree six. The thesis was called, "The Minimum Discriminant of sixth Degree of totally real algebraic Number Fields and other results".

We leave off here with our study of the "second round" of Zassenhaus's integral basis algorithm, and although we have taken only a superficial look at the circumstances surrounding this work, we hope that at least to have made evident the ties to Hensel and Weyl.

[18] (Weyl 1940, pp. 107-109)

6.3 On a problem of Hasse

Hasse appears to have visited Ohio State University for about a month in early 1968 – roughly the month of March, plus or minus a week at each end. A letter from Zassenhaus of 25 February 1968 addressed to Hasse at OSU welcomed him and apologized for the former's temporary absence, while he collaborated again with Olga Taussky at Caltech. [19] A letter from Hasse on 9 April 1968 thanked Zassenhaus for a pleasant visit.

It would seem that while Hasse was at OSU he may have communicated to Zassenhaus and his student Liang a problem [20] which these two soon solved in a computational way, publishing their result in a paper called, "On a Problem of Hasse", which appeared in the July 1969 issue of *Mathematics of Computation*. [21]

Pohst wrote of this episode,

> A major success was the proof of the isomorphy of three quintic fields which occurred as candidates for the real subfield of the Hilbert class field of $\mathbb{Q}((-47)^{1/2})$. This problem pointed out by Hasse could not be solved by theoretical methods before. Hence, the numerical solution by Zassenhaus and Liang gave major credit to methods in constructive algebraic number theory. (Pohst 1994)

After learning of the result of Zassenhaus and Liang in 1968, Hasse too praised their discovery, writing that formerly no algorithm was known, and that the way to solve the problem had escaped prominent mathematicians:

> A procedure to solve these two pure algebraic problems on algebraic extensions of an algebraic number field, given by an equation assumed cyclic, was not to be found in the literature; and notable algebraists, such as e.g. van der Waerden, could not straightaway advise any solution method. Prompted by the example here at hand, such a general procedure was developed in the work (Zassenhaus and Liang 1969), relying on a p-adic procedure developed by Zassenhaus (Zassenhaus 1969) for the factorization of polynomials. [22]

---

[19] The collaboration might have been on the last coauthored paper of Taussky and Zassenhaus, published in 1970. This paper was entitled, "On the 1-cohomology of the general and special linear groups".

[20] There is, at any rate, no sign of his having communicated it instead in any letter present in his *Nachlass*, whereas subsequent letters show Zassenhaus and Liang addressing the problem immediately after Hasse's having left Columbus.

[21] (Zassenhaus and Liang 1969)

[22] (Hasse and Liang 1969, p. 95) *Ein Verfahren zur Lösung dieser beiden rein-algebraischen Aufgaben über*

We note in passing that it even sounds as though, by stressing so heavily the algebraic nature of the problem, and the absence of a solution among well-known algebraists, Hasse might have hoped to suggest that not only number theory but pure algebra too could come under the domain of his beloved p-adic numbers. Whether his mention of van der Waerden in particular was meant to be emblematic of the abstract approach to which his concrete computational approach was opposed is another question, but here we digress.

The statements of Pohst and Hasse suggest the importance of this research episode in the history of computational algebraic number theory, and perhaps in the history of p-adic methods as well, and we therefore devote this section to a study of it.

In addition, one of our themes is the way in which computing and working with examples of algebraic number field objects can lead to new insights into the general way in which things work in number fields, and we ought to at least once illustrate this process by reviewing an example, instead of simply speaking about it in the abstract. For the very same principle holds on our own level of discourse: we will understand our subject better if we consider an example!

From Hasse in particular we have heard not only calls for such understanding through examples, as in the foreword to KAZ, but furthermore continual questing for insight into the nature of number fields through the "right" or "proper" or "natural" representations of things – the *arithmetic* representations, or representations that banish transcendental methods. In order then to exemplify all these matters which we have been discussing up to now in the abstract, we should not be surprised to find a suitable case study in Hasse. In particular, we will examine those discoveries in his collaboration with Zassenhaus and Liang which he framed as valuable insights, gained through the study of computed objects.

Of course there is nothing profound in demonstrating the general fact that in examples mathematicians find structure and patterns. What is special about algebraic number theory is that examples are so hard to come by. In this interaction of Hasse, Zassenhaus, and Liang, we will see the great pains it took – as late as roughly a century or more after the subject's inception – to compute a few class numbers, fundamental units, singular primary numbers, field generators, and Galois automorphisms. It was the challenging nature of

---

algebraische Erweiterungen eines algebraischen Zahlkörpers, die durch eine theoretisch als zyklisch bekannte Grundgleichung gegeben sind, war in der Lehrbuchliteratur nicht zu finden, und namhafte Algebraiker, wie z.B. van der Waerden, konnten auf Anhieb keinen Weg zur Lösung vorschlagen. Veranlaßt durch das hier in Rede stehende Beispiel wurde ein allgemeines solches Verfahren in der Arbeit [2] entwickelt, und zwar gestützt auf ein von Zassenhaus [3] entwickeltes p-adisches Verfahren zur Faktorisation von Polynomen.

these calculations and others like them that meant that a computational branch of algebraic number theory could constitute a subject in its own right, meriting survey talks, conferences, and the attention of world-class mathematicians. Moreover, if example objects were so hard to compute, then we should be eager to see just what sorts of structural insights these prized and hard-won objects might have furnished, to make their arduous retrieval seem worthwhile.

6.3.1 Background on the class field construction over $\mathbb{Q}(\sqrt{-47})$

Heinrich Weber (1842 - 1913) wrote the three-volume *Lehrbuch der Algebra*, [23] a massive collection of algebraic knowledge, very popular in its time. It would not be recognizable as "abstract algebra" to modern eyes, however, embracing an older view of the subject, before the dawn of the "structural" conception in which the objects of study became things like groups, rings, and fields, and the homomorphisms between them. Instead, its subject headings range over algebraic topics as Lagrange, Abel, or Galois might have viewed them – namely as directed toward the solution of equations of various degrees – as well as over many of the number theoretic topics out of which most of the modern algebraic abstractions originally sprang. The exception is the devotion of Volume II to the theory of groups, but even here groups are studied only as an aid to the solution of equations, not for their own sake. [24]

Between 1924 and 1928, at the invitation of the publisher of Weber's *Lehrbuch*, R. Fricke (1861 - 1930) wrote three new algebra volumes, intended as replacements for the books of Weber, the last edition of which had finally gone out of print. The subtitle of the first volume, "written with use of Heinrich Weber's book of the same name" (*verfasst mit Benutzung von Heinrich Webers gleichnamigem Buche*) attests to the book's purpose. In his review, L.E. Dickson wrote that indeed the book was "essentially the same as Weber's volume 1 and the earlier chapters on abstract groups in Weber's volume 2." (Dickson 1925) He stated that Fricke's intention was for the later volumes to differ more from those of Weber; however, his

[23] Weber originally conceived of it as a two-volume collection, and as planned the first editions of volumes I and II appeared in relatively quick succession, their forewords signed November 1894, and July 1896. (Weber 1895), (Weber 1896). What was published in 1908 as the third volume (Weber 1908) was in fact the second edition of his earlier book on elliptic functions and algebraic numbers (Weber 1891).

[24] See Corry (Corry 1996) on the rise of the structural image of algebra. In (Corry 2007), Corry has tracked the transition of the received view of algebra between that embraced in Weber's *Lehrbuch* and that of van der Waerden's *Moderne Algebra*.

review of the second volume (Dickson 1928) indicates that in whatever way Fricke may have altered the content, he retained the 19th century image of algebra as being about equations, not about structures, a story which Corry corroborates (Corry 1996, pp. 55-58).

In their respective third volumes, Weber and Fricke each gave polynomials, f_W resp. f_F, having real roots θ_W resp. θ_F, such that the Hilbert class field N over $\Omega = \mathbb{Q}(\sqrt{-47})$ is equal to $\Omega(\theta_W) = \Omega(\theta_F)$. They used the theory of modular functions in order to derive the polynomials f_W and f_F. Hasse, however, was not satisfied with this construction. For one thing, he seemed not even entirely convinced that the field constructed by Weber and Fricke really was the Hilbert class field over Ω, writing,

> In the tables at the end of the algebra volumes III of Weber and Fricke the equations $f_W(\theta_W) = 0$ and $f_F(\theta_F) = 0$ are indicated as "class equations" for the discriminant -47. From the developments in the text however it is not entirely clear whether these equations actually generate the absolute class field N/Ω; for they are derived from the transformation theory of modular functions of *higher* level, whereas the class field construction is carried out only with modular functions of the *first* level. [25]

For another thing, as must come as no surprise to us by now, Hasse was dissatisfied with the transcendental methods that were used to construct the field. He felt that this construction provided no true insight into the structure of the field, writing,

> Whereas it is easy in the cases $d = -23$ and $d = -31$ to give an explicit arithmetic-canonical presentation of the so defined number field K of degree $h = 3$, the same problem in the case $d = -47$, where K has degree 5, has until now been solved only through equations flowing from the transformation theory of modular functions (so-called modular equations), so that the arithmetical nature of the roots in the class field N remains in the dark. [26]

---

[25] (Hasse and Liang 1969, p. 94): *In den Tabellen am Schluß der Algebrabände III von Weber und Fricke werden die Gleichungen $f_W(\theta_W) = 0$ und $f_F(\theta_F) = 0$ zwar als "Klassengleichungen" für die Diskriminante -47 bezeichnet. Aus den Ausführungen im Text geht jedoch nicht mit voller Klarheit hervor, ob diese Gleichungen wirklich den absoluten Klassenkörper N/Ω erzeugen; denn sie werden aus der Transformationstheorie von Modulfunktionen* höherer *Stufe gewonnen, während die Klassenkörperkonstruktion nur mit Modulfunktionen* erster *Stufe durchgeführt wird.*

[26] (Hasse 1964, pp. 419-420): *Während es in den beiden Fällen $d = -23$ und $d = -31$ leicht ist, den so definierten Zahlkörper K vom Grade $h = 3$ explizit in einer arithmetisch-kanonischen Erzeugung anzugeben, ist diese Aufgabe im Falle $d = -47$ wo K den Grad 5 hat, bisher nur durch aus der Transformationstheorie der*

Years later, recalling the work in a letter of 1975 to Taussky, and thus perhaps more candidly, he wrote that Weber's generating equation lacked transparency, that "one can hardly call it 'canonical' ", and that it "says as good as nothing about the class field in question". He added that in place of this he strove for a construction by radicals. [27] For Hasse, the goal was not just to arrive at a polynomial whose root generated the field, as Weber and Fricke had done, but to construct the field in a way which he called *arithmetic* and *canonical* (*"arithmetisch-kanonisch"*).

Just as in the case of the class number formula, as Hasse considered it in the introduction to KAZ (see page 137), the result derived by transcendental methods was correct but failed to give structural insight into the object at hand. For Hasse, a field generator should be built as an algebraic function of numbers of arithmetic significance, such as fundamental units and their conjugates, field extension degrees, or primes dividing discriminants of relevant number fields. This is precisely what we will see him do in the work we review in this section.

As he explained in the introduction to his work (Hasse 1964) on the Hilbert class field over $\mathbb{Q}(\sqrt{-47})$, it was already known how to give such an *arithmetisch-kanonisch* construction of the Hilbert class fields over the fields $\mathbb{Q}(\sqrt{d})$ with $d = -23$ and $d = -31$, and Hasse's plan for the paper was to first demonstrate such a construction in order to set the example of what he sought to do for $\mathbb{Q}(\sqrt{-47})$, and then to attempt the same for this latter field.

In order to review Hasse's work, we start by introducing his notation. We also provide an English translation of his paper (ibid.) in Appendix B. In general (see Figure 6.3) the problem will be to construct the Hilbert class field N over the imaginary quadratic field $\Omega = \mathbb{Q}(\sqrt{d})$ with class number h, where d is some negative integer. K will denote the maximal real subfield of N. In general, for any field E, E_0 will denote its maximal real subfield, and E^h will denote the field $E(\rho)$, where ρ is a primitive h^{th} root of unity. [28]

Furthermore, let us recall *singular primary numbers*, which we introduced in Section 3.2.

Modulfunktionen fließende Gleichungen (sogen. Modulargleichungen) gelöst, wobei die arithmetische Natur der Wurzeln innerhalb des Klassenkörpers N im Dunkeln bleibt.

[27] Hasse wrote: *Die in Webers Algebra III angegebenen Konstruktionen, die nur einfach ein numerisch recht undurchsichtige erzeugende Gleichung mitteilen, kann man wohl kaum als "kanonisch" bezeichnen. Sie sagen einem so gut wie nichts über den betr.Klassenkörper. Stattdessen strebte ich eine Radikalerzeugung an.*

[28] These letters are the same ones that Hasse used, with the sole exception that we write $\mathbb{Q}$ for the rational number field, whereas he used P.

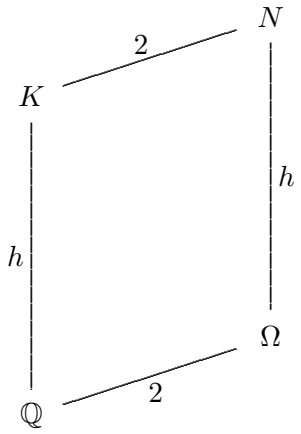

Figure 6.3: Field lattice for Hasse's problem.

Given a field k, Furtwängler constructed the Hilbert class field K of prime degree ℓ over k in the form $k(\sqrt[\ell]{\omega})$, where ω was a singular primary number. For this to work, however, k had to already contain the ℓ^{th} roots of unity. Hasse relied on precisely this same construction.

Ultimately, Hasse found an element θ such that both $N = \Omega(\theta)$, and $K = \mathbb{Q}(\theta)$, and in fact whereas nominally the task is referred to as the problem of constructing the Hilbert class field N over Ω, the actual tactics that Hasse employs work by thinking of it as a construction of K, the maximal real subfield of that class field, over $\mathbb{Q}$. We will see this, for example, in his construction of the generator θ as a value of the trace function $T_{N_0^h|K}$ from N_0^h down to K. He is therefore thinking of θ as an element of K.

The basic strategy that Hasse follows, both for the "exemplar cases" $d = -23$ and $d = -31$, and for the "challenge case" of $d = -47$, is as follows:

1. Find a singular primary number ω in Ω^h, thus constructing N^h as $\Omega^h(\sqrt[h]{\omega})$. The number ω is found using methods from (Hasse 1950a) and KAZ, which require computation of fundamental units and class numbers of Ω_0^h and Ω^h.

2. The element ω of Ω^h must be *normalized* so that it lies in the real subfield Ω_0^h. Here "normalization", as in many contexts, means choosing one representative that is in some way "best", from among a collection of objects which are in some way equivalent. In this case, if ω is a singular primary number, then consider that it is only determined up to generating the appropriate field $\Omega^h(\sqrt[h]{\omega})$, where h is prime. Clearly then, any

other number

$$\omega_0 = \omega^\mu \alpha^h$$

with $\mu \not\equiv 0 \bmod h$ and α a nonzero element of Ω^h would construct the same field, and is equivalent to ω in this sense. Normalization of ω therefore means raising it to a power that is nonzero mod h, and/or multiplying it by an h^{th} power in such a way that the resulting number lies in Ω_0^h.

3. Finally, from the generator $\sqrt[h]{\omega}$ of N^h over Ω^h, we must obtain a generator θ of K over $\mathbb{Q}$. In general, Hasse achieves this using trace functions. For example, if the normalized singular primary number ω_0 lies in N_0^h, then he might apply the trace from N_0^h down to K, so that

$$\theta = T_{N_0^h|K}(\sqrt[h]{\omega_0}).$$

In order to understand what sort of *"arithmetisch-kanonisch"* construction Hasse had in mind, we consider now his results, beginning with the cases $d = -23$ and $d = -31$, which he handles simultaneously by simply assuming $d = -27 \pm 4$. Here the field $\mathbb{Q}(\sqrt{d})$ has class number $h = 3$, and Hasse constructs $K = \mathbb{Q}(\theta)$ where θ satisfies the irreducible equation

$$\theta^3 \mp \theta - 1 = 0 \tag{6.1}$$

and is given "arithmetically" by

$$\theta = \sqrt[3]{\frac{\alpha}{9}} + \sqrt[3]{\frac{\alpha'}{9}}, \tag{6.2}$$

where

$$\alpha = \frac{9 + \sqrt{-3d}}{2}.$$

Here the "prime" notation on α denotes the application of that automorphism of $N^3 = K(\sqrt{-3}, \sqrt{d})$ that fixes K and $\sqrt{d}$, and carries $\sqrt{-3}$ to $-\sqrt{-3}$. In order to substantiate the "arithmetic" nature of this characterization, Hasse is satisfied to observe that the radicand $\alpha/9$ is related to the fundamental unit

$$\varepsilon_0 = \frac{(27 \mp 2) + e\sqrt{-3d}}{2}$$

of the field Ω_0^3 and to the prime number 3 by the equations:

$$\frac{\alpha}{\alpha'} = \pm\varepsilon_0 \qquad\qquad \alpha\alpha' = \pm 3. \tag{6.3}$$

Hasse's language does make sense. If arithmetic is all about understanding the numbers in a field as products of powers of units and primes (ideal primes, as need be), then a generating element θ constructed as an algebraic function (note $\alpha = \sqrt{3\varepsilon_0}$) of units and relevant primes (the prime 3 in this case being highly relevant, as the class number of the field Ω), can surely be called "arithmetically characterized". Over and above the constructions of Weber and Fricke by relatively unrelated transcendental methods, it is easy to imagine how a construction such as this arithmetic one could lead to more immediate insight into the nature of algebraic number fields underlying the class field construction. This seems to have been Hasse's motivation.

In the second half of the paper, Hasse goes on to attempt the same sort of construction now for $d = -47$, for which $h = 5$. In fact, 47 is the smallest prime p for which $\mathbb{Q}(\sqrt{-p})$ has class number divisible by 5, as Hasse notes in the introduction to the paper. As also noted there, the work proves substantially more complex in this case. To begin with, Hasse must construct more fundamental units and class numbers than he did the first time, in order to find the singular primary number ω.

Not only that, but computing one of these units involves an extremely heavy computation, namely the expansion of a product of 23 binomial factors. For this Hasse used an electronic computer at the University of Hamburg, called the Hamburg TR4. The TR4 was a model of computer produced in Germany by the Siemens corporation. Before moving on, we devote the next section to an examination of this aspect of the work in a little more detail.

6.3.2 Computing by machine and by hand

Hasse was in fact already using computers at least by 1964. In order to compute the class number h_0 of Ω_0^5, according to a technique covered in (Hasse 1950a) and using something called the Bergström product formula, he needed to expand the product

$$\theta = \prod_a \left((-\zeta)^a - (-\zeta)^{-a}\right)$$

in which ζ was a primitive $5 \cdot 47^{\text{th}}$ root of unity, and in which a ran over a system of 23 residues mod $5 \cdot 47$ (the number of residues, as given in (ibid., p. 54), is $\frac{1}{2}\frac{\varphi(f)}{m}$, where f is

the modulus $5 \cdot 47$ and m is the degree of the field, in this case $m = 4$):

$$1, 19, 21, 29, 39, 51, 61, 69, 71, 81, 99, 101, 109,$$
$$111, 121, 129, 131, 139, 179, 191, 199, 219, 229$$

This would then yield a certain unit η_0, itself used in determining the class number h_0. As Hasse wrote,

> I would not have succeeded in carrying this out without mechanical or electronic aid to computation. By means of the Hamburg electronic computer TR 4 was found the agreement [29]
>
> $$\eta_0 = \frac{1}{2}\left(\frac{47 - 5\sqrt{5}}{2} + \frac{-5 + \sqrt{5}}{2}\sqrt{-e\sqrt{5} \cdot d}\right) = \varepsilon_0$$
>
> with the afore-determined relative fundamental unit ε_0. [30]

In contrast, another computation arising in this study was deemed by Hasse "indeed somewhat troublesome, but entirely to be accomplished by hand". [31] He thanked Klaus Alber (his former PhD student of 1959) for carrying out the work. The task was to determine the minimal polynomial for the number

$$A = \left(\sqrt[5]{\omega} - \frac{1}{\sqrt[5]{\omega}}\right) - \left(\frac{\sqrt[5]{\omega}^2}{\varepsilon_0} - \frac{\varepsilon_0}{\sqrt[5]{\omega}^2}\right)$$

and the tactic was to expand out the powers A^2, A^3, A^4, and A^5 of the above expression, writing the results as linear combinations over the basis

$$\sqrt[5]{\omega}^{-2},\ \sqrt[5]{\omega}^{-1},\ 1,\ \sqrt[5]{\omega},\ \sqrt[5]{\omega^2}.$$

Since it was known that A had to satisfy an equation of degree 5, the homogeneous linear system on the coefficients of these basis representations then only needed to be solved.

It makes some comment on the availability of computers and the ease of doing symbolic computation on them at this time, that this problem was deemed suitable for solving by

---

[29] Note that earlier in the paper Hasse defined $e = (1 + \sqrt{5})/2$.

[30] (Hasse 1964, pp. 428-429): *Die Durchführung wäre mir ohne mechanische oder elektronische Rechenhilfsmittel wohl nicht gelungen. Mittels des Hamburger elektronischen Rechenautomaten TR 4 ergab sich die Übereinstimmung ... mit der zuvor bestimmten Relativgrundeinheit ε_0.*

[31] (ibid., p. 433): *zwar etwas mühevollen, aber durchaus von Hand zu erledigenden.*

hand, even while Hasse had a computer available to him. While the expansion of the Bergström product with its 2^{23} terms absolutely required a high speed computing machine, this job given to Alber was less trouble, or perhaps only less financial cost, to have done by hand than to have run on a machine. This makes quite a contrast with our present day situation, in which the necessary symbolic computation facilities are ready at hand in standard computer algebra systems.

6.3.3 The second class field construction

Returning to the case $d = -47$, this time Hasse constructs $K = \mathbb{Q}(\theta)$ where θ satisfies the irreducible equation

$$\theta^5 + 10\theta^3 - 235\theta^2 + 2610\theta - 9353 = 0 \tag{6.4}$$

and is given "arithmetically" by

$$\theta = \sqrt[5]{\omega} + \sqrt[5]{\omega'} + \sqrt[5]{\omega''} + \sqrt[5]{\omega'''} \tag{6.5}$$

where the radicand ω, which in this case is simply the singular primary number found in Ω^5, is related to the fundamental unit ε_0 of Ω_0^5 (given in the middle of page 209), by

$$\omega = \varepsilon_0^2 \varepsilon_0'.$$

As before, the "prime" notation denotes application of one of the automorphisms of the field N^5. And once again, this is clearly a satisfactorily *arithmetic* construction.

Hasse however remained dissatisfied with what he considered the excessive height of the irreducible equation (6.4). (the height refers to the maximum of the absolute values of the coefficients), referring to it as *unverhältnismäßig hohe*: "disproportionately high". [32]

Here again we see Hasse exhibiting the mathematician's intuition that the somewhat "ugly" construction (the polynomial with excessively high coefficients) was perhaps the "wrong" one. He wondered whether by normalizing the singular primary number ω in a different way he might be able to lower the height of the equation. He wondered also whether in doing this he would wind up with Weber's or Fricke's equation. He closed the paper by saying that these questions remained for a further investigation.

[32] (Hasse 1964, p. 434)

6.3.4 Setting problems for Zassenhaus and Liang

As Hasse explains in (Hasse and Liang 1969), his construction of the Hilbert class field over $\Omega = \mathbb{Q}(\sqrt{-47})$ is based on a one-to-one correspondence between on the one side generations

$$K = \mathbb{Q}(\theta), \quad N = \Omega(\theta) \tag{6.6}$$

by the one real root θ of a suitable irreducible polynomial $f(x)$ of degree 5 over $\mathbb{Q}$, and on the other side the generation

$$N^5 = \Omega^5(\sqrt[5]{\omega}) \tag{6.7}$$

by a singular primary number. This one-to-one correspondence, moreover, is mediated by something called the *Lagrange radical*, defined by

$$L = \sum_{\mu \bmod 5} \rho^{-\mu} \theta^{R\mu},$$

where ρ is a primitive 5^{th} root of unity, and R is a generating automorphism for the Galois group of N over Ω. Namely, if θ satisfies (6.6), then

$$\omega = L^5$$

is the desired singular primary number in (6.7), which in fact lies in Ω_0^5. If, conversely, $\omega \in \Omega_0^5$ satisfying (6.7) is given, then θ satisfying (6.6) can be obtained as

$$\theta = \frac{1}{5}\left(a + T_{N_0^5|K}(\sqrt[5]{\omega}),\right) \tag{6.8}$$

where a is an arbitrary rational number. All this is explained by Hasse. [33]

Returning now to Hasse's goal of comparing his own construction of the Hilbert class field over $\mathbb{Q}(\sqrt{-47})$ with the constructions of Weber and Fricke, let us introduce notation. The polynomial in (6.4) will be called f_H, its real root (6.5) will be called θ_H, and the singular primary number ω used in the construction will be called ω_H. Corresponding entities for Weber resp. Fricke will be denoted f_W, θ_W, ω_W, resp. f_F, θ_F, ω_F.

The equations f_W and f_F, as we noted earlier, were given by Weber and Fricke as

$$f_W = x^5 - x^3 - 2x^2 - 2x - 1,$$

[33](Hasse and Liang 1969, pp. 90-91). Whereas Liang was responsible for some of the results in the paper, it was written by Hasse. See page 222.

$$f_F = x^5 - x^4 + x^3 + x^2 - 2x + 1.$$

As for θ_W and θ_F, these simply denote real roots of these equations, whereas ω_W and ω_F were not actually given yet, but Hasse wanted to compute them.

Toward these ends, Hasse asked Zassenhaus and Liang to solve two problems (Hasse and Liang 1969; Zassenhaus and Liang 1969):

1. To confirm that θ_H, θ_W, θ_F generate the same field by expressing them rationally in terms of each other. In particular, they should be expressible as polynomials of degree less than 5 in each other, say θ_H in terms of θ_W, and θ_W in terms of θ_F.

2. To find a generating element R of the Galois group of N over Ω, that is, to compute the action of R on the generators θ_H, θ_W, θ_F by writing θ_H^R, θ_W^R, θ_F^R as polynomials of degree less than 5 over Ω in, resp. θ_H, θ_W, θ_F (or perhaps in a fixed generator, say θ_W).

The purpose of the second task was that then ω_W and ω_F could be computed via the Lagrange radical, and one could "further reveal the arithmetic relationship between the radicands ω_H, ω_W, ω_F" (*"ferner den arithmetischen Zusammenhang zwischen den Radikanden ω_H, ω_W, ω_F aufdecken"* (Hasse and Liang 1969, p. 94)). Namely, for this "arithmetic relationship" Hasse sought to represent each of ω_W and ω_F in the form

$$\omega_H^{S^\nu} \eta_0^5 \tag{6.9}$$

where S is a generating automorphism of the Galois group of N^5/N, ν is a least positive residue mod 4, and $\eta_0 \in \Omega_0^5$ is a unit. Ultimately, Zassenhaus and Liang would solve all of these problems by numerical p-adic methods.

6.3.5 Solutions found

A letter of 31 August 1968 from Zassenhaus to Hasse suggests that, if indeed Hasse mentioned these problems to Zassenhaus and Liang while visiting OSU, then the two must have set to work on them right away, mentioning "several months" (*"mehrere Monate"*) of work at a time only about five months after Hasse's visit had ended:

> Mr. Liang and I have worked already several months on the problem you put, to compute the automorphisms of the Hilbert class field of

> $\mathbb{Q}(\sqrt{-47})$. The computation itself naturally involves no notable difficulties, it is the methodology. Leopold and a student of his sent me recently a communication, that they have found the first equation of degree 7 over the rational number field with the 168-group; very nice and interesting! [34]

The statement comparing "the computation itself" (*"die Rechnung selbst"*) to "the methodology" (*"die Methodik"*) is interesting. It seems to mean that, whereas any necessary computations could easily be carried out quickly enough by the IBM 7094 that was on hand at OSU (the model is mentioned in later letters), the real challenge was something to do with the methods. But *what* to do with the methods? Was the difficulty in developing the necessary data structures to represent whatever methods they intended to apply? Or was the challenge simply to choose the right methods themselves?

As for Leopoldt, this student of Hasse was brought directly into computational work, beginning advisement by Hasse shortly after the end of the war. [35] Although we cannot give adequate time to him, a thorough look at his work would be a valuable part of a study such as ours, on the origins of practical computation in algebraic number theory. Instead we simply observe here that the communication from Leopoldt to Zassenhaus helps to demonstrate the emergence of a community of mathematicians working on this subject around this time.

In any case, a solution was right around the corner. Zassenhaus and Liang sent Hasse a postcard five days later, on 5 September 1968, announcing the solution to some, but not all, of Hasse's questions. The handwriting looks hurried, giving the postcard the appearance of having been dashed off in a moment of excitement at the discovery of a solution. Disappointingly however, the card is stamped "return to sender," Hasse having already moved on from the University of Washington math department to which it was addressed. Hasse was officially retired by this time, and somewhat itinerant. The message did of course eventually reach him. The postcard read as follows. Here, Zassenhaus and Liang use K for the Hilbert class field over $k = \mathbb{Q}(\sqrt{-47})$, and E for its maximal real subfield. They use ω for the

[34] *Herr Liang und ich arbeiten schon mehrere Monate an der von Ihnen gestellten Aufgabe, die Automorphismen des Hilbertklassen-körpers von $\mathbb{Q}(\sqrt{-47})$ zu berechnen. Die Rechnung selbst bereitet natürlich keine nennenswerte Schwierigkeiten, es ist die Methodik. Leopold und ein Schüler von ihm schickten mir drage neulich eine Mitteilung, dass sie die erste Gleichung 7.Grades über dem rational Zahlenkörper mit der 168-Gruppe gefunden haben, sehr schön und interessant!*

[35] (Leopoldt 1973)

element $\left(1+\sqrt{-47}\right)/2$ of the natural integral basis $\{1,\omega\}$ for k.

> Dear Professor Hasse:
>
> Finally J. Liang succeeded in translating the p-adic method to answer your first questions: The 3 equations:
>
> $f_H = x^5 + 10x^3 - 235x^2 + 2610x - 93353$
> $f_W = x^5 - x^3 - 2x^2 - 2x - 1$
> $f_F = x^5 - x^4 + x^3 + x^2 - 2x + 1$
> of discriminant: H: $47^2 \times 5^2 \times 11^2$, W & F: 47^2
> have solutions θ_H, θ_W, θ_F generating the same finite extensions E of $\mathbb{Q}$, K of $\mathbb{Q}(\sqrt{-47})$ with the following results: The automorphism σ of K which is the Frobenius substitution for $(2, \frac{1+\sqrt{-47}}{2})$ over $\mathbb{Q}(\sqrt{-47})$ carries θ_W into:
> $\frac{1}{47}\left((-56+18\omega)\theta_W^4 + (30-153\omega)\theta_W^3 + (55-16\omega)\theta_W^2 + (58-22\omega)\theta_W + 54 - 14\omega\right)$
> and θ_F into:
> $\frac{1}{47}\left((-44-6\omega)\theta_F^4 + (22+3\omega)\theta_F^3 + (-21-5\omega)\theta_F^2 + (-72+3\omega)\theta_F + 68 + 5\omega\right)$
>
> Best regards Yours sincerely
> Joseph Liang H. Zassenhaus

Here again the meaning of the talk of methods is a little unclear, and we must wonder about the origin of the ideas. Zassenhaus wrote that Liang had "succeeded in translating the p-adic method". What could be the possible significance of this statement? Did it mean that Liang decided to try to bring known p-adic methods to bear on this problem, and succeeded in finding a way to apply them? Did it mean that the three were already aware that p-adic methods would be attempted, and Liang succeeded in translating them into data structures and algorithms on the machine? If p-adic methods were discussed while Hasse was at OSU, who suggested them?

Hasse's well known role as champion of the p-adics may lead us to wonder whether it might have been he who suggested the idea of applying p-adic methods to this problem. However, there was a short note from Zassenhaus to Hasse on 15 October 1968, attributing at least part of the methods to Liang:

> [illeg. ''Enclosed''?] find worked out the result of our [illeg.] computation, and also a remark on the methods of Mr. Liang. Perhaps

> you can give further questions? Many thanks for your postcard, which of course made us happy.

Meanwhile, a later note from Liang to Hasse, sent after not just the first but all of Hasse's questions had been solved, attributed a p-adic method to Zassenhaus:

> Dear Professor Hasse:
>
> By using the p-adic method suggested by Prof. Zassenhaus and with the help of the IBM Computer 7094, we finally succeeded in solving all the questions you presented to us on these three equations.

In addition, in (Hasse and Liang 1969, p. 95) Hasse described the method developed by Zassenhaus and Liang in (Zassenhaus and Liang 1969) as "based on" (*"gestützt auf"*) "a p-adic method developed by Zassenhaus", citing Zassenhaus's then very recent paper on the Hensel factorization algorithm (Zassenhaus 1969).

Returning to the solutions found by Zassenhaus and Liang, Hasse felt that the polynomials showing the action of the automorphism R should be written with respect to the integral basis $\left\{1, \sqrt{-47}\right\}$ instead of the basis $\{1, \omega\}$. In his own paper with Liang he would rewrite them in this form, giving, for example,

$$\theta_H^R = \frac{1}{47}\left(-2\sqrt{-47} + \frac{-47-11\sqrt{-47}}{2}\theta_W + 7\sqrt{-47}\theta_W^2 + \frac{-47-3\sqrt{-47}}{2}\theta_W^3 + \frac{47+\sqrt{-47}}{2}\theta_W^4\right)$$

and adding the interesting comment,

> Here the numbers of Ω are represented through the organic basis $1, \sqrt{-47}$ (Gauss sums) instead of $1, \frac{1+\sqrt{-47}}{2}$ in (Zassenhaus and Liang 1969). Only then emerges an arithmetic relation to the discriminant -47: all first coordinates are divisible by -47, and thus all θ-coefficients by $\sqrt{-47}$, so that the denominator 47 at the front is partially compensated. [36]

This is a prime example of the way in which Hasse sought to reveal arithmetic relations by representing things in the right way, and moreover of the way in which having a numerical example to play with could allow such revelations.

---

[36] (Hasse and Liang 1969, p. 95): *Hier sind die Zahlen aus* Ω *durch die organische Basis* $1, \sqrt{-47}$ *(Gaußsche Summen) statt* $1, \frac{1+\sqrt{-47}}{2}$ *in [2] dargestellt. Erst dann tritt eine arithmetische Beziehung zur Diskriminante* -47 *hervor: sämtliche erste Koordinaten sind durch* -47*, also sämtliche* θ*-Koeffizienten durch* $\sqrt{-47}$ *teilbar, so daß der voranstehende Nenner* 47 *teilweise kompensiert wird.*

With these two problems solved, Hasse then turned to the third problem, on the relation between the radicands ω_H, ω_W, ω_F. In a letter of 9 October 1968 he wrote to Liang to express his satisfaction with the results so far, but to add that this last problem had to be solved as well before they could coauthor a paper extending the 1964 paper of Hasse that first embarked on these problems. Namely, Hasse indicated the problem of computing the representations of ω_W and ω_F in the form (6.9). He elaborated, furthermore, that the unit η_0 would in the case of ω_F take the form

$$e^a \varepsilon_0^b \varepsilon_0'^c$$

and in the case of ω_W the form

$$\theta^a \theta'^b \theta''^c$$

where e, ε_0, and θ denoted three particular units which Hasse had computed before, and the "prime" notation as usual meant the application of the automorphism S. The question put to Liang then was to determine the necessary ν, a, b, and c. Hasse closed with,

> I should be very grateful if you could give your consideration to these further numerical questions. They are of quite a different type, though, from the type of the former questions, because here multiplicative representations by a unit basis are to be handled. [37]

We should note as well that at least by this time, possibly even sooner, Hasse had already found the right way to lower the excessive height of the equation (6.4), namely, by a linear transformation of the generator θ_H to $(\theta_H + 2)/5$, in which he took advantage of the Lagrange radical correspondence in (6.8) by taking the arbitrary additive rational $a = 2$. The resulting equation

$$x^5 - 2x^4 + 2x^3 - 3x^2 + 6x - 5 = 0$$

(it appears in (Hasse and Liang 1969)) was not, after all, the same as either of the equations f_W, f_F of Weber and Fricke, but was substantially lowered in height, to be on par with those. To be precise, if $h(\theta)$ is the polynomial in (6.4), and $g(\theta)$ the new, lower one, then the substitution $\theta_H \mapsto (\theta_H + 2)/5$ that Hasse mentions satisfies

$$5^5 g\left(\frac{\theta + 2}{5}\right) = h(\theta).$$

[37] Hasse wrote in English.

While Liang set to work on the final challenge, meanwhile Zassenhaus sent the first draft manuscript of (Zassenhaus and Liang 1969) to Hasse, who replied with a critique on 17 October 1968. In his reply Hasse maintained his commitment to the divisor-theoretic view that he inherited from Kronecker and Hensel, while at the same time acknowledging that it was less well-known, and that non-experts would need more verbose clarifications than the coauthors Zassenhaus and Liang had supplied so far. Thus, he began:

> Dear Mr. Zassenhaus,
>
> Heartfelt thanks for the sending of the manuscript of your work with Mr. Liang on my problem. I have delved into it, and understood well the train of thought and calculations. I fear however that in some places you are too terse with words, for those not so familiar with the p-adics to understand the matter in all details. Moreover I find in the reading some inelegance and inconsistencies in the mathematical notations, which you should eliminate before going to press. I put these critical remarks of mine together for you below. [38]

Elaborating, he wrote, for example,

> P. 5. The reader unversed in p-adics must miss here a reason for this, that one puts the characteristic b casually introduced on p. 1 into the denominator. [39]

Lower down in the letter, Hasse objected to the use of the ideal-theoretic equation $P_i = p_i O_K$. In the Dedekind-Hilbert theory, this is the way of indicating that P_i is the ideal in K lying over p_i. It says that P_i is obtained as the set of all linear combinations of elements in p_i with coefficients from the ring of integers O_K of the field K. To Hasse, who of course subscribed wholeheartedly to the Kronecker-Hensel theory of divisors, P_i and p_i were really the same object, and as such ought to be "identified". As we see below, his

[38] *Herzlichen Dank für die Zusendung des Manuskripts Ihrer Arbeit mit Herrn Liang über mein Problem. Ich habe mich gleich darein vertieft und die Gedankenführung und Rechnungen gut verstanden. Ich fürchte aber doch, dass Sie an einigen Stellen zu knapp mit Worten sind, als dass auch mit der p-adik nicht so vertraute die Sache bis ins Letzte verstehen können. Darüber hinaus finde ich beim Durchlesen einige Unschönheiten und Inkonsequenzen in der mathematischen Ausdrucksweise, die Sie vor der Drucklegung beseitigen sollten. Ich stelle Ihnen diese meinen kritischen Bemerkungen nachstehend zusammen.*

[39] *S. 5. Der in der p-adik unerfahrene Leser muss hier eine Begründung dafür vermissen, dass man die auf S.1 beiläufig eingeführte Charakteristik b in den Nenner hineinmanövriert.*

characterization of the theory of divisors as "the later theory" shows that he truly believed it to have succeeded and replaced the theory of ideals:

> Incidentally I find less beautiful the notation $P_i = p_i O_K$ (p. 1, line 6 from bottom). For this recalls a point which one should have left behind long ago, where the ''prime ideals'' would be defined as sets of numbers. In the later theory they are simply things of the same kind as numbers, with which one computes, and their interpretation as sets formed of infinitely many numbers only disturbs; for the true *p-adiker* in any case, this set interpretation has never been available, for he has learned his algebraic number theory with divisors, following Kronecker-Hensel. You will reply that the difference between these structures does not find expression in the simultaneous consideration of various fields, if as here a prime ideal is completely inert. But Artin once said that mathematics would appear all too frightfully complicated, were one to precisely express everything logically and pedantically, and not make up one's mind to identify things which are (in the broadest sense!) isomorphic. [40]

Perhaps then we may count this as yet another reason why Hasse liked divisor theory better than ideal theory: that he felt it involved an essential simplification, that it was less pedantic. As for his talk of the "disturbing" infinite sets, if this is an echo of Kronecker it is surely only the faintest one. Hasse worked in his career with as many "infinite" objects as any other mathematician, and his objection here could only have been to needless complexity.

Besides these points, Hasse touched in his critique on many issues of notation, demonstrating his meticulousness and care for clear expression. For one thing, he urged use of the traditional exponential notation for the application of automorphisms; it would turn

[40] *Wenig schön finde ich übrigens auch die Bezeichnung $P_i = p_i O_K$ (S.1,Z.6 v.u.). Denn sie erinnert an einer Stelle, wo man längst darüber hinweg sein sollte, daran, dass die "Primideale" als Zahlmengen definiert wurden. In der späteren Theorie einfach sind sie doch Dinge vom gleichen Typus wie Zahlen, mit denen man rechnet, und ihre Bedeutung als aus unendlich vielen Zahlen aufgebaute Mengen stört nur; für den p-adiker echten Stils ist diese Mengenbedeutung sowieso nie vorhanden gewesen, weil der seine algebraische Zahlentheorie nach Kronecker-Hensel mit Divisoren gelernt hat. Sie werden entgegnen, dass ja dann der Unterschied zwischen diesen Gebilden bei simultaner Betrachtung verschiedener Körper nicht zum Ausdruck kommt, wenn wie hier ein Primideal voll-träge ist. Aber Artin hat einmal gesagt, dass die Mathematik ganz fürchterlich kompliziert aussehen würde, wollte man alles logisch pedantisch genau ausdrücken und sich nicht entschliessen, isomorphes (im weitesten Sinne!) zu identifizieren.*

out that this was the only suggestion of Hasse's that Zassenhaus and Liang did not accept. For another example, Hasse objected to the parenthetical notation for moduli, preferring " mod m" to "(m)":

> It recalls much too much a multiplication; consider however, in how many _different_ senses mathematicians use _one and the same_ sign (...). One should guard oneself from increasing further this ambiguity! [41]

On 28 October 1968 Zassenhaus replied to say that almost all of the suggested changes to the manuscript were made, and that Liang was working on Hasse's new problem, applying p-adic logarithms to it.

In a letter of 10 November 1968 to Zassenhaus, Hasse agreed that p-adic logarithms were the natural tool here, "as generally in numerical investigations on units in algebraic number fields". [42]

At the same time, Hasse was busy with other work. For one thing, he was preparing a paper on another topic for the Journal of Number Theory, which he discussed in this letter with the senior editor Zassenhaus. For another, he asked a computational job of Zassenhaus and Liang, to generate examples for another project. We copy Hasse's description of the computational problem below for further insight into the sort of number theoretic problems which he sought in this era to support by computed evidence. Let us recall meanwhile that Hasse had retired two years earlier in 1966, and may these examples illustrate clearly that he remained very active afterward. He wrote:

> In my studies on the divisibility of the class number of quadratic number fields by powers of 2, I need a numerical example, which after some flailing attempts I recognized as too difficult for hand computation. Perhaps you or Mr. Liang could also help me here with your computer. I would like to formulate it for you below, along with the easy reduction to finitely many tests.

---

[41] *Sie erinnert vielzusehr an eine Multiplikation; bedenken Sie doch, in wie viel _verschiedenen_ Sinnen der Mathematiker _ein und dasselbe_ Zeichen (...) benutzt. Man sollte sich hüten, diese Vieldeutigkeit noch zu steigern!*

[42] *Die Benutzung der p-adischen Logarithmen ist hier, wie überhaupt bei numerischen Untersuchungen über Einheiten in algebraischen Zahlkörpern, das naturgemässe Hilfsmittel.*

I seek two prime numbers $p, q \equiv 1 \mod 4$ with $\left(\frac{p}{q}\right) = 1$, and then by the reciprocity law also $\left(\frac{q}{p}\right) = 1$, and with the property that the two equations

$$px^2 - qy^2 = \pm 4$$

are rationally solvable.

Reduction to finitely many tests (see my blue *Zahlentheorie*, 2nd ed., p. 556):

Let $d = pq$, and let u, v be the least positive solution of $u^2 - dv^2 = 4$, so that $e = \frac{u \pm v\sqrt{d}}{2}$ is the norm-positive fundamental unit of the field of $\sqrt{d}$. If one then writes the two equations in the form

$$(px_1)^2 - dy_1^2 = 4p \qquad \text{resp.} \qquad (qy_2)^2 - dx_2^2 = 4q$$

or thus

$$p = N(a_1) \text{ with } a_1 = \frac{px_1 + y_1\sqrt{d}}{2} \quad \text{resp.} \quad q = N(a_2) \text{ with } a_2 = \frac{qy_2 + x_2\sqrt{d}}{2},$$

then a_1, a_2 can be, by multiplication with powers of e, reduced into the intervals

$$1 < a_1 < e \qquad \text{resp.} \qquad 1 < a_2 < e.$$

That means for

$$y_1 = \frac{a_1 - a_1'}{\sqrt{d}} \qquad \text{resp.} \qquad x_2 = \frac{a_2 - a_2'}{\sqrt{d}}$$

the inequalities

$$-\frac{p-1}{\sqrt{d}} < y_1 < \frac{e - \frac{p}{e}}{\sqrt{d}} \qquad \text{resp.} \qquad -\frac{q-1}{\sqrt{d}} < x_2 < \frac{e - \frac{q}{e}}{\sqrt{d}}.$$

If in these intervals there is no integral solution x_1, y_1, resp. x_2, y_2, then there is altogether no solution.

I seek a smallest possible pair of primes of this kind. Already for the first four pairs (p, q) which are $\equiv 1 \mod 4$ and quadratic residues mod each other, namely $(5, 29)$, $(5, 41)$, $(5, 61)$, $(13, 17)$, I cannot myself

> carry out the necessary computations. I would be very thankful if you could help me with this. [43]

Just ten days later, on 20 November 1968, Hasse wrote to Zassenhaus enthusiastically to say that he had received Liang's solution to the final problems, and was now writing up the results:

> I received Mr. Liang's solution of the further question I raised about the class field of $\sqrt{-47}$. I am so happy about it, and now I am busy from morning to evening with a manuscript for the Acta Arithmetica which continues my paper on this field and shall be published with Liang and myself as co-authors. I write the paper in German because the first one was in German, but I shall send Liang a hand-written English copy of my proposed text. Please tell him all that. [44]

The paper (Hasse and Liang 1969) was received by the editors of *Acta Arithmetica* on 10 January 1969.

After this time, Hasse and Liang kept up correspondence for several years. At first, this consisted in the immediate continuation of their investigations, now moving to the class field construction over $\mathbb{Q}(\sqrt{-71})$, with $h = 7$. In reading their discussions it again is clear that Hasse actually made use of his works (Hasse 1950a) and KAZ as references on these computational problems.

Another interesting point arose after Liang had discussed computing certain fundamental units, and in Hasse's reply of 2 February 1969 he wrote,

---

[43] *Bei meinen Untersuchungen über die Teilbarkeit durch 2-Potenzen der Klassenzahl quadratischer Zahlkörper brauche ich ein Zahlenbeispiel, das ich nach einigen tastenden Versuchen als zu schwierig für Handrechnung erkannte. Vielleicht können Sie oder Herr Liang mir auch da mit Ihrem Computer helfen. Ich möchte es Ihnen nachstehend formulieren, zugleich mit der leicht möglichen Reduktion auf endlich viele Versuche. ... Ich suche zwei Primzahlen* $p, q \equiv 1 \bmod 4$ *mit* $\left(\frac{p}{q}\right) = 1$ *und dann nach dem Reziprozitätsgesetz auch* $\left(\frac{q}{p}\right) = 1$*, und mit der Eigenschaft, dass die beiden Gleichungen*

$$px^2 - qy^2 = \pm 4$$

ganzrational lösbar sind. ... Ich suche ein möglichst kleines Primzahlpaar dieser Art. Schon bei den ersten vier Paaren (p, q)*, die* $\equiv 1 \bmod 4$ *und gegen seitig quadratische Reste sind, nämlich bei* $(5, 29), (5, 41), (5, 61), (13, 17)$ *kann ich die nötigen Rechnungen nicht mehr selbst ausführen. Wenn Sie mir da helfen könnten wäre ich sehr dankbar.*

[44] Hasse wrote in English.

> It was one of the wise sayings of Artin's that, what you can define uniquely, you can also compute. And so I think that this paper may some day lead to a canonical way of finding a set of fundamental units.

Let us recall that the first paper of Zassenhaus, as noted by Pohst (see Table 6.1), on the computation of the group of units of a number field was published shortly hereafter in 1972. It would be interesting to investigate whether his results had any origins in ideas discussed by Hasse and Liang. This, however, must await another study.

6.3.6 The p-adic algorithm

The technique employed by Zassenhaus and Liang to compute the action of a generating automorphism σ of N over Ω was the p-adic Newton iteration which Hensel had used in Chapter 4 of TAZ, as we noted in Section 2.4.2. We review their method in this section.

In order to apply their technique, Zassenhaus and Liang needed two clever ideas: for one, if they were to perform $\mathfrak{P}$-adic lifting with $\mathfrak{P}$ a prime of N, then they needed a way to work computationally with such a prime; for another, they needed an initial approximation of the image $\sigma\theta$ of θ under σ modulo such a prime.

The way to find an initial approximation came out of Hilbert ramification theory. Let $G = \mathrm{Gal}(N|\Omega)$. If we pick a prime $\mathfrak{P}$ of N, its decomposition group $D_{\mathfrak{P}}$ will be a subgroup of G, and its Frobenius element $\varphi_{\mathfrak{P}}$ will generate the factor group $D_{\mathfrak{P}}/E_{\mathfrak{P}}$, where $E_{\mathfrak{P}}$ is the inertia group of $\mathfrak{P}$. So if we can pick $\mathfrak{P}$ so that $D_{\mathfrak{P}} = G$ and $E_{\mathfrak{P}} = \{1\}$, then $\varphi_{\mathfrak{P}}$ will be a generator of G, and we know its action mod $\mathfrak{P}$; namely, if we let $\sigma = \varphi_{\mathfrak{P}}$, then we have $\sigma\theta \equiv \theta^p \bmod \mathfrak{P}$.

But to have $D_{\mathfrak{P}} = G$ is just to have Ω be the decomposition field of $\mathfrak{P}$. This means that we want $\mathfrak{P}$ to lie over a rational prime p that splits completely in Ω and not in any intermediate field $\Omega \subsetneq L \subseteq N$. [45] As for $E_{\mathfrak{P}} = \{1\}$, this just means that we want p to stay unramified in N, and, given the first condition, this second condition will follow for free. For p must be unramified in Ω if it splits completely there, and N is unramified over Ω, being its Hilbert class field. Therefore it will be sufficient to find a prime p that factors as $\mathfrak{p}_1\mathfrak{p}_2$ in Ω, and such that both $\mathfrak{p}_i$ remain inert in N. In their paper, Zassenhaus and Liang note that the prime $p = 2$ works, for the case that Hasse asked them to work on.

[45] See corollary on p. 105 of (Marcus 1977).

As for the matter of working computationally with the primes $\mathfrak{P}_1$, $\mathfrak{P}_2$ of N lying over $\mathfrak{p}_1$, $\mathfrak{p}_2$, since they are unramified over p, it follows that one can simply compute power series in p itself, instead of power series in $\mathfrak{P}_i$.

Since there are two primes however, $\mathfrak{P}_1$ and $\mathfrak{P}_2$, it was necessary to combine results by Chinese remaindering. Namely, after computing approximations of $\sigma\theta$ modulo sufficiently high powers of both $\mathfrak{P}_1$ and $\mathfrak{P}_2$, Zassenhaus and Liang put the results together using the Chinese remainder theorem to get an approximation of $\sigma\theta$ modulo an equally high power of 2. Once this power was high enough, the exact value of $\sigma\theta$ was determined.

We now outline the algorithm.

In order to get started, we need to know the value of $\sigma\theta$ mod $\mathfrak{P}_1$ and mod $\mathfrak{P}_2$. Since we chose σ to be the Frobenius element of $\mathfrak{P}_1$, we know that

$$\sigma\theta \equiv \theta^p \bmod \mathfrak{P}_1.$$

Therefore we reduce x^p mod $f(x)$, giving a polynomial $\sigma_{1,0} \in \mathbb{Z}[x]$ and we have

$$\sigma_{1,0}(\theta) \equiv \sigma\theta \bmod \mathfrak{P}_1.$$

By an argument (Zassenhaus and Liang 1969, p. 516) which we omit here, we can compute another polynomial $\sigma_{2,0} \in \mathbb{Z}[x]$ such that

$$\sigma_{2,0}(\theta) \equiv \sigma\theta \bmod \mathfrak{P}_2.$$

Given this starting point, we now need to be able to lift p-adically. Zassenhaus and Liang actually used a quadratic lifting algorithm, i.e. one which takes an approximation mod $\mathfrak{P}_i^{2^k}$ and produces an approximation mod $\mathfrak{P}_i^{2^{k+1}}$. This however is somewhat more complex than a linear algorithm, i.e. one which takes an approximation mod $\mathfrak{P}_i^m$ and produces an approximation mod $\mathfrak{P}_i^{m+1}$, and so we will explain the linear version of the algorithm first, before explaining the quadratic version.

The steps of the linear algorithm are as follows.

Linear p-adic lifting algorithm

Input: $\sigma_{i,m}(x) \in \mathbb{Z}[x]$ such that

$$f(\sigma_{i,m}(\theta)) \equiv 0 \bmod \mathfrak{P}_i^m, \tag{6.10}$$

with $m \geq 1$.
Output: $\sigma_{i,m+1}(x) \in \mathbb{Z}[x]$ such that

$$f(\sigma_{i,m+1}(\theta)) \equiv 0 \bmod \mathfrak{P}_i^{m+1}.$$

1. Since $f(x)$ is irreducible, it is relatively prime to its derivative $f'(x)$. For use later in the algorithm, we use the Euclidean algorithm to compute polynomials $R(x), Q(x)$ such that
$$R(x)f(x) + Q(x)f'(x) = 1.$$

2. For the sake of simplicity, let $s(x) = \sigma_{i,m}(x)$. We will compute $g(x) \in \mathbb{Z}[x]$ such that
$$f(s(\theta) + g(\theta)p^m) \equiv 0 \bmod \mathfrak{P}_i^{m+1}.$$
Then $\sigma_{i,m+1}(x) = s(x) + g(x)p^m$ is the desired result.

3. We assume now the desired condition
$$f(s(\theta) + g(\theta)p^m) \equiv 0 \bmod \mathfrak{P}_i^{m+1} \tag{6.11}$$
and see if this will tell us what $g(x)$ should be.

4. According to Hensel's theory of divisors, (6.11) means there is some conjugate θ_0 of θ (dependent upon i) such that
$$f(s(\theta_0) + g(\theta_0)p^m) \equiv 0 \bmod p^{m+1}. \tag{6.12}$$
For simplicity, set $s_0 = s(\theta_0)$ and $g_0 = g(\theta_0)$.

5. An ordinary Taylor expansion says that for any y, h we have
$$f(y+h) = f(y) + f'(y)h + h^2(\cdots).$$
So with $y = s_0$, $h = g_0p^m$ we get
$$\begin{aligned} f(s_0 + g_0p^m) &= f(s_0) + f'(s_0)g_0p^m + g_0^2p^{2m}(\cdots) \\ f(s_0 + g_0p^m) &\equiv f(s_0) + f'(s_0)g_0p^m \bmod p^{m+1}. \end{aligned}$$
Then by (6.12) we have
$$f'(s_0)g_0p^m \equiv -f(s_0) \bmod p^{m+1}. \tag{6.13}$$

6. The assumption (6.10) on the input implies that

$$f(s_0) \equiv 0 \bmod p^m, \tag{6.14}$$

so applying the lemma at the end of this section to the function $F(x) = f(s(x))$, we get $F_1(x) \in \mathbb{Z}[x]$ such that $f(s_0) = p^m F_1(\theta_0)$. Then (6.13) becomes

$$f'(s_0)g_0 p^m \equiv -F_1(\theta_0)p^m \bmod p^{m+1}$$

which implies

$$\begin{aligned} f'(s_0)g_0 &\equiv -F_1(\theta_0) \bmod p \\ Q(s_0)f'(s_0)g_0 &\equiv -Q(s_0)F_1(\theta_0) \bmod p \\ (1 - R(s_0)f(s_0))\, g_0 &\equiv -Q(s_0)F_1(\theta_0) \bmod p \\ g_0 &\equiv -Q(s_0)F_1(\theta_0) \bmod p \end{aligned}$$

where in the last step we have used $f(s_0) \equiv 0 \bmod p$, which follows from (6.14).

7. Therefore, we compute

$$-Q(s(x))F_1(x),$$

reduce this mod $f(x)$ and mod p, and call the result $g(x)$. We can check that this $g(x)$ actually satisfies the desired condition. We set $\sigma_{i,m+1}(x) = \sigma_{i,m}(x) + g(x)p^m$, return this value, and halt.

The algorithm that Zassenhaus and Liang actually used achieved quadratic convergence instead of linear. The extra complication involved in this is that the inverse $Q(x)$ of $f'(x)$ mod p cannot be used as is on each iteration, but must be lifted to increasingly accurate approximations. In this quadratic procedure we get not just $\sigma_{i,j}(\theta) \equiv \sigma\theta \bmod \mathfrak{P}_i^j$, but

$$\sigma_{i,j}(\theta) \equiv \sigma\theta \bmod \mathfrak{P}_i^{2^j}.$$

Finally, the $\sigma_{i,j}$ are put together in a Chinese remaindering process. An element $e_0 \in \mathcal{O}_\Omega$ satisfying

$$e_0 \equiv 1 \bmod \mathfrak{p}_1, \qquad\qquad e_0 \equiv 0 \bmod \mathfrak{p}_2$$

is computed, and then with the clever recurrence relation

$$e_{i+1} = 3e_i^2 - 2e_i^3$$

$e_1, e_2, \ldots, e_\nu$ are computed so that in general

$$e_j \equiv 1 \bmod \mathfrak{p}_1^{2^j}, \qquad e_j \equiv 0 \bmod \mathfrak{p}_2^{2^j}.$$

Then defining

$$\Sigma_j = e_j\sigma_{1j}(\theta) + (1 - e_j)\sigma_{2j}(\theta)$$

for each j, we have

$$\Sigma_j \equiv \sigma_{1j}(\theta) \equiv \sigma(\theta) \bmod \mathfrak{P}_1^{2^j}$$
$$\Sigma_j \equiv \sigma_{2j}(\theta) \equiv \sigma(\theta) \bmod \mathfrak{P}_2^{2^j}$$

which implies

$$\Sigma_j \equiv \sigma(\theta) \bmod p^{2^j}.$$

The process is continued until ν is large enough so that

$$f(\Sigma_\nu) = 0,$$

at which point Σ_ν expresses $\sigma\theta$, as was desired.

A lemma

In the paper (Zassenhaus and Liang 1969), the authors give no explanation as to why we get the function $F_1(x)$ that we used in Step 6 of our algorithm above. Therefore in order to clarify this step, we prove the existence of the function $F_1(x)$ in the following lemma. We retain all the notation from this section.

Lemma:

If $F(x) \in \mathbb{Z}[x]$, $\deg F < h$, and $p^m \mid F(\theta_0)$, then $F(x) = p^m F_1(x)$ for some $F_1(x) \in \mathbb{Z}[x]$.

Proof:

Let $d = \deg F$, and let $\theta_0, \theta_1, \ldots, \theta_d$ be $d+1$ distinct conjugates of θ, which we have since $d < h$. Then in fact $p^m \mid F(\theta_i)$ for $i = 0, 1, \ldots, d$. If $F(x) = a_0 + a_1x + \cdots + a_dx^d$, then this says that

$$\begin{bmatrix} 1 & \theta_0 & \cdots & \theta_0^d \\ 1 & \theta_1 & \cdots & \theta_1^d \\ \vdots & \vdots & & \vdots \\ 1 & \theta_d & \cdots & \theta_d^d \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \bmod p^m.$$

But $p \nmid \mathrm{disc}(\theta_0)$, since p is not ramified in N, so the determinant of the matrix on the left is nonzero mod p. This says that the vector containing the coefficients of $F(x)$ must be 0 mod p^m, which was to be proved.

6.4 On Hensel factorization

Finally, we come to work of Zassenhaus published in 1969 on a way to factor polynomials, using Hensel's lemma. Symbolically at least, this is a fine way to end up our study of the shift from computability in principle to computability in practice in algebraic number theory, Zassenhaus being the latest figure we have chosen to consider (though of course many came after him), and Hensel the earliest apart from Kronecker, whose work we have considered only peripherally.

Hensel's use of the lemma named after him was, moreover, entirely geared toward computability in principle. His procedure for factoring a polynomial with rational coefficients over a p-adic number field $\mathbb{Q}_p$ served the theoretical result of making his *prime divisors* well-defined entities, since for a number field $\mathbb{Q}(\alpha)$ having a primitive element α satisfying an irreducible polynomial $F(x)$ over $\mathbb{Q}$, and for a rational prime p, the prime divisors of $\mathbb{Q}(\alpha)$ associated with p corresponded to the irreducible factors of $F(x)$ over the field of p-adic numbers $\mathbb{Q}_p$. In his demonstration of the possibility of computing such a factorization Hensel relied on entirely infeasible searches through enormous – though finite – spaces, to get the factorization started.

In Zassenhaus on the other hand, Hensel's lemma was put to a practical purpose, in an algorithm which could (and would) actually be used to factor polynomials. Regarding the source of his ideas, it is clear from his citations that Zassenhaus did not reinvent the lemma, but did indeed find it in Hensel.

In his paper on Hensel Factorization (Zassenhaus 1969), however, Zassenhaus cited not TAZ, but a paper of Hensel's published ten years later (Hensel 1918). Nor can we say that it were his involvement in computational number theory that first brought Hensel's lemma to Zassenhaus's awareness: in 1954, five years before his work with Taussky at Caltech, he published a paper entitled *Über eine Verallgemeinerung des Henselschen Lemmas* ("On a Generalization of Hensel's Lemma") (Zassenhaus 1954). Again in 1965, he published "On the Hensel lemma for Lie algebras" (Zassenhaus 1965).

Regarding Zassenhaus's involvement with p-adics in works published in 1969, the paper

on Hensel factorization was communicated to the journal on 9 July 1968, with the paper "On a Problem of Hasse" received later, on 13 November 1968. This supports the theory that the idea for the p-adic approach to the problem of Hasse came from Zassenhaus (as opposed to Liang), although we must then wonder what caused him to think of it in the case of the factorization problem. If it was simply his familiarity with Hensel's work, then at least here we have some continuity, a causal connection from Hensel to Zassenhaus. If the idea came from Hasse on his then recent visit to Ohio State, then once again this would be a forward transmission of ideas coming from Hensel.

6.4.1 Zassenhaus's algorithm

The Journal of Number Theory was published by Ohio State University starting in 1969, and had Zassenhaus as editor in chief from its beginning until his death in 1991. Hasse and Taussky, among two dozen others, were on the editorial board. Like Zassenhaus, they served from the first issue until their deaths, in 1979 and 1995 respectively.

In the first volume of the journal Zassenhaus published the paper, "On Hensel Factorization, I" (Zassenhaus 1969). The abstract is simple:

> A p-adic method for the constructive factorization of monic polynomials over a dedekind ring $\mathfrak{o}$ and the ideal theory of $\mathfrak{o}[x]$ are developed.

In the paper, Zassenhaus brought the old, impractical factorization method of Hensel from TAZ together with recent work of Berlekamp on the practical factorization of polynomials over finite fields. Berlekamp's procedure could replace the brute force search with which Hensel's version of the algorithm was to be initialized, and then Hensel's lifting procedure could be followed. The work of Berlekamp had been published in three papers, from April 1967, June 1968, and August 1968 (the last was evidently added to Zassenhaus's references in proof, having been published after his initial communication).

Zassenhaus's paper starts out in an extremely formal, abstract, and axiomatic style, presenting Hensel's lemma initially in the following way, without any suggested interpretation, so that the equations must appear very odd to anyone who did not already know a natural setting in which the lemma would arise:

> Let R be a unital commutative ring containing elements $f_1, f_2, f, d, r_1, a_1, a_2, r_2$ satisfying
>
> $$f_1 f_2 = f + d^2 r_1$$

$$a_1 f_1 + a_2 f_2 = d\,(1 + r_2)\,.$$

Upon transition to:

$$\begin{aligned} f_1^* &= f_1 - a_2 d r_1, & f_2^* &= f_2 - a_1 d r_1, \\ a_1^* &= a_1\,(1 + 2a_1 a_2 r_1 - r_2)\,, & a_2^* &= a_2\,(1 + 2a_1 a_2 r_1 - r_2)\,, \\ r_1^* &= r_1\,(a_1 a_2 r_1 - r_2)\,, & r_2^* &= -\,(r_2 - 2a_1 a_2 r_1)^2 \end{aligned}$$

we obtain the corresponding relations for the starred elements:

$$f_1^* f_2^* = f + d^2 r_1^*, \qquad a_1^* f_1^* + a_2^* f_2^* = d\,(1 + r_2^*)\,.$$

(Zassenhaus 1969)

Zassenhaus does eventually discuss the natural interpretation of the lemma, though only much later. Five pages from the end of the twenty-page paper, he writes that, "the by now classical form of Hensel's lemma is obtained if we..." at which point he provides the appropriate interpretation.

In addition, after so much abstraction, the reader is finally rewarded with an example calculation at the very end of the paper, in which Zassenhaus shows how to factor $f(x) = x^2 - 9x + 20$ using the prime $p = 2$. He uses Berlekamp's method to obtain the initial factorization $f \equiv x\,(x-1)$, and then lifts this p-adically to the factorization $f(x) = (x - 4)(x - 5)$.

The example avoids one of the main challenges in applying Hensel's lemma to the problem of factorization over $\mathbb{Q}$. Namely, if a polynomial $f(x)$ decomposes mod p into a product of a large number of factors, we may have to try many different combinations of these factors to find a polynomial which lifts to an actual divisor of $f(x)$ over $\mathbb{Q}$, or else to find that none of them does, and that $f(x)$ is irreducible over $\mathbb{Q}$. For example, [46] the polynomial

$$f(x) = x^{16} + 11x^4 + 121$$

is irreducible over $\mathbb{Q}$, but factors mod 13 as a product of two quadratic factors $a_1(x)$, $a_2(x)$, and four cubic factors $b_1(x), b_2(x), b_3(x), b_4(x)$. In order to prove that the polynomial is irreducible over $\mathbb{Q}$, we would have to try grouping the six factors mod 13 into two products $u(x), v(x)$ in quite a few different ways, and lift each such factorization until its coefficients

[46] The example is taken from (Geddes, Czapor, and Labahn 1992, p. 374).

were reduced mod 13^k (reduced symmetrically around 0), where $13^k > 2B$ for some known bound B on the height of any potential factors of $f(x)$ over $\mathbb{Q}$, such as the Mignotte bound. [47] Namely, we would have to try taking u to be each of the six factors on its own, e.g.

$$u = a_1 \qquad\qquad v = a_2 b_1 b_2 b_3 b_4$$

then taking u to be each product of two factors, e.g.

$$u = a_2 b_3 \qquad\qquad v = a_1 b_1 b_2 b_4$$

and finally taking u to be each product of three factors, e.g.

$$u = b_1 b_3 b_4 \qquad\qquad v = a_1 a_2 b_2$$

for a total of

$$\binom{6}{1} + \binom{6}{2} + \binom{6}{3} = 41$$

liftings to perform. Zassenhaus does address the problem (Zassenhaus 1969, p. 308), but gives no solution other than simply trying all combinations.

Apart from the three papers of Berlekamp, only one other work is referenced by Zassenhaus, and that is a twenty-page article of Hensel's, appearing in the *Mathematische Zeitschrift* of 1918 (Hensel 1918). It is a curious choice. The paper is cited only once by Zassenhaus, as a reference on Hensel's lemma. The odd thing about this is that Hensel's lemma is not given in that paper, but only discussed once, in entirely different terms than are used in Zassenhaus's work. Moreover, instead of presenting any details on the lemma or even stating it precisely, Hensel only refers *his* reader to the pages in TAZ where it can be found:

> It can also be decided, as may be merely mentioned here, by a finite number of tests, into how many p-adic prime factors of lower degree $F(x)$ decomposes and what their degrees are; and those prime factors can be determined to any predetermined degree of accuracy (cf. Hensel, "Theorie der algebraischen Zahlen", p. 66 ff.). (ibid., p. 439) [48]

[47] See (Mignotte 1982).

[48] *Es kann auch, wie hier nur erwähnt werden mag, durch eine endliche Anzahl von Versuchen entschieden werden, in wie viel p-adische Primfaktoren niederen Grades $F(x)$ zerfällt und welches ihre Grade sind; und jene Primfaktoren können mit jeder vorgegebenen Genauigkeit bestimmt werden ....*

If Hensel himself only deferred to TAZ, why would Zassenhaus not simply cite TAZ directly, instead of sending his readers on a goose chase? One possible reason is that he felt the work of 1918 would be more accessible to his audience.

It is well known that Hensel's book of 1908 was one of the major inspirations for Steinitz's seminal 1910 work on the general, axiomatic treatment of fields. [49] Reciprocally, Hensel himself stayed up to date on the new "structural view" of algebra that was arising during these decades [50]. For example, his subsequent book, *Zahlentheorie* of 1913 (Hensel 1913) begins with a consideration of the new concepts of fields, modules, groups, and rings. The group concept was new enough at this time that Hensel could present two alternative names for these structures, *Gruppe*, which he attributed to Weber, and *Strahl* (meaning "ray"), which he attributed to Fueter. [51]

Similarly, by the time of the 1918 paper that Zassenhaus chose to cite, Hensel was setting out to give a reduction of p-adic field theory to the theory of *congruence fields* (*"Kongruenzkörper"*), i.e. fields of the form $k[x]/(f(x))$ where $f(x)$ is irreducible over $k[x]$. He referred, not coincidentally, to Steinitz for the basic theory of these congruence fields. He was thus keeping right up with the times. The treatment in TAZ, on the contrary, while more elementary and thus simpler, was not nearly as sophisticated, and in that way perhaps more arcane to the eyes of most 1960s mathematicians. It could be that Zassenhaus chose this work of Hensel's as reference for reasons such as these.

[49] See Corry (Corry 1996, pp. 184-197) for discussion of Steinitz's work (Steinitz 1910) and Hensel's influence.

[50] See (Corry 1996) generally on this topic.

[51] See (Hensel 1913, p. 11). Hensel makes no mention of any connection with *ray class groups*, from class field theory, though this seems a likely theory for the origin of the term.

Chapter 7

Epilogue

From the 18th to 23rd of August, 1969, a conference called "Computers in Number Theory" was held in Oxford, England, under the sponsorship of the Atlas Computer Laboratory. The Atlas computers were designed and built by researchers at the University of Manchester, England, with work starting in 1956 and culminating in three computing installations: two at the Universities of Manchester and of London, in 1962 and 1963 respectively, and one at the Atlas Computer Laboratory in 1964, which was located in Chilton, near Oxford (Williams 1985).

An Atlas Computer Laboratory publication of 1969 [1] described various statistics and operational parameters of the machinery in use in the laboratory at the time, of which we note a few here:

- The machine executes on average about 350,000 instructions a second.
- Time to sort 5000 numbers into order: 1 second.
- Time to calculate 5000 decimal digits of π: 20 minutes.
- Languages accepted:
  - Fortran
  - Algol
  - Machine code ABL

[1] `http://chilton-computing.org.uk/acl/literature/acl/p006.htm`

  - Atlas Autocode
  - Extended Mercury Autocode

- Weekly throughput:
  - run 2,500 complete jobs;
  - read in a million cards and 30 miles of paper tape;
  - print 2 million lines of output;
  - punch 30,000 cards;
  - handle 1,500 reels of magnetic tape.

- Job sources:
  - 75% from universities (600 separate projects on the books, about 200 worked on each week)
  - 15% from government and similar laboratories, including meteorological
  - 10% research and development work of Atlas laboratory itself

- Distribution of university jobs:
  - Mathematics: 17 %
  - Physics: 20 %
  - Chemistry: 17 %
  - Engineering: 22 %
  - Medical and Biological Sciences: 6 %
  - Social Sciences: 8 %
  - Others: 10 %

- Typical week's work valued at about £45,000.

Among the four or five dozen presenters at the Oxford 1969 conference put on by the Atlas Laboratory, Hasse presented his and Liang's work on the construction of the class field over $\mathbb{Q}(\sqrt{-47})$ that we discussed in Section 6.3, and Taussky presented a paper in

continuation of her work with Scholz from the 1930s. Among other notable names in attendance were E. Berlekamp, Erdős, S. Kuroda, D.H. and E. Lehmer, Mordell, E.S. Selmer, J.-P. Serre, H.M. Stark, H.P.F. Swinnerton-Dyer, and J. Tate.

In the prefatory remarks to the proceedings, editors A.O.L. Atkin of Brown University and B.J. Birch of the University of Oxford wrote that,

> The papers illustrate all aspects of the use of computers in number theory: as an essential part of a proof, as an aid to discovery (Gauss would surely have approved), and negatively as a possible ally in doing what has not yet been done. The attitude sometimes maintained a few years ago, that a computer is a disreputable device in the context of "pure" mathematics, was noticeably absent at the Symposium. Computors and noncomputors alike were concerned with getting on with the job, rather than worrying about the relative reliability of computers and papers in mathematical journals. (Atkin and Birch 1971, p. xi)

giving some sense of the prevailing attitude toward computers, and the uses to which they were put. Regarding the future of their subject, the editors noted,

> On Wednesday evening there was an open discussion on "Number Theoretic Subroutines and Tables". As might have been expected with so large a number of original thinkers no substantial agreement was reached, but the three following conclusions commanded the support of most of the 40 people present. First that a complete list of what exists, in print and privately, would be useful. Second, that the subject is too various to lend itself to an agreed package of subroutines and a universal language. Third, that some facility should exist for making known the "results" of unsuccessful but substantial computation. (ibid., p. xii)

The task of handling the first of these goals, a complete list of what existed in the subject up to that time, seems to have been given to one of the attendees of the conference, Horst Günter Zimmer (b. 1937).

Zimmer was a student of Peter Roquette (who studied with Hasse) at Tübingen, PhD 1966. He would later be the editor of the English edition of Hasse's *Zahlentheorie*, which was published in 1980, a role which suggests that Zimmer might have been sympathetic to the outlook on the history of algebraic number theory expressed there.

Zimmer's survey (Zimmer 1972) was called "Computational Problems, Methods, and Results in Algebraic Number Theory", and was published in 1972, as Volume 262 in the

Springer *Lecture Notes in Mathematics* series. Zimmer explains in the preface that at the Oxford conference he was asked to write a survey of the emerging field of computational algebraic number theory, a task which he carried out mainly while visiting at UCLA during what they called the "Algebra Year", 1969/70.

The survey received high praise. The reviewer R. Finkelstein for *Mathematical Reviews* wrote (my emphasis):

> This outstanding monograph is a survey of numerical investigations concerning algebraic number theory, with special emphasis on the computer-oriented viewpoint. Its twelve chapters contain algorithms for solving problems about finite fields, the factorization of polynomials, Galois groups, continued fractions, field extensions, modules and orders, products of linear forms, units, class numbers and class groups of algebraic number fields, Diophantine equations and the Hasse principle for cubic surfaces. In addition, there is a list of 408 references, most of which are discussed in the text. *To this reviewer's knowledge, this is the first book of this kind on algebraic number theory to have appeared in print*, and he would like to suggest that it be updated periodically.

Similarly, in the acknowledgements section of his "Course in Computational Algebraic Number Theory", Volume 138 in the Springer Graduate Texts in Mathematics series, published in 1993, Henri Cohen wrote,

> In roughly chronological order I need to thank, Horst Zimmer, whose Springer Lecture Notes on the subject (Zimmer 1972) was both a source of inspiration and of excellent references for many people at the time when it was published. Then, certainly, thanks must go to ...

And again, Hasse wrote to Zimmer on 2 July 1972 regarding the survey, both expressing his great admiration for it, and providing a few critical comments and questions. He wrote,

> Lieber Herr Zimmer,
>
> Now that I have somewhat more thoroughly looked over and for the most part read your Lecture Notes, I would like to express to you once again my great admiration for the completeness of this gigantic work. I can well imagine how much time and trouble it cost you to gain an overview of the content of all these 408 works, of which only one, namely the

> last, cost you none. [2] This work is for the number theorist who is interested in numerics -- and among these I count myself -- a highly valuable reference book, from which one can learn a great deal.
>
> ... [3]

The words of Finkelstein, Cohen, and Hasse suggest that Zimmer's survey was the first complete review of the newly emerging subject. The histogram in Figure 7.1 shows the number of works cited by Zimmer for each year. (Excepted are the several unpublished manuscripts in Zimmer's bibliography, which have no year.)

Zimmer seems to have had some influence not just from Hasse but also from Zassenhaus. To begin with, of the 408 entries in the bibliography of his survey, the one belonging to himself was for a 1969 manuscript at UCLA called "Factorization of polynomials according to a method of Zassenhaus".

Moreover, in a letter of 4 May 1967, Hasse had written to Zimmer to say that while he had recommended Zimmer, at the latter's request, for a position as Assistant Professor at Western Michigan University, he urged Zimmer to instead work at Ohio State with Zassenhaus, where he described the mathematical climate as livelier and more directed toward the algebraic and number theoretic side of things. [4]

Altogether, Zassenhaus had 16 entries out of the 408 in Zimmer's bibliography (4 of these as second author). Taussky had 12 (3 as second author); Hasse had 12 (4 as second author). In total, these three had 38 entries, representing about 10 percent of the early activity in this subject, if Zimmer's survey was comprehensive.

Hasse's KAZ and (Hasse 1950a) were present in Zimmer's bibliography, as was his collaboration with Liang. Taussky's 1934 work with Scholz was named, as well as her continuation of it from the Oxford 1969 conference, and the reprint in (Todd 1962) of her 1953 survey

---

[2] Zimmer himself was first author on only one work in the bibliography, and it was the last one listed. In fact he was also second author on one other paper.

[3] *Nachdem ich jetzt Ihre Lecture Note etwas gründlicher angesehen und zu großen Teilen auch gelesen habe, möchte ich Ihnen noch einmal meine große Bewunderung über die Vollendung diese gigantischen Werks aussprechen. Ich kann mir sehr gut denken, wieviel Zeit und Mühe es gekostet hat, eine Übersicht über den Inhalt aller dieser 408 Arbeiten zu gewinnen, von denen nur eine, nämlich die letzte, Ihnen keine Mühe gemacht hat. Dies Werk ist für den Zahlentheoretiker, der numerisch interessiere ist – und zu diesen zähle ich mich –, ein sehr wertvolles Nachschlagewerk geworden, aus dem man zudem viel lernen kann.*

[4] *Bei Professor Zassenhaus wären Sie allerdings mathematisch doch wohl besser aufgehoben. Ich würde unter allen Umständen versuchen, dort anzukommen. Das mathematische Klima in Ohio State University ist doch wohl erheblich belebter und mehr nach der algebraischen und zahlentheoretischen Seite ausgerichtet.*

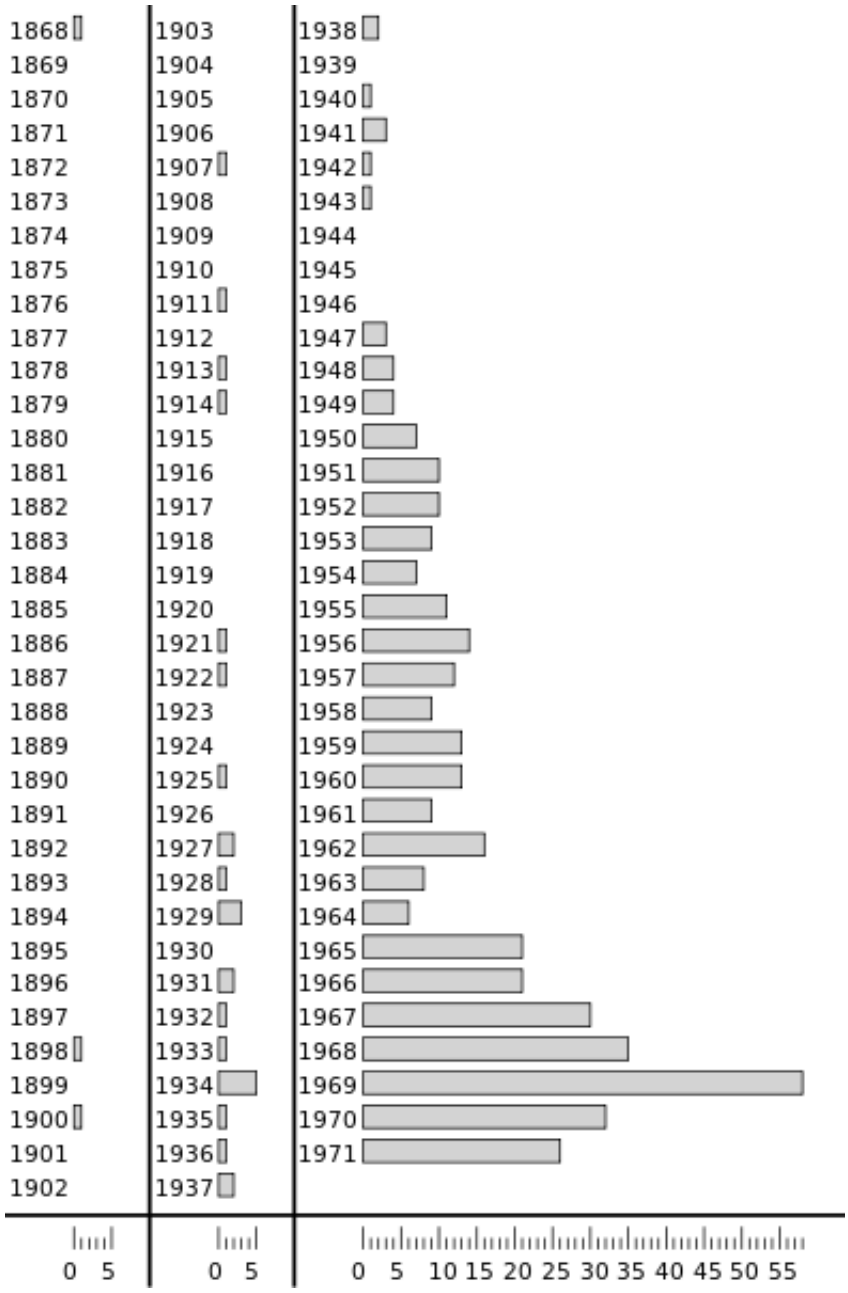

Figure 7.1: Number of works cited per year in bibliography of Zimmer's survey (ibid.).

(Taussky 1953) on computational problems in algebraic number theory. All three papers coming out of the 1959 collaboration between Taussky, Zassenhaus, and Dade were named. Rounds I and II of Zassenhaus's maximal order (or integral basis) algorithm were there, along with his collaboration with Liang on the problem of Hasse, and his paper on Hensel factorization.

The Oxford 1969 conference and Zimmer's survey seem strong evidence that a computational branch of algebraic number theory was, by the late 60s and early 70s, gaining visibility as a mathematical research area in its own right. As D.H. Lehmer said in his opening address at the Oxford conference,

> Not only the number of the contributors, but also their geographic distribution attests to the fact that the subject of the Symposium is now of widespread interest. (Lehmer 1971)

In the same year, Lehmer wrote in another place that

> The era of the automatic digital computer is nearing the end of its second decade. By this time a fair proportion of number theorists are becoming aware of its existence and are at least wondering what the commercial electronic computer might be able to do for them. Many number theorists have already experienced one or more instances of aid from this quarter. (Lehmer 1969)

After another two decades, in 1989, Zassenhaus and Pohst would publish their book, "Algorithmic Algebraic Number Theory", of which Cohen wrote,

> Although I have met Michael Pohst and Hans Zassenhaus only in meetings and did not have the opportunity to work with them directly, they have greatly influenced the development of modern methods in algorithmic number theory. They have written a book [Poh-Zas] which is a landmark in the subject. (Cohen 1993).

Yet another decade later, in 2000, Cohen's second book on computational algebraic number theory, Volume 193 in Graduate Texts in Mathematics, was published. He expressed there his view that the research program of computing invariants of number fields was largely accomplished, ironically referring to it as "the Dedekind program", which just goes to show that alternate perspectives on the significance of the major figures in our subject's history are always possible. He wrote,

> The computation of invariants of algebraic number fields such as integral bases, discriminants, prime decompositions, ideal class groups, and unit groups is important both for its own sake and for its numerous applications, for example, to the solution of Diophantine equations. The practical completion of this task (sometimes known as the Dedekind program) has been one of the major achievements of computational number theory in the past ten years, thanks to the efforts of many people. Even though some practical problems still exist, one can consider the subject as solved in a satisfactory manner, and it is now routine to ask a specialized Computer Algebra System such as Kant/Kash, LiDIA, Magma, or Pari/GP, to perform number field computations that would have been unfeasible only ten years ago.

Many mathematicians contributed over its formative years to the establishment of a computational branch of algebraic number theory, whereas we have had time to consider only a few of them in depth here.

Harvey Cohn, for example, published many papers in the early computer era on machine exploration of algebraic number theoretic questions. He alone had 27 entries in Zimmer's bibliography (3 of those as second author). He shared the Number Theory chapter with Taussky in Todd's 1962 volume (Todd 1962); he presented work at the Oxford 1969 conference; in 1985 he published a book entitled "Introduction to the construction of class fields". When Zimmer published a German language summary of his survey, Cohn was selected to review it for Mathematical Reviews.

Time permitting, Cohn would make an interesting subject for further study. His background seems to have been an unusual one. In a letter to Hasse of 17 October 1969, he wrote,

> `You know, I have learned algebraic number theory like an ‘‘applied mathematician’’ and now I find the more abstract approach to be a fascinating Wonderland.`

His PhD was with Lars Ahlfors at Harvard in 1948, entitled *Diophantine Aspects of Poincaré Theta Functions*.

Cohn's 1978 book, "A classical invitation to algebraic numbers and class fields" (Cohn 1978) is especially interesting. Henri Cohen described the book as "A highly recommended

concrete introduction to algebraic number theory and class field theory, with a large number of detailed examples." (Cohen 1993, p. 519). Olga Taussky's name appears after Cohn's on the book's cover, where she is credited with its two appendices. The first of these contains her notes on Artin's class field lectures, which had circulated by hand since 1932, as we mentioned on page 98. They were published here for the first time. The second appendix is on connections between algebraic number theory and integral matrices, the same connection that lay behind Taussky's collaboration with Zassenhaus and Dade in 1959.

Like so many mathematicians who devoted themselves to the more concrete approach to mathematics afforded by computational work, Cohn seemed to express some concern over the growth of unbounded abstraction in the mathematics of the 50s and 60s. Earlier we saw for example Hasse's dislike of the cohomological methods of post-war number theory (page 95), and we saw that Zassenhaus objected to the methods of the Bourbakists at least in regards to education (page 182). Cohn too expressed such a view in (Cohn 1978). The very first page of the book after the title page displays only a quotation from George Orwell's *1984*:

> The purpose of Newspeak was not only to provide a medium of expression, but to make all other modes of thought impossible. It was intended that when Newspeak had been adopted once and for all and Oldspeak forgotten, a heretical thought should be literally unthinkable, at least so far as thought is dependent on words. This was done chiefly by eliminating undesirable words and by stripping such words as remained of unorthodox meanings, and so far as possible of all secondary meanings whatever.

In his introduction to the book he did not comment directly on the quotation, but a likely interpretation seems to be that the "New Encyclopedia" of Bourbaki was to be compared to the "Newspeak" of Orwell's story. Meanwhile Cohn did make such remarks as that, "number theory began with concrete observations at least as palpable as those in the physical world," and, "Today, a student wandering into a course might regard class field theory as belonging to 'abstract algebra' rather than 'number theory' (and might even regard number theory as having outgrown its need for numbers)." He added that the purpose of his book was, "to make the incredible current state of affairs more nearly believable and to that extent more accessible."

The clash between on the one hand the philosophy thus expressed by Cohn, and by Hasse

and Zassenhaus alike, and on the other hand a philosophy more in favour of "unbounded abstraction", has been a major theme in the history of 20th century mathematics. It has been expressed perhaps more famously in such episodes as Mordell's scathing review of the 1962 book, *Diophantine Geomtery*, by Serge Lang, [5] for example. Our topic can be regarded as a small part of this larger question. We have seen how one line of research, rooted in a particular set of late nineteenth century mathematical values, evolved through a period of broadly shifting values in the mid 20th century. The appearance of the electronic computer seems to have encouraged this computational side of algebraic number theory to become even more truly computational, moving from theoretical computation to practical. Meanwhile, the more abstract side also went ever more boldly in its own direction. The goal of better understanding the causes behind the diverging values represented by these very separate traditions points to further studies in the history of the mathematics of the twentieth century.

In addition to Harvey Cohn, more time still could be devoted to a study of the influence of D.H. and Emma Lehmer on our subject, or for example to the work of Hasse's student H.W. Leopoldt, or the work of H. Swinnerton-Dyer, to name just a few. Corry's study of the collaboration between the Lehmers and Vandiver (Corry 2008a,b) covers a major portion of this story. We may hope that in our look at Hasse, Taussky, and Zassenhaus, we have been able to find some signs of the influence that the computability in principle of Hensel, and Kronecker before him, had on the development of computability in practice in algebraic number theory. While the direct ties of teacher to student linking Hensel to Hasse are obvious, we hope to have revealed some less immediately apparent influences as well.

Taussky's instrumental role as an algebraic number theorist with access to computers, and the know-how to operate them, connected her both with Hasse, and with Zassenhaus. Hasse sent Taussky copies of Weyl 1940, and of his own KAZ of 1952. He suggested number theoretic problems that might be worth tackling on the computer. She sought his approval of her 1953 survey of problems in computational algebraic number theory before she published it in 1956. At the very beginning of her career in the 1930s as well, we saw Taussky and Scholz sending copies of their work to Hasse, and relying on tables filled with algebraic number theoretic data that he had computed, showing that, from very early on, Taussky was aware of Hasse as a prominent number theorist who supported computation and table work.

[5] See Mordell's review (Mordell 1964), as well as Lang's reflections on the event (Lang 1995).

Zassenhaus's work in the field of computational algebraic number theory began when he visited Caltech in 1959, and collaborated with Taussky. His close colleague in the subject, Michael Pohst, wrote that it was out of this work that his involvement in the subject emerged for the first time (Pohst 1994, p. 7). In 1977 Zassenhaus was editor of a volume, *Number Theory and Algebra* (Zassenhaus 1977), which collected papers in honour of three people with whom Zassenhaus was associated: Henry B. Mann (a colleague at Ohio State), Arnold E. Ross (whom we discussed in the introduction to Chapter 6), and Olga Taussky-Todd. He wrote in the preface,

> We, their colleagues, pupils, collaborators, and friends find it fitting to dedicate to them the fruits of our work so as to pass onto researchers coming after us the spirit of patient toil in the service of the queenly science which our three honorees implanted in us.

That Zassenhaus had at least the editorship of this volume (and likely some initiative in its conception), and that he would write such remarks in the preface, suggests that Zassenhaus felt that these people, Taussky among them, had been important influences on him. Reciprocally, we saw in Section 5.5 that Taussky had a great deal to say about Zassenhaus in her autobiographical remarks about her career.

Hasse set those problems regarding the class field construction over $\mathbb{Q}(\sqrt{-47})$ which Zassenhaus and Liang solved by p-adic methods. In his work Zassenhaus made several citations of Hensel 1908, and Weyl 1940. Finally, bringing us full-circle, the project with Liang came right on the heels of Zassenhaus's revival of Hensel's lemma in earlier work of the same year. The lemma, which had served Hensel in 1908 for the demonstration of the computability in principle of the factorization of a polynomial, was finally used by Zassenhaus in 1968 a practical polynomial factorization algorithm.

Appendix A

Hensel's theory as generalization of Kummer's

"In der Chemie hat man ferner zur Prüfung der in einem unbekannten aufgelöseten Körper enthaltenen Stoffe die Reagentien, welche Niederschläge geben, aus denen die Anwesenheit der verschiedenen Stoffe sich erkennen läßt. Ganz Dasselbe findet für die complexen Zahlen Statt; denn es sind die oben mit Ψ bezeichneten complexen Zahlen ebenso die Reagentien für die idealen Primfactoren, und die reale Primzahl q, welche nach der Multiplication mit einer solchen als Factor aus dem Producte heraustritt, ist genau Dasselbe, wie der unlösiche Niederschlag, der nach Anwendung des Reagens zu Boden fällt."

— Ernst Eduard Kummer, 1846

E. E. Kummer (1810-1893) invented *ideal prime factors* in order to recover unique factorization for rings of cyclotomic integers $\mathbb{Z}[\alpha]$, α a primitive λ^{th} root of unity, his seminal treatise appearing in (Kummer 1847b). [1] Kummer explained his theory of ideal divisors by comparing number theory to chemistry, primes to atoms, prime factorizations to chemical formulae:

> Remark: Here, where I leave the general theory of the decomposition of complex numbers, if incomplete, in order to give some applications in the following sections, I cannot refrain from remarking upon the great analogy which this theory has with *chemistry*. Chemical bonds correspond for complex numbers to multiplication; elements, or really the atomic weights thereof, correspond to prime

[1] We will refer to this work as K1847 throughout this appendix.

> factors; and chemical formulae for the decomposition of substances are precisely the same as the formulae for the decomposition of numbers. (Kummer 1847b, p. 359)

When he wrote in 1846, the chemical element fluorine had not yet been isolated. Its existence had been postulated in 1810 by A.-M. Ampère (1775-1836), and in 1876 it was finally isolated by French chemist H. Moissan (1852-1907), who was later awarded the Nobel prize, in part for this work. Along the way, many had been maimed or killed in attempts to isolate the element, dangerous due to its extreme reactivity, and these became known as the "fluorine martyrs". For Kummer and his contemporaries, fluorine was a theoretical element, thought to be analogous to chlorine, and known only by its presence in compounds like NaF (sodium fluoride) and MgF_2 (magnesium fluoride). He continued:

> Even the ideal numbers of our theory have their counterpart in chemistry, perhaps even all too often, as hypothetical radicals, which up to now have not yet been isolated, but which, like the ideal divisors, have their reality in compounds. Fluorine, not yet isolable, and yet numbered among the elements, can be counted as an analogue of an ideal prime factor. (Kummer 1847b, p. 360)

In the course of our examination of Kummer's theory of ideal prime divisors, we will see how this analogy plays out. By the end, the meaning of the German quotation with which we opened this appendix will be made clear.

Some years after Kummer's introduction of ideal prime divisors, Richard Dedekind (1831-1916), Leopold Kronecker (1823-1891), and Kurt Hensel (1861-1941) each gave their own framework with which to generalize his idea to general number fields. Dedekind's theory, versions of which he published between 1871 and 1894, uses his own invention of *ideals*, and is very different from Kummer's, both in the objects the theory deals with, and in the methods of proof employed. Kronecker's theory, the main treatise on which appeared in 1882, is not something that the present author can speak knowledgeably about, nor can many people in the world. According to (Edwards, Neumann, and Purkert 1982), Kronecker's principal treatise on the subject (Kronecker 1882) has been viewed as sketchy and inconsistent by prominent mathematicians (Dedekind included) from Kronecker's time forward. Edwards et. al. suggest (Edwards, Neumann, and Purkert 1982, p. 53) that in fact it was not so much through his written papers that Kronecker had an influence on mathematics, as through his personal influence on those few who had the patience to work through

his often obscure ideas.

Among those few was Kurt Hensel. It may therefore be that some of Kronecker's ideas about algebraic number theory made it into Hensel's version of the theory of ideal divisors. Hensel's book on the subject (Hensel 1908) [2] does include Kronecker's idea of a *fundamental form*, and related ideas, and it includes his own treatment of *inessential discriminant divisors*, which he worked out for his PhD dissertation (Hensel 1884), while a student of Kronecker in Berlin. Whether Kronecker's ideas about recovering unique factorization however are a part of Hensel's framework the present author cannot say. At any rate, Hensel's theory of prime divisors comes in Chapters 6 and 7 of TAZ, whereas the most obviously Kroneckerian work with forms does not come until Chapter 10.

What we can say positively, and will examine in this Appendix, is that Hensel's theory of divisors appears as a perfect generalization and extension of Kummer's method. Considering Dedekind's divergence from Kummer's methods, and Kronecker's obscurity, Hensel's theory can perhaps be called the true successor to Kummer's, i.e., it appears a claim worth considering, that it was not until TAZ that the theory begun in K1847 truly moved forward into full generality.

Kummer did continue to work on his own theory up until at least 1859, when he published the large treatise (Kummer 1859) on reciprocity laws, but according to Weil (Kummer 1975, p. 2) he moved on to other subjects around this time. By 1859 Kummer was working with number fields of the form $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{\mu})$ obtained by adjoining to a cyclotomic field $K = \mathbb{Q}(\zeta_\ell)$ of ℓ^{th} roots of unity the ℓ^{th} root of a number $\mu \in K$ which was not already an ℓ^{th} power in K – that is, such fields as were named by Hilbert *Kummer fields*, and were the subject of the fifth part (and one third of the pages) of the *Zahlbericht* (Hilbert 1897). But Kummer never attained to completely general number fields, as did Hensel.

The view that Hensel's work, not Kronecker's or Dedekind's, was the actual continuation of Kummer's work, has been examined before by Weyl in (Weyl 1940). Here we hope to offer a few new reflections on the matter. It is sometimes casually stated that Kummer used "p-adic analysis" (e.g. (Kummer 1975, p. 1)) although the term is anachronistic and no explanation is given. In this appendix we offer some such explanation.

One question is whether Zolotarev's theory of 1880 was as nearly a perfect generalization of Kummer's as was Hensel's, as Piazza's and Neumann's discussions (Neumann 2007; Piazza

[2] We will refer to this work as TAZ throughout this appendix.

2007) suggest it might have been. In that case, Hensel's theory might only be the one that first brought a direct generalization of Kummer's theory to the attention of mathematicians in Western Europe. Zolotarev was known in the east, for example to N. Tchebotarev (Neumann 2007, p. 86), but was cited neither in (Hilbert 1897) nor in (Weyl 1940).

Another question is whether Hensel or even Zolotarev was the first to think these ideas through. Dedekind claimed in 1878 to have considered a generalization of Kummer's theory along these same lines, only to have abandoned it because he felt that reliance upon the minimal polynomial of an arbitrary primitive element α for the field in question obscured the true invariance with respect to this choice, which divisibility by ideal prime divisors actually possesses. (Dedekind 1930-1932b, p. 202)

We leave these questions behind however, and turn now to the matter at hand, an exposition using modern concepts and terminology, of both Kummer's and Hensel's definitions of ideal prime divisors, as given in K1847 and TAZ, in which the former will appear as a special case of the latter. While Hensel's treatment is close enough to present-day conceptions that the translation from his language to our own was quite easy, Kummer's language comes from a significantly earlier era, and assimilating what he does with the way we do things today required much more work. This can perhaps be attributed in part to the effect of Hilbert's *Zahlbericht* in shaping the received view of algebraic number theory, and its appearance a decade before Hensel, but fifty years after Kummer.

For further help in understanding Kummer's theory the reader is referred to the excellent book (Edwards 1977), especially Chapter 4, which is filled with numerical examples and exercises, and in addition makes an effort to motivate much of what Kummer did. A 1910 review of TAZ by L.E. Dickson (Dickson 1910) provides a very clear and concise summary of Hensel's theory.

A.1 Preliminaries

We assume as prerequisites elements of abstract algebra, such as the theory of irreducible polynomials, fields and their isomorphisms, commutative diagrams, and Galois theory, but try to define all number theoretic concepts used, except for basic congruences, with which we assume the reader is already familiar.

Algebraic numbers and fields

By $\mathbb{C}$ we mean the field of complex numbers. Any number $\alpha \in \mathbb{C}$ that is a root of a polynomial $h(x) \in \mathbb{Q}[x]$ is called an *algebraic number*. The monic irreducible factor of $h(x)$ of which α is a root is an invariant associated to α, called the *minimal polynomial* of α, and denoted $m_\alpha(x)$. If the degree of $m_\alpha(x)$ is n, then α is said to be an algebraic number of *degree* n.

For example, $\alpha = \sqrt{2}$ is a root of the polynomial $h(x) = 2x^3 - 2x^2 - 4x + 4$, and is therefore an algebraic number, but $h(x)$ factors over $\mathbb{Q}$ as

$$h(x) = 2\,(x-1)\left(x^2-2\right)$$

so that $x^2 - 2$, the monic irreducible factor of $h(x)$ of which α is a root, is the minimal polynomial $m_\alpha(x)$ of α, and α is an algebraic number of degree 2.

By $\mathbb{Q}$ we mean the field of rational numbers. Given any algebraic number α of degree n, we will mean by the *algebraic number field* $\mathbb{Q}(\alpha)$ the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and α. It can be thought of as the collection of all rational functions in α, with rational numbers as coefficients. Even though there are always other algebraic numbers β besides α such that $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$, still the degree n of α is an invariant of the field $\mathbb{Q}(\alpha)$ and is referred to as the *degree* of the field. So for example the degree of the field $\mathbb{Q}(\sqrt{2})$ is 2.

Integers, and the integral basis

In his *Disquisitiones Arithmeticae* of 1801, Gauss gave us the *fundamental theorem of arithmetic*, which states, roughly, that each whole number has a unique factorization into primes. The importance of this theorem in arithmetic can be suggested by noting the criterion it gives for divisibility: one whole number divides another if and only if the second one contains all the primes that the first one does, and possibly more. The falsity of the fundamental theorem in certain number fields $\mathbb{Q}(\alpha)$ is the reason for Kummer's invention of ideal prime factors.

Gauss's theorem applies to the set of ordinary integers $\mathbb{Z}$. In the following sections, we are going to be considering altered versions of this theorem that apply to other number systems. In order to get there, we are going to have to redefine the key concepts involved in the statement of the theorem, namely *integrality*, *divisibility*, and *primality*, in ways that are suitable for these other number systems. We will begin now, by determining the correct notion of integrality for algebraic number fields.

In the context of algebraic number theory, the familiar subset $\mathbb{Z}$ of integers in $\mathbb{Q}$ is referred to as the set of *rational integers*. An algebraic number β in any number field $\mathbb{Q}(\alpha)$ is called *integral*, or is said to be an *algebraic integer*, if all the coefficients of its minimal polynomial $m_\beta(x)$ lie in $\mathbb{Z}$. Thus for example $\sqrt{2}$ is an integer of the field $\mathbb{Q}(\sqrt{2})$ since its minimal polynomial $x^2 - 2$ has all its coefficients in $\mathbb{Z}$, whereas $\frac{1+\sqrt{2}}{2} \in \mathbb{Q}(\sqrt{2})$ is not an integer in this field, since its minimal polynomial $x^2 + x - \frac{1}{4}$ has a coefficient not lying in $\mathbb{Z}$. Following Dedekind, we will denote the set of all algebraic integers in a number field F as $\mathcal{O}_F$.

The very first appearance historically of this definition of algebraic integers is hard to track down. It appeared in Dedekind (Dedekind and Lejeune Dirichlet 1871) in 1871, and he later stated (Dedekind and Lejeune Dirichlet 1894, p. 524) that he did not know of any earlier appearance of this definition in print, but it remains unclear whether Dedekind was actually the first to use it or not. [3]

One sign that we have the "right" notion of integrality, is the basic result that an algebraic number field $\mathbb{Q}(\alpha)$ is obtained as the set of all quotients β/γ, where β and γ are algebraic integers lying in the field $\mathbb{Q}(\alpha)$. Thus, just as $\mathbb{Q}$ may be obtained by taking all quotients of elements of $\mathbb{Z}$ (with nonzero denominator), the same relation holds between $\mathbb{Q}(\alpha)$ and its own set of integers. A definition which makes a new structure behave similarly to an old, familiar structure has a good chance of being the "right" one. In fact, an even stronger result is true; namely, $F = \mathbb{Q}(\alpha)$ is recovered already as the set of all quotients β/c in which $\beta \in \mathcal{O}_F$ as before, but in which c is confined to $\mathbb{Z}$.

For the study of an algebraic number field $F = \mathbb{Q}(\alpha)$, an idea of fundamental importance is the *integral basis*. If the degree of F is n, then an integral basis for F is any set of n elements $\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(n)}$ of $\mathcal{O}_F$ such that every element β of $\mathcal{O}_F$ can be written uniquely in the form

$$\beta = b_1\gamma^{(1)} + b_2\gamma^{(2)} + \cdots + b_n\gamma^{(n)},$$

where $b_1, b_2, \ldots, b_n$ are rational integers. In other words, every $\beta \in \mathcal{O}_F$ is equal to exactly one $\mathbb{Z}$-linear combination over the $\gamma^{(i)}$. It follows easily (using the result named at the end of the last paragraph) that the entire field F is spanned by an integral basis if now the coefficients are allowed to vary over $\mathbb{Q}$.

---

[3] See (Edwards 1980, p. 332) for further discussion of the seemingly lost origin of this idea, including the question of whether Kronecker might already have been using it as early as 1857.

For example, the set $\{1, \sqrt{2}\}$ forms an integral basis for the field $\mathbb{Q}(\sqrt{2})$. The algebraic integer $\sqrt{2} = 0 \cdot 1 + 1 \cdot \sqrt{2}$ is indeed a $\mathbb{Z}$-linear combination over this set, whereas the number $\frac{1+\sqrt{2}}{2}$ is not.

p-adic numbers

Let p be a fixed rational prime. We will now define $\mathbb{Q}_p$, *the p-adic completion of the rational numbers.*

Let us first say a few informal words regarding motivation. We begin with the observation that every nonnegative rational integer N has a base-p representation, for any positive rational prime p. For example the base-5 representation of 698 is $(10243)_5$, which we may be apt to write in the form

$$698 = 1 \cdot 5^4 + 0 \cdot 5^3 + 2 \cdot 5^2 + 4 \cdot 5^1 + 3 \cdot 5^0.$$

We will turn this expression around, however, and write it instead as a series in *ascending* powers of the prime 5,

$$698 = 3 \cdot 5^0 + 4 \cdot 5^1 + 2 \cdot 5^2 + 0 \cdot 5^3 + 1 \cdot 5^4,$$

in anticipation of the next idea, which is to generalize to *infinite* series of this form. We leave the full motivating story and development to TAZ Chapters 1 and 2, and simply note here that these infinite series are first motivated when we try to represent a *negative* rational integer N by a power series in p, with nonnegative modulo p reduced coefficients. After that, trying to represent rational numbers whose denominators are divisible by p motivates the idea of allowing the power series to begin with finitely many negative powers of p, like a Laurent series in the study of complex analysis. [4] Referring again to TAZ for the details, we leap now to the final result.

The field $\mathbb{Q}_p$ consists of all series of the form

$$c_\rho p^\rho + c_{\rho+1} p^{\rho+1} + c_{\rho+2} p^{\rho+2} + \cdots, \qquad c_\rho \neq 0$$

be they finite or infinite, where ρ is any integer – positive, negative, or zero – and where the coefficients c_i are modulo p reduced residues $0, 1, \ldots, p-1$. Such series may be referred to as

[4] Later, when we move to the p-adic completion $\mathbb{Q}_p(\alpha)$ of an algebraic number field we will move to power series in fractional powers of p, much like Puiseux series. These analogies were in no way lost on Hensel when he invented the p-adic numbers, but were rather a conscious motivation.

p-adic series or *p-adic numbers*. The number ρ is called the *order* of the p-adic number. In situations where the base p is obvious or implied, the series may be written in abbreviated fashion as

$$c_\rho\, c_{\rho+1} \ldots c_0, c_1\, c_2\, c_3 \ldots$$

for negative ρ, as

$$c_0, c_1\, c_2\, c_3 \ldots$$

when $\rho = 0$, and as

$$0, 0 \ldots 0 c_\rho\, c_{\rho+1}\, c_{\rho+2} \ldots$$

when ρ is positive.

The reader unfamiliar with the idea of the p-adic numbers may be alarmed by the divergence of these series. There are two solutions to this problem: one is to regard p-adic numbers merely as *formal* series; the other is to invent a new notion of size under which the distance of a growing p-adic series from some limit will be seen to *decrease* with each newly added term.

Hensel did in fact introduce such an alternative notion of magnitude, and, like all inventors of such radical notions, he argued for its reasonableness. Hensel philosophizes over the matter in the opening of Chapter 2 of TAZ, where, motivating the idea through a comparison to power series representations of functions in the study of analysis, he argues that the natural idea is to regard that p-adic number as smaller whose order ρ is larger. In that case, the partial sums

$$\begin{aligned} a_\rho &= c_\rho p^\rho \\ a_{\rho+1} &= c_\rho p^\rho + c_{\rho+1} p^{\rho+1} \\ a_{\rho+2} &= c_\rho p^\rho + c_{\rho+1} p^{\rho+1} + c_{\rho+2} p^{\rho+2} \\ &\ldots\ldots \end{aligned}$$

of a p-adic series will be converging to a limit L if the differences $a_\rho - L, a_{\rho+1} - L, a_{\rho+2} - L, \ldots$ are divisible by higher and higher powers of p.

Leaving the rigorous demonstration to Hensel, a few examples should suffice here to show that $\mathbb{Q}$ can be embedded in $\mathbb{Q}_p$; that is, that each rational number has a representation as a p-adic series. We have already seen how the nonnegative rational integer 698 could be represented by a finite 5-adic series. Consider now the 7-adic representation of -18.

According to Hensel's notion of convergence, we need to give a 7-adic series whose successive partial sums are congruent to -18 modulo correspondingly high powers of 7. We find:

$$\begin{aligned} 3 &\equiv -18 \bmod 7 \\ 3 + 4 \cdot 7 &\equiv -18 \bmod 7^2 \\ 3 + 4 \cdot 7 + 6 \cdot 7^2 &\equiv -18 \bmod 7^3 \\ 3 + 4 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 &\equiv -18 \bmod 7^4 \\ &\cdots\cdots \end{aligned}$$

and we see that $3, 46666\ldots$ is the 7-adic representation of -18. We note that the expansion is infinite, but repeating.

Consider next a fractional number, but not one whose denominator is divisible by 7. Take $1/6$. Since the denominator is relatively prime to 7, it has an inverse modulo every power of 7, and therefore the fraction $1/6$ has a meaning with respect to all these moduli. In this case, we find

$$\begin{aligned} 6 &\equiv 1/6 \bmod 7 \\ 6 + 5 \cdot 7 &\equiv 1/6 \bmod 7^2 \\ 6 + 5 \cdot 7 + 5 \cdot 7^2 &\equiv 1/6 \bmod 7^3 \\ &\cdots\cdots \end{aligned}$$

Incidentally, Hensel provides algorithms with which to compute these p-adic representations to any desired degree of accuracy in TAZ Chapter 2.

For one final example, we consider a fractional number whose denominator in least terms *is* divisible by 7, say, $a = -18/343$. In such a case, we begin by computing the power r of p that divides the denominator, and for this example we get 7^3. We then compute the p-adic representation of $p^r a$, and simply "shift" its digits r places to the left. We already determined that the 7-adic representation of -18 is $3, 4666666\ldots$, so for $-18/343$ we get immediately $3466, 6666\ldots$.

We have suggested by these examples that $\mathbb{Q}_p$ contains a number representing each rational number, as is in fact true. (See TAZ Chapter 2 §4.) Strictly speaking, however, it is incorrect to call $\mathbb{Q}$ a subfield of $\mathbb{Q}_p$, and to write $\mathbb{Q} \subseteq \mathbb{Q}_p$, since a rational number is not a p-adic series – they are two entirely different sorts of things. To be strictly correct, we can only say that $\mathbb{Q}_p$ contains a subfield *isomorphic to* $\mathbb{Q}$. (See any basic algebra text for

the notions of fields, subfields, and isomorphisms, e.g. Gallian 1998.) However, for the sake of simplicity we will choose to speak from here on out as though $\mathbb{Q}$ is a subfield of $\mathbb{Q}_p$, and will write $\mathbb{Q} \subseteq \mathbb{Q}_p$.

As for the reverse inclusion, does it hold as well, or are there p-adic numbers that are not equal to any rational number? The answer is that $\mathbb{Q}_p$ is in general much larger than $\mathbb{Q}$, containing in particular certain irrational algebraic numbers. For example, in Chapter 4 §6 of TAZ Hensel demonstrates that $\mathbb{Q}_p$ always contains all the $p-1^{\text{st}}$ roots of unity. On page 64 he notes that $\mathbb{Q}_5$ does not contain a square root of 2, but it does contain a cube root of 2. In fact (see TAZ, p. 39) all and only the elements of $\mathbb{Q}$ are equal to the *finite* or *infinite periodic* series in $\mathbb{Q}_p$, while all *infinite, non-repeating* p-adic numbers are irrational, resembling perfectly the familiar laws holding for decimal expansions of real numbers.

This completes our brief introduction to $\mathbb{Q}_p$, and for further reading we refer the reader to the first two chapters of TAZ. Modern treatments of the p-adic numbers abound, but in the author's opinion none is as good as the original!

Integrality in $\mathbb{Q}_p$

We saw before that when we passed from $\mathbb{Q}$ to an algebraic extension $F = \mathbb{Q}(\alpha)$, then a broader, more inclusive notion of integrality became appropriate; the set of integers was widened from $\mathbb{Z}$ to $\mathcal{O}_F$. Now that we have seen that $\mathbb{Q}_p$ is significantly larger than $\mathbb{Q}$, we should expect to once again need a suitable generalized definition of integrality for this broader domain.

This time, however, the extension will turn out to be much more radical. When we broadened $\mathbb{Z}$ to $\mathcal{O}_F$, this extension of the set of integers was *conservative*, in the sense that nothing that used to be non-integral became integral – the proper fractions in $\mathbb{Q}$ remained proper fractions. On the contrary, when we are finished defining the integers of $\mathbb{Q}_p$, we will find that many proper fractions in the subfield $\mathbb{Q}$ are to be regarded as integral in $\mathbb{Q}_p$.

Namely, any quotient $\frac{a}{b} \in \mathbb{Q}$ written in least terms, whose denominator is not divisible by p will be considered an integer in $\mathbb{Q}_p$. For example, $\frac{2}{3}$ is an integer in $\mathbb{Q}_5$, but not in $\mathbb{Q}_3$.

To give such a definition was a bold move by Hensel, representing a departure from the methodological beliefs of his predecessors. After Dedekind introduced the definition of algebraic integers in (Dedekind and Lejeune Dirichlet 1894), he moved immediately to a proof of conservativity:

> First of all we must confirm that the new, expanded concept of whole number can never be in contradiction with the old, narrower sense of the same word. [5]

Edwards (Edwards 1980, p. 332) suggests that Kronecker too looked for a definition of algebraic integer such that, "A rational number is an integer in the new sense if and only if it is an ordinary integer."

Returning to Hensel's definition of integers in $\mathbb{Q}_p$, there are two approaches that we can take as regards motivation: one is to describe the fruits that the new definition will bear, and in this direction we will give a preview of just one fact, namely, that Hensel's notion of integrality in $\mathbb{Q}_p$ will yield precisely the notion of divisibility that Kummer's theory of 1847 needed, as we will see below. The other approach, more accessible for the time being, is to argue that the definition we make will seem correct because it will cause our new structures to behave analogously to old, familiar ones – this is the same sort of motivation we gave for Dedekind's definition of integrality in $\mathbb{Q}(\alpha)$.

To that end we begin by recalling once again the fundamental theorem of arithmetic in $\mathbb{Z}$, but stating it this time more carefully. What it says is that (forgetting about the order in which factors are written) each whole number can be written uniquely as a product of primes and *units*, where a unit is defined to be an integer that divides 1. In $\mathbb{Z}$ there are only two units, namely 1 and -1, but among the integers of larger fields $\mathbb{Q}(\alpha)$ there may be a much wider variety of units. For example, $\sqrt{-1}$ is a unit in $\mathbb{Q}(\sqrt{-1})$, since $\left(\sqrt{-1}\right)\left(-\sqrt{-1}\right) = 1$, and $7 + 5\sqrt{2}$ is a unit in $\mathbb{Q}(\sqrt{2})$ since $\left(7 + 5\sqrt{2}\right)\left(-7 + 5\sqrt{2}\right) = 1$.

The key idea with the p-adic numbers $\mathbb{Q}_p$ is to recover the fundamental theorem of arithmetic in the special form that *p is prime, and every number not divisible by p is a unit*, and this is accomplished by defining integrality in $\mathbb{Q}_p$ in a very simple way: a p-adic number will be called *integral*, or *a p-adic integer* if and only if its p-adic order is nonnegative. That is, the integral p-adic numbers are those whose representation as a power series in p has p to a nonnegative power in the first term. For example,

$$2 \cdot 11^4 + 1 \cdot 11^5 + 0 \cdot 11^6 + 1 \cdot 11^7$$
$$7 \cdot 11^1 + 8 \cdot 11^2 + 7 \cdot 11^3 + 8 \cdot 11^4 + 7 \cdot 11^5 + 8 \cdot 11^6 + \cdots$$
$$3 \cdot 11^0 + 1 \cdot 11^1 + 4 \cdot 11^2 + 1 \cdot 11^3 + 5 \cdot 11^4 + 9 \cdot 11^5 + 2 \cdot 11^6 + 6 \cdot 11^7 + \cdots$$

[5] (Dedekind and Lejeune Dirichlet 1894, p. 524) *Vor Allem müssen wir uns versichern, dass der neue, erweiterte Begriff der ganzen Zahl mit dem alten, engeren Sinne desselben Wortes niemals in Widerspruch gerathen kann.*

are 11-adic integers, but

$$\frac{5}{11^3} + \frac{2}{11^2} + \frac{8}{11} + 3 \cdot 11^0 + 2 \cdot 11^1$$

is not.

After defining the multiplication of p-adic numbers, Hensel proves (TAZ, p. 28) that the order of a product of two p-adic numbers A and B is equal to the sum of the orders of A and B. For example, in the product

$$\begin{aligned}&(2 \cdot 11^4 + 1 \cdot 11^5 + 0 \cdot 11^6 + 1 \cdot 11^7)(\tfrac{5}{11^3} + \tfrac{2}{11^2} + \tfrac{8}{11} + 3 \cdot 11^0 + 2 \cdot 11^1) \\ &= 10 \cdot 11^1 + 9 \cdot 11^2 + 7 \cdot 11^3 + 9 \cdot 11^4 + 10 \cdot 11^5 + 10 \cdot 11^6 + 3 \cdot 11^7 + 2 \cdot 11^8\end{aligned}$$

the orders 4 and -3 of the factors sum to the order 1 of the product.

According to this result we see that p has the characteristic property of a prime number in $\mathbb{Q}_p$: if p divides a product, then it must divide one of the factors. For if p divides $A \cdot B$, then $(A \cdot B)/p$ is a p-adic integer, i.e. has nonnegative order. But viewing a p-adic number as a power series in p, it is obvious that dividing by p lowers the order by 1. Therefore the order of $A \cdot B$ must be at least 1. But since this is equal to the sum of the orders of A and B, we see that at least one of A and B must have order ≥ 1, and therefore be divisible by p, as was to be shown.

Hensel shows that a p-adic number in $\mathbb{Q}_p$ is a unit if and only if its order is 0, and states the fundamental theorem of arithmetic in $\mathbb{Q}_p$, that every p-adic number A can be written uniquely in the form

$$A = p^\rho E$$

where E is a p-adic unit. (Cf. TAZ pages 27 and 33.)

p-adic algebraic numbers $\mathbb{Q}_p(\alpha)$

We come now finally to the construction of a p-adic completion $\mathbb{Q}_p(\alpha)$ of an algebraic number field $F = \mathbb{Q}(\alpha)$. Following Hensel, we assume that $m_\alpha(x)$ is irreducible not only over $\mathbb{Q}$ but also over $\mathbb{Q}_p$. Supposing furthermore for simplicity's sake that F is, say, of degree 3 (the general development going similarly), we let $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ be an integral basis for F, and recall that an arbitrary number $\beta \in F$ has a representation

$$\beta = a\gamma^{(1)} + b\gamma^{(2)} + c\gamma^{(3)}$$

over this basis, with a, b, c in $\mathbb{Q}$. But a, b, c have representations as p-adic series:

$$\begin{aligned} a &= a_\rho p^\rho + a_{\rho+1} p^{\rho+1} + a_{\rho+2} p^{\rho+2} + \cdots \\ b &= b_\sigma p^\sigma + b_{\sigma+1} p^{\sigma+1} + b_{\sigma+2} p^{\sigma+2} + \cdots \\ c &= c_\tau p^\tau + c_{\tau+1} p^{\tau+1} + c_{\tau+2} p^{\tau+2} + \cdots \end{aligned}$$

which we may rewrite as

$$\begin{aligned} a &= a_\nu p^\nu + a_{\nu+1} p^{\nu+1} + a_{\nu+2} p^{\nu+2} + \cdots \\ b &= b_\nu p^\nu + b_{\nu+1} p^{\nu+1} + b_{\nu+2} p^{\nu+2} + \cdots \\ c &= c_\nu p^\nu + c_{\nu+1} p^{\nu+1} + c_{\nu+2} p^{\nu+2} + \cdots \end{aligned}$$

by setting ν to be the minimum of ρ, σ, τ, and allowing some of the lead coefficients in these series to be zero if necessary. We may then collect our representation $a\gamma^{(1)} + b\gamma^{(2)} + c\gamma^{(3)}$ of β with respect to powers of p, giving:

$$\begin{aligned} \beta \;=\; & \left(a_\nu \gamma^{(1)} + b_\nu \gamma^{(2)} + c_\nu \gamma^{(3)}\right) p^\nu + \left(a_{\nu+1} \gamma^{(1)} + b_{\nu+1} \gamma^{(2)} + c_{\nu+1} \gamma^{(3)}\right) p^{\nu+1} \\ & + \left(a_{\nu+2} \gamma^{(1)} + b_{\nu+2} \gamma^{(2)} + c_{\nu+2} \gamma^{(3)}\right) p^{\nu+2} + \cdots \end{aligned} \tag{A.1}$$

so that β now appears as a p-adic series of order ν whose coefficients are what we call *modulo p reduced algebraic integers of F*, that is, linear combinations of the elements $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ of the integral basis, with coefficients being modulo p reduced rational integers. Clearly in this case there are only p^3 modulo p reduced algebraic integers, and in general p^n, when the degree of F is n.

For example, the number field $\mathbb{Q}(\sqrt{2})$ has the integral basis $\{1, \sqrt{2}\}$, and the polynomial $x^2 - 2$ is irreducible over $\mathbb{Q}_5$, so every element of the 5-adic completion $\mathbb{Q}_5(\sqrt{2})$ can be represented in the form

$$(a_\nu + b_\nu\sqrt{2})5^\nu + (a_{\nu+1} + b_{\nu+1}\sqrt{2})5^{\nu+1} + (a_{\nu+2} + b_{\nu+2}\sqrt{2})5^{\nu+2} + \cdots$$

where $a_\nu, a_{\nu+1}, a_{\nu+2}, \ldots$ and $b_\nu, b_{\nu+1}, b_{\nu+2}, \ldots$ lie in the set $\{0, 1, 2, 3, 4\}$. Each of the coefficients $(a_\mu + b_\mu\sqrt{2})$ in this series is a modulo 5 reduced algebraic integer of $\mathbb{Q}(\sqrt{2})$.

Since a, b, c were rational numbers, however, the coefficients in the representation (A.1) of β must form either a terminating or a repeating sequence. We recall now that, when we considered terminating and repeating p-adic series whose coefficients were mere *rational* integers reduced modulo p, we thereby obtained only a new representation of the elements

of $\mathbb{Q}$; whereas when we allowed p-adic series that were non-terminating and non-repeating then we enlarged the domain to the new and larger field $\mathbb{Q}_p$. We now perform precisely the analogous enlargement of the algebraic number field $\mathbb{Q}(\alpha)$ by allowing non-terminating, non-repeating p-adic series with modulo p reduced *algebraic* integers of $\mathbb{Q}(\alpha)$ for coefficients. The resulting enlarged domain is called $\mathbb{Q}_p(\alpha)$. By dint of our assumption that $m_\alpha(x)$ is irreducible over $\mathbb{Q}_p$, it is a field, and, by an informality similar to the one discussed earlier, we will say that it contains $\mathbb{Q}(\alpha)$ as subfield, even though $\mathbb{Q}(\alpha)$ is in fact only embedded isomorphically in $\mathbb{Q}_p(\alpha)$.

The construction however is not yet done. While the field $F = \mathbb{Q}_p(\alpha)$ does consist of all and only the power series in p that we have just described, we will not continue to think of these p-adic algebraic numbers as power series in p, but instead as powers series in a different base $\pi \in \mathcal{O}_F$. The reason for this is that in general the presence of irrational algebraic numbers means that p may lose the characteristic property of a prime number, with respect to our chosen notion of integrality. As a consequence, we will lose the fundamental theorem of arithmetic in the form in which we stated it for $\mathbb{Q}_p$. A number $\pi \in \mathcal{O}_F$ can always be found, however, whose substitution for p will solve all of these problems; namely: (i) we will represent the elements of $\mathbb{Q}_p(\alpha)$ as power series in π instead of p (and will accordingly confine the power series coefficients to belong to a smaller set of reduced algebraic integers); (ii) we will say that an element of $\mathbb{Q}_p(\alpha)$ is integral if and only if its order as a power series in π is nonnegative; (iii) with respect to this new notion of integrality π will turn out to be prime, and all numbers not divisible by π will turn out to be units, so that we will once again have the special form of the fundamental theorem of arithmetic that we want in a p-adic field, namely, we will get the result (TAZ, p. 139) that every p-adic algebraic number $\beta \in \mathbb{Q}_p(\alpha)$ can be written uniquely in the form:

$$\beta = \varepsilon \pi^\rho,$$

where ε is a unit of $\mathbb{Q}_p(\alpha)$.

A simple example demonstrates the problem. Consider $F = \mathbb{Q}_3(\sqrt{3})$. Here, we have the integral basis $\left\{1, \sqrt{3}\right\}$, so that when the general element $\beta \in F$ is expanded as a power series in 3, it looks like:

$$\beta = \left(a_\rho + b_\rho\sqrt{3}\right) 3^\rho + \left(a_{\rho+1} + b_{\rho+1}\sqrt{3}\right) 3^{\rho+1} + \left(a_{\rho+2} + b_{\rho+2}\sqrt{3}\right) 3^{\rho+2} + \cdots,$$

where $a_\rho, a_{\rho+1}, a_{\rho+2}, \ldots$ and $b_\rho, b_{\rho+1}, b_{\rho+2}, \ldots$ lie in the set $\{0, 1, 2\}$. The element $\sqrt{3}$ has

the expansion

$$(0 + 1 \cdot \sqrt{3}) \cdot 3^0 + 0 + 0 + 0 + \cdots,$$

so that it is of order 0, and hence not divisible by 3. The product $\sqrt{3}\sqrt{3}$ is however divisible by 3, despite neither of its factors being divisible by 3, so that 3 fails to have the characteristic property of a prime number in $\mathbb{Q}_3(\sqrt{3})$. In this case, it turns out that we can take $\pi = \sqrt{3}$ as the prime number in F.

On pages 141 to 142 of TAZ Hensel gives a procedure whereby the prime number π can be computed. Its defining characteristic is quite simple, and is given in terms of *norm* functions, which we pause now to introduce. To give a preview: the prime number π will be characterized as any element of $\mathbb{Q}_p(\alpha)$ whose norm down to $\mathbb{Q}_p$ is of minimal positive p-adic order.

Let K be any field and suppose that $f(x)$ is an irreducible polynomial of degree n over K. Let α be an element such that $f(\alpha) = 0$. We are deliberately vague here about what α is. We only need α's algebraic properties with respect to K, which are entirely captured by the fact that the minimal polynomial of α is $f(x)$.

We consider the field $L = K(\alpha)$ and define the *norm from L down to K* as follows. For any element β in L, we have that the minimal polynomial of β over K is of degree m dividing n. We define the characteristic polynomial of β relative to L/K as

$$\chi_{L/K,\beta}(x) = m_\beta(x)^{n/m}.$$

We define

$$N_{L/K}(\beta) := (-1)^n \chi_{L/K,\beta}(0),$$

i.e., equal to the constant coefficient of the characteristic polynomial of β, up to sign. When the fields L and K are obvious from the context, we may omit them, and write simply 'N' for the norm.

It is straightforward to check that if $\chi_{L/K,\beta}$ has n different roots $\beta_1, \ldots, \beta_n$, then

$$N_{L/K}(\beta) = \beta_1 \cdots \beta_n.$$

In particular, if $K = \mathbb{Q}$ then we see that the norm we define here coincides with the usual definition, where the norm is defined to be the product of the conjugates.

The reason why we introduce this perhaps seemingly anachronistic notion of norm is that when we are considering field extensions of $\mathbb{Q}_p$, we do not have an algebraic closure readily available in which we can split any particular polynomial.

There is evidence in TAZ Chapter 7 § 2 that Hensel is aware of this problem to some extent. He notes that if $K = \mathbb{Q}_p$ and (in modern notation) $L = \mathbb{Q}_p(\alpha) = \mathbb{Q}_p[x]/k(x)$, where $k(x) \in \mathbb{Z}_p[x]$, then this field is isomorphic to $L^{(\delta)} = \mathbb{Q}_p[x]/k^{(\delta)}(x)$, where $k^{(\delta)} \in \mathbb{Z}[x]$ is the polynomial obtained from $k(x)$ by truncating the coefficients of $k(x)$ modulo $p^{\delta+1}$, where δ is the exponent of p in the discriminant of $k(x)$.

Elements in the field $L^{(\delta)}$, in their turn, can obviously be approximated by elements from the algebraic number field $\mathbb{Q}[x]/(k^{(\delta)})$, which we can embed in $\mathbb{C}$. Hensel also notes that norms can be read off from constant coefficients of characteristic equations, so we will use that as definition here and circumvent the technical difficulties that arise by trying to approximate p-adic fields by number fields for which a field containing an algebraic closure is readily available.

Returning now to the defining property of the prime number π in the field $\mathbb{Q}_p(\alpha)$, Hensel defines π to be any number in $\mathbb{Q}_p(\alpha)$ whose norm down to $\mathbb{Q}_p$ is of the smallest possible positive p-adic order in $\mathbb{Q}_p$. He shows (TAZ pages 141-142) that in fact we can always choose $\pi \in \mathcal{O}_{\mathbb{Q}(\alpha)}$. According to this definition we can confirm the example we gave earlier, of $\sqrt{3}$ as a prime number in $\mathbb{Q}_3(\sqrt{3})$. By definition, the norm of $\sqrt{3}$ is clearly -3, and has 3-adic order 1, which is certainly the smallest possible positive 3-adic order. This confirms that $\sqrt{3}$ functions as a prime number in $\mathbb{Q}_3(\sqrt{3})$.

In general, supposing the order of $N(\pi)$ is f, that is, supposing that p^f is the largest power of p that divides $N(\pi)$, then we have $1 \leq f$ by definition, and, since $N(p) = p^r$, we know that $f \leq r$. In fact we must have that $f \mid r$, since otherwise we would have $r = qf + c$ for some $0 < c < f$, and then p/π^q would be an element of $\mathbb{Q}_p(\alpha)$ having norm of order c, thus a lower positive order than that of π, contrary to our choice of π. We will use the fact that $f \mid r$ in the next section.

Hensel demonstrates (TAZ, pp. 139-140) that the property of having norm of minimal positive order is sufficient to guarantee that (i) π behaves as prime number in $\mathbb{Q}_p(\alpha)$ (that is, it divides a product if and only if it divides one of the factors); that (ii) all numbers not divisible by π are units; and that (iii) we get the fundamental theorem of arithmetic for $\mathbb{Q}_p(\alpha)$ in the form stated earlier, that every $\beta \in \mathbb{Q}_p(\alpha)$ can be written uniquely in the form

$$\beta = \varepsilon \pi^\rho$$

where ε is a unit in $\mathbb{Q}_p(\alpha)$.

In particular, $p \in \mathbb{Q}_p(\alpha)$ can be written in the form

$$p = \varepsilon_0 \pi^e$$

which is why we say figuratively that the power series in π look like series in a fractional power of p, in analogy to Puiseux series.

For a complete, detailed treatment of the construction of $\mathbb{Q}_p(\alpha)$, the reader is referred to Chapter 6 of TAZ.

A.2 Hensel's prime divisors

From here on, as an aid to those who might wish to compare the discussion in this Appendix with our two primary sources K1847 and TAZ, we will make an effort to use letters – Greek, Roman, and German – in a way as consistent as possible with both Kummer and Hensel. This is permitted only by the fact that Hensel appears to have attempted to do the same.

Certain alphabetic conventions have developed over the years quite generally in algebraic number theory, so that many of our choices will appear familiar to modern readers. One possibly jarring departure however is that from now on we will speak of q-adic, rather than p-adic numbers. When giving the basic development of these numbers in Chapters 1 through 6 of TAZ, Hensel did indeed use p, and π for a prime number in $\mathbb{Q}_p(\alpha)$; but in giving the general definition of a *divisor* in Chapter 7, he switched to q, and χ for a prime number in $\mathbb{Q}_q(\alpha)$, probably in reference to the prime q that Kummer used in K1847 throughout his definition of ideal prime factors. We therefore follow suit with both Kummer and Hensel in using q instead of p.

We will now set out the crucial part of Hensel's theory, in which he defines the *ideal prime divisors* $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_h$ of a given rational prime q, for a given algebraic number field $\mathbb{Q}(\alpha)$, and says what it means for an arbitrary number β in $\mathbb{Q}(\alpha)$ to be divisible by one or another of the $\mathfrak{q}_i$ to one power or another. In this we follow Chapter 7, §§3-4 of TAZ. In the subsequent section, we will set out the corresponding part of Kummer's theory, and will show how it is perfectly generalized by Hensel's.

To begin with, let an algebraic number α be given, and suppose its minimal polynomial $m_\alpha(x)$ over $\mathbb{Q}$ is of degree n. Let a rational prime q be given. Our first step is to compute the factorization of $m_\alpha(x)$ into irreducible factors over $\mathbb{Q}_q$, using Hensel's algorithm from

TAZ Chapter 4. We write

$$m_\alpha(x) = k_1(x)k_2(x)\cdots k_h(x) \qquad (q)$$

where the $k_i(x) \in \mathbb{Q}_q[x]$ are the irreducible factors of $m_\alpha(x)$ over $\mathbb{Q}_q$, and where the "(q)" on the right is simply a reminder that the equation holds in $\mathbb{Q}_q$.

Because $m_\alpha(x)$ falls into h irreducible factors over $\mathbb{Q}_q$, Hensel will say that there are precisely h *prime divisors* associated with q for the field $\mathbb{Q}(\alpha)$, and will denote these by $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_h$. Thus, there is one prime divisor $\mathfrak{q}_i$ corresponding to each irreducible factor $k_i(x)$.

Now letting an arbitrary $\beta \in \mathbb{Q}(\alpha)$ be given, our task is to say the precise power μ_i to which each prime divisor $\mathfrak{q}_i$ will be said to divide β. That is, we must define the power μ_i for which we will say that $\mathfrak{q}_i^{\mu_i}$ divides β (written $\mathfrak{q}_i^{\mu_i}|\beta$), but $\mathfrak{q}_i^{\mu_i+1}$ does not divide β, (written $\mathfrak{q}_i^{\mu_i+1} \nmid \beta$), which is expressed briefly by saying that $\mathfrak{q}_i^{\mu_i}$ *precisely divides* β, and is written $\mathfrak{q}_i^{\mu_i} \parallel \beta$. This is the moment when the inventor of the theory – Hensel in this case, and Kummer in the next section – must define things in the right way, in order to successfully achieve a "fundamental theorem of arithmetic" for ideal divisors.

Students of algebraic number theory familiar with the Dedekind-Hilbert theory of *ideals* may notice a subtle shift in emphasis here, in that instead of focusing on the way in which the prime q factors in $\mathbb{Q}(\alpha)$, we are instead asking for the powers to which the ideal factors of q divide any given number β. Were we to take $\beta = q$, then these two perspectives would coincide.

Let $k(x)$ now denote one of the irreducible polynomials $k_i(x)$, and $\mathfrak{q}$ the corresponding prime divisor $\mathfrak{q}_i$. Let r be the degree of $k(x)$. Hensel proceeds (TAZ Chapter 7 §§ 2-3) by truncating the q-adic coefficients of $k(x)$ modulo $q^{(\delta+1)}$, where δ is the q-adic order of the discriminant of $k(x)$, thus obtaining $k^{(\delta)}(x) \in \mathbb{Q}[x]$. This polynomial has roots $\gamma_1, \ldots, \gamma_r$ in $\mathbb{C}$ and Hensel shows that for each γ_j, the minimal polynomial $m_{\gamma_j}(x)$ is irreducible over $\mathbb{Q}_q$, so his construction of $\mathbb{Q}_q(\gamma_j)$ applies. Furthermore, he shows that $k(x)$ has a root $\xi_j \in \mathbb{Q}_q(\gamma_j)$ and that

$$k(x) = (x - \xi_1)\cdots(x - \xi_r) \qquad (q)\,.$$

In modern language this equality indeed holds in the ring $(\mathbb{Q}_q \otimes_{\mathbb{Q}} \mathbb{C})[x]$.

Hensel uses the ξ_j to build a q-adic analogue of conjugacy in the following way. Since $\beta \in \mathbb{Q}(\alpha)$, we can write β as a $\mathbb{Q}$-rational expression in α, i.e., there is a rational function $\varphi(x) \in \mathbb{Q}(x)$ such that $\beta = \varphi(\alpha)$. He obtains a q-adic conjugate of β in each of the $\mathbb{Q}_q(\gamma_j)$

by considering $\beta_j = \varphi(\xi_j)$. Let χ_j be a prime number in $\mathbb{Q}_q(\gamma_j)$. He shows that there is a single μ such that the χ_j-adic order of β_j is μ for all $1 \leq j \leq r$, and *he defines μ to be the power to which the prime divisor $\mathfrak{q}$ divides β.* This is the fundamental definition in Hensel's theory of prime divisors.

Other key definitions in Hensel's theory are the *norm*, *degree*, and *order* of the prime divisor $\mathfrak{q}$. (See TAZ, p. 143).) If q^f is the power of q dividing $N(\chi_j)$ for all j from 1 to r (by construction, they are all the same), then we define the *norm* of $\mathfrak{q}$ to be q^f, and we define the *degree* of $\mathfrak{q}$ to be f. Recalling that we must have $f \mid r$, and setting $ef = r$, we define e to be the *order* of $\mathfrak{q}$. We note in passing that the degree and order of a prime divisor in Hensel's theory coincide with the inertia degree and ramification index of a prime ideal in Hilbert ramification theory (Hilbert 1897, Ch. 10).

Proceeding in the way shown above, we determine the power μ_i to which each prime divisor $\mathfrak{q}_i$ of q divides β. The distinct prime divisors associated to a given rational prime are considered to be relatively prime to one another, so we write that

$$\mathfrak{q}_1^{\mu_1}\mathfrak{q}_2^{\mu_2}\cdots\mathfrak{q}_h^{\mu_h} \parallel \beta.$$

We close this section with a brief indication of how it is that Hensel's definition of prime divisors provides him with a "fundamental theorem of arithmetic", i.e. allows him to "save unique factorization" in Kummer's sense. A key observation is that only finitely many rational primes p can be such that any of their prime divisors divide β to a positive or negative power, as Hensel proves in TAZ Chapter 7 § 4. Supposing that β is an algebraic integer, let $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots, \mathfrak{t}$ be all the prime divisors that divide β to a positive power. Here we do not make any distinction as to whether these prime divisors belong to one or to many different rational primes. If the powers to which $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots, \mathfrak{t}$ divide β are $h, k, l, \ldots, m$, then Hensel expresses this by writing

$$\beta \sim \mathfrak{p}^h\mathfrak{q}^k\mathfrak{r}^l\cdots\mathfrak{t}^m.$$

Hensel calls the expression on the right the *divisor* of β, and he proves that each algebraic integer has a unique divisor. This is the fundamental theorem of arithmetic for divisors.

Let γ now be another algebraic integer belonging to the same field $\mathbb{Q}(\alpha)$, and suppose that

$$\gamma \sim \mathfrak{p}^{h'}\mathfrak{q}^{k'}\mathfrak{r}^{l'}\cdots\mathfrak{t}^{m'}$$

where we now allow that some of the $h', k', l', \ldots, m'$ may be zero, if necessary, so that $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots, \mathfrak{t}$ are the same prime divisors that divide β. Hensel demonstrates that in this

case γ divides β in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ if and only if $h' \leq h, k' \leq k, l' \leq l, \ldots, m' \leq m$. This shows that that the fundamental theorem of arithmetic for divisors has the expected consequences for divisibility.

For full details, the reader is referred to Chapter 7 of TAZ.

A.3 Kummer's prime divisors

For λ a positive rational prime, and α a solution of the equation $\alpha^\lambda = 1$, with $\alpha \neq 1$, Kummer is concerned in K1847 with the integers of the field $\mathbb{Q}(\alpha)$. Such a field, today called a cyclotomic field, has an especially simple integral basis, namely $\alpha, \alpha^2, \ldots, \alpha^{\lambda-1}$, so that $\mathcal{O}_{\mathbb{Q}(\alpha)}$ is obtained as the set of all expressions of the form

$$a_1\alpha + a_2\alpha^2 + \cdots + a_{\lambda-1}\alpha^{\lambda-1},$$

where $a_1, a_2, \ldots, a_{\lambda-1} \in \mathbb{Z}$. $\mathcal{O}_{\mathbb{Q}(\alpha)}$ is therefore equal to the ring $\mathbb{Z}[\alpha]$ of all polynomials in α with coefficients in $\mathbb{Z}$.

Fixing a rational prime q different from λ, we will review the definition Kummer gave of the ideal prime divisors of q. The case $q = \lambda$ requires a special treatment, and Kummer handles it separately. We are interested in the more general construction for $q \neq \lambda$, and its comparison to Hensel's construction.

Such a prime q has an *order* with respect to λ, which is the smallest positive integer f such that

$$q^f \equiv 1 \bmod \lambda.$$

The order f of q must be a divisor of $\lambda - 1$, and we set $e = (\lambda - 1)/f$.

Fundamental to Kummer's theory are *the e periods $\eta_0, \eta_1, \ldots, \eta_{e-1}$ of length f*, which we define next. The periods had been studied earlier by Gauss, in the *Disquisitiones Arithmeticae*, and in K1847 Kummer relies in a couple of places on Gauss's results, one example of which we will see below. Taking γ to be any primitive residue mod λ, that is, a remainder mod λ such that $\gamma^0, \gamma^1, \gamma^2, \ldots, \gamma^{\lambda-2}$ represent each of the $\lambda - 1$ nonzero residues mod λ,

Kummer defines

$$\begin{aligned}
\eta_0 &= \alpha^{\gamma^0} + \alpha^{\gamma^e} + \alpha^{\gamma^{2e}} + \cdots + \alpha^{\gamma^{(f-1)e}} \\
\eta_1 &= \alpha^{\gamma^1} + \alpha^{\gamma^{e+1}} + \alpha^{\gamma^{2e+1}} + \cdots + \alpha^{\gamma^{(f-1)e+1}} \\
\eta_2 &= \alpha^{\gamma^2} + \alpha^{\gamma^{e+2}} + \alpha^{\gamma^{2e+2}} + \cdots + \alpha^{\gamma^{(f-1)e+2}} \\
&\vdots \\
\eta_{e-1} &= \alpha^{\gamma^{e-1}} + \alpha^{\gamma^{2e-1}} + \alpha^{\gamma^{3e-1}} + \cdots + \alpha^{\gamma^{fe-1}}.
\end{aligned}$$

We will occasionally write η for η_0. We define $R = \mathbb{Z}\eta_0 + \cdots + \mathbb{Z}\eta_{e-1}$, i.e. the ring of all algebraic integers in $\mathbb{Q}(\eta)$ of the form $a_0\eta_0 + \cdots + a_{e-1}\eta_{e-1}$ for $a_0, \ldots, a_{e-1} \in \mathbb{Z}$.

Throughout this section, we will introduce modern notation to handle situations which Kummer dealt with in other ways. As was the case with Hensel, Kummer did not speak of isomorphisms (he did not have this language available to him), but instead in terms of substitutions. We introduce the automorphism $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ which maps α to α^γ, and fixes $\mathbb{Q}$, and the automorphism $\tau : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ defined by $\tau = \sigma^e$. We note that σ permutes the periods η_i cyclically, and that τ cyclically permutes the terms belonging to any single period.

We now take a detour through Hensel's theory, employing modern tools like Galois theory along the way, before returning to Kummer's development. We need the infrastructure with which to compare Kummer's and Hensel's theories. From our present perspective, we know from the well-developed theory of cyclotomic fields (see e.g. (Hilbert 1897, Ch. 21)) that q splits in $\mathbb{Q}(\alpha)$ as the product of e prime divisors each of degree f and order 1. Then, going to Hensel's theory of prime divisors, it must be that $\Phi_\lambda(x)$, the λ^{th} cyclotomic polynomial and the minimal polynomial for α, factors in $\mathbb{Q}_q$ as

$$\Phi_\lambda(x) = k_0(x)k_1(x)\cdots k_{e-1}(x) \qquad (q)$$

where each of the $k_i(x)$ is a polynomial of degree f.

Taking $k(x)$ to be any of the $k_i(x)$, say $k_1(x)$, we perform Hensel's construction of a root of $k(x)$. Truncating the q-adic coefficients of $k(x)$ modulo $q^{\delta+1}$, where δ is the q-adic order of the discriminant of $k(x)$, we obtain $k^{(\delta)}(x) \in \mathbb{Q}[x]$, which is irreducible not just over $\mathbb{Q}$ but also over $\mathbb{Q}_q$. Let $\gamma \in \mathbb{C}$ be a root of $k^{(\delta)}(x)$. Then $k^{(\delta)}(x) = (x-\gamma)\,g(x)$ for some $g(x) \in \mathbb{Q}(\gamma)[x]$. Then by Hensel's lemma this factorization lifts to a factorization $k(x) = (x-\xi)\,\bar{g}(x)$, for some $\bar{g}(x) \in \mathbb{Q}_q[\gamma][x]$, and $\xi \in \mathbb{Q}_q[\gamma]$. Note that since $k^{(\delta)}(x)$ is irreducible over $\mathbb{Q}_q$, we have that $\mathbb{Q}_q[\gamma]$ is a field.

Since $k(\xi) = 0$, we have $\Phi_\lambda(\xi) = 0$ as well, that is, the field $\mathbb{Q}_q[\gamma]$ contains a primitive λ^{th} root of unity ξ. Therefore it contains all λ^{th} roots of unity, since ξ generates the rest. So $\Phi_\lambda(x)$ splits in $\mathbb{Q}_q[\gamma]$, and so does each $k_i(x)$. In particular, we may define the e periods of length f in $\mathbb{Q}_q[\gamma]$:

$$\begin{aligned}
U_0 &= \xi^{\gamma^0} + \xi^{\gamma^e} + \xi^{\gamma^{2e}} + \cdots + \xi^{\gamma^{(f-1)e}} \\
U_1 &= \xi^{\gamma^1} + \xi^{\gamma^{e+1}} + \xi^{\gamma^{2e+1}} + \cdots + \xi^{\gamma^{(f-1)e+1}} \\
U_2 &= \xi^{\gamma^2} + \xi^{\gamma^{e+2}} + \xi^{\gamma^{2e+2}} + \cdots + \xi^{\gamma^{(f-1)e+2}} \\
&\vdots \\
U_{e-1} &= \xi^{\gamma^{e-1}} + \xi^{\gamma^{2e-1}} + \xi^{\gamma^{3e-1}} + \cdots + \xi^{\gamma^{fe-1}}.
\end{aligned}$$

Since each $k_i(x)$ splits in $\mathbb{Q}_q[\gamma]$, whereas $k_i(x)$ is irreducible of degree f over $\mathbb{Q}_q$, and $\mathbb{Q}_q[\gamma]$ is degree f over $\mathbb{Q}_q$, $k_i(x)$ cannot split in any proper subfield of $\mathbb{Q}_q[\gamma]$, so the latter is in fact a splitting field for $k_i(x)$. Therefore it is Galois over $\mathbb{Q}_q$, and we get a group G of f automorphisms $\phi_1, \ldots, \phi_f$ of $\mathbb{Q}_q[\gamma]$ that fix $\mathbb{Q}_q$.

Meanwhile, we have a field embedding $\varepsilon : \mathbb{Q}(\alpha) \to \mathbb{Q}_q[\gamma]$ which sends α to ξ, and which satisfies $\varepsilon|_{\mathbb{Q}} = \iota$, where ι is the canonical embedding of $\mathbb{Q}$ into $\mathbb{Q}_q$ which Hensel discusses in TAZ Chapter 2 § 5. Now if $E = \varepsilon(\mathbb{Q}(\alpha))$, then it is clear that all powers of ξ must lie in E. Moreover, since each ϕ_i fixes $\mathbb{Q}_q$ and hence also $\mathbb{Q}$, it must permute the roots of $\Phi_\lambda(x)$, and so each $\phi_i(\xi)$ is a power of ξ and belongs to E. Therefore we can define f automorphisms $\rho_i : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ by $\rho_i = \varepsilon^{-1}\phi_i\varepsilon$. Then the ρ_i form a group, namely the unique subgroup of order f in $\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q})$, which is $\langle\tau\rangle$. Then each ϕ_i equals $\varepsilon\tau^{c_i}\varepsilon^{-1}$ for some power c_i, which says that G fixes each of $U_0, \ldots, U_{e-1}$, so that these must lie in the fixed field $\mathbb{Q}_q$.

Therefore for $i = 0, 1, \ldots, e-1$ we can define a field embedding

$$S_i : \mathbb{Q}(\eta) \to \mathbb{Q}_q$$

by stipulation that $S_i(\eta_0) = U_i$, and $S_i|_{\mathbb{Q}} = \iota$. Then S_i is just the common restriction to $\mathbb{Q}(\eta)$ of each $\varepsilon\tau^j\sigma^i : \mathbb{Q}(\alpha) \to \mathbb{Q}_q[\gamma]$, for $0 \le j < f$. We will also write S_i for the map $\varepsilon\sigma^i$, with no risk of confusion. The relevant field lattice is diagrammed in Figure A.1, where the labels on the edges denote the degrees of field extensions.

In K1847 Kummer used a precursor to the embeddings S_i without fully realizing them. Namely, Kummer observed that if he took $g(y)$ to be the minimal polynomial for the periods η_i, and if he considered the congruence $g(y) \equiv 0 \bmod q$, then this congruence had e roots

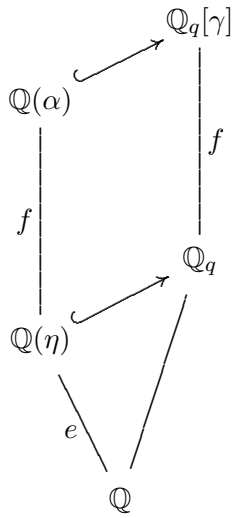

Figure A.1: Field lattice for Henselian treatment of a cyclotomic field.

among the residue classes mod q, which he referred to as $u_0, u_1, \ldots, u_{e-1}$ (K1847, p. 330). Where he used the remainders u_i mod q in his theory, we are going to use our $U_i \in \mathbb{Q}_q$, so that, in a sense, where Kummer only realized that the periods η_i could be represented mod q, we have realized that they can be represented mod arbitrarily high powers of q (cf. (Weyl 1940, pp. 87-88)). Where Kummer substituted u_i for η_0, we will apply a mapping S_i. Kummer too needed to perform substitutions not just on elements of the ring $R = \mathbb{Z}\eta_0 + \cdots + \mathbb{Z}\eta_{e-1}$ that we defined earlier, but more generally on elements of $\mathbb{Z}[\alpha]$, and for this he relied on a result (K1847, p. 337), based on Article 348 of the *Disquisitiones Arithmeticae*. Namely, each element of $\mathbb{Z}[\alpha]$ has a unique representation in the form

$$\varphi_0 + \alpha\varphi_1 + \alpha^2\varphi_2 + \cdots + \alpha^{f-1}\varphi_{f-1}$$

where $\varphi_0, \varphi_1, \ldots, \varphi_{f-1}$ belong to R. Once an element $\beta \in \mathbb{Z}[\alpha]$ is brought into this form, Kummer could substitute u_i for η_0 in each φ_j.

We next define three important norm maps. With $\phi_0, \phi_1, \ldots, \phi_{f-1}$ as defined above, we define $N_1 : \mathbb{Q}_q[\gamma] \to \mathbb{Q}_q$ for all $\beta \in \mathbb{Q}_q[\gamma]$ by

$$N_1(\beta) = \prod_{j=0}^{f-1} \phi_j(\beta).$$

Furthermore we define $\bar{N}_1 : \mathbb{Q}(\alpha) \to \mathbb{Q}(\eta)$ for all $\beta \in \mathbb{Q}(\alpha)$ by

$$\bar{N}_1(\beta) = \prod_{j=0}^{f-1} \tau^j(\beta),$$

naming it thus in order to recall the correspondence $\phi_j = \varepsilon\tau^{c_j}\varepsilon^{-1}$; and finally $N_0 : \mathbb{Q}(\eta) \to \mathbb{Q}$ for all $\beta \in \mathbb{Q}(\eta)$ by

$$N_0(\beta) = \prod_{i=0}^{e-1} \sigma^i(\beta).$$

We note that of these norms, Kummer spoke only of N_0 (calling it N). The commutativity of the following diagram

$$\begin{array}{ccc} \mathbb{Q}(\alpha) & \xhookrightarrow{S_i} & \mathbb{Q}_q[\gamma] \\ \Big\downarrow{\scriptstyle \bar{N}_1} & & \Big\downarrow{\scriptstyle N_1} \\ \mathbb{Q}(\eta) & \xhookrightarrow[S_i]{} & \mathbb{Q}_q \end{array}$$

is easily confirmed.

After this long detour we can now return to Kummer. In (K1847, § 3), he shows how we can compute a number $\psi \in \mathbb{Z}[\alpha] \cap \mathbb{Q}(\eta)$ such that $N_0(\psi)$ is divisible by q but not by q^2. This number is crucial in Kummer's definition of ideal prime divisors. Since the N_0 norm of ψ is divisible by q precisely once, we know that among $S_0(\psi), S_1(\psi), \ldots, S_{e-1}(\psi)$ exactly one will have q-adic order 1, while all the rest have q-adic order 0. For Kummer, this condition was expressed in terms of making substitutions of his u_i for the periods η_i in the expression for ψ, and in terms of the resulting congruences mod q. Kummer adds (in his own language) that we can in fact choose ψ so that specifically $S_0(\psi)$ has q-adic order 1, while $S_1(\psi), \ldots, S_{e-1}(\psi)$ are of order 0. Using $|\cdot|_q$ to denote q-adic order, this is expressed as

$$\begin{aligned} &|S_0(\psi)|_q = 1 \\ &|S_i(\psi)|_q = 0 \text{ for } i \text{ from 1 to } e-1. \end{aligned} \tag{A.2}$$

We assume that ψ is so chosen, and we define

$$\psi_0 = S_0(\psi) \in \mathbb{Q}_q[\gamma].$$

The defining condition on ψ, that its norm be divisible by q but minimally so, should remind us of the defining condition on Hensel's prime numbers χ in q-adic algebraic fields, i.e. that their norm be of minimal positive q-adic order. This is no mere coincidence, as it turns out that for cyclotomic fields, *Kummer's ψ_0 can play the role of Hensel's prime number χ*.

To see this, we begin by recalling that from the general theory of cyclotomic fields we know that the prime divisors belonging to q are all of degree f, which means that the prime number $\chi \in \mathbb{Q}_q[\gamma]$ is characterized as any element of this field whose norm $N_1(\chi)$ down to $\mathbb{Q}_q$ is precisely divisible by q^f. But we have

$$\begin{aligned} N_1(\psi_0) &= N_1(S_0(\psi)) \\ &= S_0(\bar{N}_1(\psi)) \\ &= S_0(\psi^f) \\ &= S_0(\psi)^f \\ &= \psi_0^f. \end{aligned}$$

Therefore

$$\begin{aligned} |N_1(\psi_0)|_q &= \left|\psi_0^f\right|_q \\ &= f\,|\psi_0|_q \\ &= f, \end{aligned}$$

using (A.2). This confirms that Kummer's ψ_0 is a prime number in $\mathbb{Q}_q[\gamma]$ in Hensel's sense.

We come now at last to Kummer's own definition of ideal prime divisors. He was investigating the irreducible numbers in R that divided a rational prime q of order f mod λ, and he observed (K1847, § 6) that *if there was* a number $\varphi \in R$ with $N_0\varphi = q$, then the conjugates $\varphi, \sigma\varphi, \sigma^2\varphi, \ldots, \sigma^{e-1}\varphi$ were the irreducible factors of q. He noted moreover that for each $0 \le i \le e-1$ there was some $0 \le r \le e-1$ such that, for any number $\beta \in \mathbb{Z}[\alpha]$,

$$\sigma^i\varphi \mid \beta \implies S_r(\beta) \equiv 0 \bmod q \tag{A.3}$$

although, again, for Kummer $S_r(\beta)$ only meant the substitution of his u_i for the η_i in β. Finally, in reference to the above implication, he made the comment with which he introduced ideal prime factors to the mathematical world. We reproduce it here, translating

both into English, and into the formalism we have been using up to this point. The original is reproduced in the footnote. Interpolations and uses of our alternative formalism are enclosed in brackets.

> A converse of this theorem [(A.3)] cannot be immediately established; for in many cases there exists no such prime factor $[\varphi]$ of q, whereas the congruence condition $[S_r(\beta) \equiv 0 \mod q]$ is actually fulfilled. This congruence condition however, as the enduring property of a complex number $[\beta]$, independent of the haphazard question whether q can be represented as the product of e conjugate complex numbers, shall now be used as the definition of complex prime factors, which themselves then either can be represented by actual complex numbers, or just as well not; in which last case they will be called *ideal* prime factors. [6]

The idea then was that, if, using a notation like Hensel's (which Kummer did not use), the prime factors belonging to the rational prime q were called $\mathfrak{q}_0, \mathfrak{q}_1, \ldots, \mathfrak{q}_{e-1}$, then we would say that β was divisible by $\mathfrak{q}_i$ just in case we had $S_i(\beta) \equiv 0 \mod q$. The coincidence of this notion with Hensel's is already almost apparent. For, noting that by definition of the embeddings S_i we have $S_i(\beta) = S_0(\sigma^i\beta)$, we see already that divisibility of β by $\mathfrak{q}_i$ is a matter of a certain conjugate of β having a q-adic representation of positive order.

In order to say the precise power μ to which one of the prime divisors $\mathfrak{q}$ would divide β, however, Kummer gave (K1847, § 5) an alternative condition, which was equivalent to $S_i(\beta) \equiv 0 \mod q$, and was more easily extended to the case in which $\mathfrak{q}$ was contained in β more than once. Namely, this was where Kummer made use of the number ψ. His definition (K1847, pp. 342-343) stated that $\mathfrak{q}_i^\mu$ would be said to divide β just in case

$$q^\mu \mid \beta \left(\frac{N_0\psi}{\sigma^{e-i}\psi} \right)^\mu$$

with this last division taking place over $\mathbb{Z}[\alpha]$.

Let us think about what this condition means. By choice of ψ, the factor $(N_0\psi)^\mu$ in the numerator on the right is divisible precisely by q^μ. Therefore Kummer's condition will be

---

[6](K1847, p. 342): *Eine Umkehrung dieses Satzes lässt sich nicht ohne Weiteres aufstellen; denn in vielen Fällen existiert ein solcher Primfactor von q nicht, während die Congruenzbedingung* $f(\alpha) \equiv 0, \mod q$ *für* $\eta = u_r$ *wirklich erfüllt wird. Diese Congruenzbedingung aber, als die bleibende und jener Zufälligkeit, ob q sich als Product von e conjugirten complexen Zahlen darstellen lasse, nicht unterworfene Eigenschaft einer complexen Zahl, soll nun als Definition der complexen Primfactoren benutzt werden, welche selbst sodann entweder als wirkliche complexe Zahlen für sich darstellbar sein können, oder auch nicht; in welchem letzteren Falle sie* ideale *Primfactoren genannt werden sollen.*

satisfied if $\sigma^{e-i}\psi$ divides β over $\mathbb{Z}[\alpha]$, but in fact this divisibility is just slightly too strong: it implies Kummer's condition, but is not implied by it. What Kummer's condition implies is a weaker form of divisibility. Namely, it simply says that *in the quotient $\beta/\sigma^{e-i}\psi$ there are not more factors of q in the denominator than there are in the numerator.* On reflection we realize that this is precisely Hensel's notion of divisibility, i.e. q-adic divisibility. In Hensel's q-adic sense, $\sigma^{e-i}\psi$ divides β just in case the quotient $\beta/\sigma^{e-i}\psi$ has nonnegative order in $\mathbb{Q}_q[\gamma]$. (I do not claim that Hensel was actually motivated by such an observation.)

Finally, let us complete our comparison of Kummer and Hensel by showing how easily Kummer's condition can be transformed into Hensel's. Since $N_0\psi$ is divisible by q precisely once, we set $N_0\psi = qr$, where $r \in \mathbb{Z}$ and $q \nmid r$. Let $\beta = \varphi(\alpha) \in \mathbb{Z}[\alpha]$ be given. Note that for any embedding S_i we have

$$S_i(\beta) = S_i(\varphi(\alpha)) = \varphi(S_i(\alpha)) = \varphi(\xi^{\gamma^i}).$$

Then

$$\begin{aligned}
& \mathfrak{q}_i^\mu \mid \beta \quad \text{in Kummer's sense} \\
\iff \quad & q^\mu \mid \beta \left(\tfrac{N_0\psi}{\sigma^{e-i}\psi}\right)^\mu \text{ over } \mathbb{Z}[\alpha] \\
\iff \quad & q^\mu \mid \left(\sigma^i\beta\right) \left(\tfrac{N_0\psi}{\psi}\right)^\mu \text{ over } \mathbb{Z}[\alpha] \\
\iff \quad & \exists \gamma \in \mathbb{Z}[\alpha] : q^\mu\gamma = \left(\sigma^i\beta\right) \tfrac{q^\mu r^\mu}{\psi^\mu} \\
\iff \quad & \exists \gamma \in \mathbb{Z}[\alpha] : \tfrac{\gamma}{r^\mu}\psi^\mu = \sigma^i\beta \\
\iff \quad & \exists \delta \in \mathbb{Z}_q[\alpha] : \delta\psi^\mu = \sigma^i\beta \\
\iff \quad & \exists \delta \in \mathbb{Z}_q[\alpha] : S_0(\delta)\psi_0^\mu = S_i\beta \\
\iff \quad & \exists \delta \in \mathbb{Z}_q[\alpha] : S_0(\delta)\psi_0^\mu = \varphi(\xi^{\gamma^i}) \\
\iff \quad & \psi_0^\mu \mid \varphi(\xi^{\gamma^i}) \text{ over } \mathbb{Z}_q[\gamma] \\
\iff \quad & \mathfrak{q}_i^\mu \mid \beta \quad \text{in Hensel's sense.}
\end{aligned}$$

A.4 Conclusions

We have seen how Hensel's notion of integrality in p-adic fields provided precisely the notion of divisibility needed to explain Kummer's definition of divisibility by ideal prime divisors. We saw that Kummer's substitutions of his residues u_i mod q for the η_i in elements of the ring R were really just a precursor of embeddings of $\mathbb{Q}(\eta)$ into the q-adic field $\mathbb{Q}_q$. We saw that Kummer's ψ, when embedded as $\psi_0 \in \mathbb{Q}_q[\gamma]$, was the same as Hensel's prime number χ in the case of a cyclotomic field, and finally we saw how easy and straightforward it was to transform Kummer's relation $\mathfrak{q}_i^\mu \mid \beta$ into Hensel's relation $\mathfrak{q}_i^\mu \mid \beta$.

As for Kummer's analogy with chemistry, he went on:

> In chemistry furthermore, in order to test the substances contained in an unknown dissolved compound, one has reagents, which give precipitates, from which the presence of various substances can be recognized. Precisely the same thing occurs with the complex numbers; for the complex numbers denoted by Ψ above are like the reagents for the ideal prime factors, and the real prime number q, which, after multiplication with such, appears as a factor in the product, is precisely the same as the insoluble precipitate, which after application of the reagent falls to the bottom. (Kummer 1847b, p. 360)

The analogy is quite good. A simple chemical reaction of the kind Kummer discussed would take place if, unknown to us, NaF was dissolved in a beaker of water, and we added $\mathsf{MgCl_2}$ as a reagent, causing $\mathsf{MgF_2}$ to precipitate out, according to the reaction formula

$$\mathsf{MgCl_2} + 2\mathsf{NaF} \to \mathsf{MgF_2} + 2\mathsf{NaCl}.$$

If we could recognize the $\mathsf{MgF_2}$ precipitate, we would know that F had been present in the unknown solute.

Similarly, Edwards notes (Edwards 1977, pp. 105-106) that for the case $\lambda = 23$, that is, for the ring of integers built out of 23^{rd} roots of unity, Kummer proved that there is no complex integer having the prime $q = 47$ for norm, but determined that

$$\beta = \alpha^{10} + \alpha^{-10} + \alpha^8 + \alpha^{-8} + \alpha^7 + \alpha^{-7}$$

has norm 47^2. We therefore should expect that β contains an ideal prime factor of 47. Edwards notes that the number

$$\psi(\alpha) = 1 - \alpha + \alpha^{-2}$$

has norm $47 \cdot 139$, which is divisible by 47 exactly once. Since $q = 47 \equiv 1 \bmod 23$, we have $f = 1$ and $e = 22$. Therefore let us define $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_{22}$ to be the 22 ideal prime factors of 47, where $\mathfrak{q}_i$ is that ideal prime factor whose presence is detected by the "reagent"

$$\Psi_i = \frac{N\psi(\alpha)}{\psi(\alpha^i)}.$$

Then by experimentation using MAPLE we discover that $47 \mid \Psi_7\beta$ over $\mathbb{Z}[\alpha]$; namely, we find that

$$\Psi_7\beta = 47\gamma,$$

where

$$\gamma = -57\alpha^{21} + 5\alpha^{20} - 60\alpha^{19} - 21\alpha^{18} + 39\alpha^{17} + 3\alpha^{16} + 108\alpha^{15} + 45\alpha^{14} + 55\alpha^{13} + 49\alpha^{12} - 3\alpha^{11} + 56\alpha^{10} - 35\alpha^{9} - 36\alpha^{8} + 48\alpha^{7} - 58\alpha^{6} - 50\alpha^{5} - 27\alpha^{4} - 152\alpha^{3} - 77\alpha^{2} - 122\alpha - 95.$$

Thus, in summary, the reaction

$$\mathsf{MgCl_2} + 2\mathsf{NaF} \rightarrow \mathsf{MgF_2} + 2\mathsf{NaCl}$$

is mirrored by the equation

$$\Psi_7\beta = 47\gamma,$$

in the following way. The number β is like the compound NaF. We believe that β contains an ideal prime factor $\mathfrak{q}_i$ of 47, as the chemists of 1846 believed that NaF contained the "hypothetical radical" F. As the chemists would add $\mathsf{MgCl_2}$, we multiply by Ψ_7. (Or they might try a different reagent, like $\mathsf{Ba(NO_3)_2}$, and we might try a different conjugate Ψ_j, some $j \neq 7$.) And as the precipitate $\mathsf{MgF_2}$ indicates the presence of F, leaving NaCl behind, likewise the rational prime factor 47 indicates the presence of $\mathfrak{q}_7$, leaving the factor γ behind. See Table A.1.

β	NaF
$\mathfrak{q}_i$	F
Ψ_7	$\mathsf{MgCl_2}$
47	$\mathsf{MgF_2}$
$\mathfrak{q}_7$	F
γ	NaCl

Table A.1: Correspondence for an example of Kummer's chemistry analogy.

As for Hensel, his generalization made Kummer's methods applicable to the "chemistry" of all number fields, not just cyclotomic. The factorization algorithm for which he introduced Hensel's lemma in TAZ Chapter 4 made it possible to compute any number field's "periodic table", i.e. to compute how many ideal prime divisors were assigned to any given rational prime; and his procedure for computing prime numbers π on TAZ pages 141-142 gave a way to manufacture "reagents". In this way he carried on Kummer's tradition in which algebraic number theory sometimes looked like an empirical science, where it was possible to run tests and see results.

Appendix B

Hasse's first paper on $\mathbb{Q}(\sqrt{-47})$

On the Class Field of the Quadratic Number Field with Discriminant -47

Helmut Hasse

7 February 1964

Among imaginary quadratic number fields $\Omega = \mathbb{Q}(\sqrt{d})$ with prime discriminant $d = -p\,(\equiv 1 \mod 4)$ and odd class number h, the first cases with $h > 1$ are well known:

$$d = -23 \qquad h = 3,$$
$$d = -31 \qquad h = 3,$$
$$d = -47 \qquad h = 5.$$

In general the class field N of Ω is normal over the rational number field $\mathbb{Q}$, with dihedral Galois group of order $2h$. The cyclic normal subgroup of order h corresponds to the quadratic subfield Ω. For the h conjugate subgroups of order 2, the corresponding subfields K are extensions of degree h over $\mathbb{Q}$, and one of these is characterized as the maximal real subfield of N.

Whereas it is easy in the cases $d = -23$ and $d = -31$ to give an explicit arithmetic-canonical representation of the so defined number field K of degree $h = 3$, the same problem in the case $d = -47$, where K has degree 5, has until now been solved only through equations flowing from the transformation theory of modular functions (i.e. so-called modular

equations), so that the arithmetical nature of the roots in the class field N remains in the dark. [1]

Some time ago H. Koch (Berlin) asked me whether one could not handle the case of $d = -47$ just as simply as the cases $d = -23$ and $d = -31$, and at first I thought that indeed one easily could. On closer inspection it became apparent however, that for $d = -47$ a considerably greater effort would be necessary. I communicate hereafter the result of my efforts, in whose final stage I was aided by Klaus Alber (Hamburg). [2] In this I rely on the arithmetic theory of cyclic biquadratic number fields, as I have developed it in an earlier work, [3] as well as certain results from my monograph on the class number of Abelian number fields. [4] I begin by clarifying, by means of the examples $d = -23$ and $d = -31$, what kind of arithmetic-canonical representation I have in mind.

B.1 The Cases $d = -23$ and $d = -31$

The two cases allow for a common treatment; they differ only by the sign in

$$d = -27 \pm 4 = -3^3 \pm 2^2.$$

In the following, the upper and lower signs always correspond, respectively, to the cases $d = -23$ and $d = -31$.

---

[1] See H. Weber, *Algebra III*, 2nd ed., Braunschweig 1908, §131, as well as R. Fricke, *Algebra III*, Braunschweig 1928, §4 (p. 492). There the equations

$$x^5 - x^3 - 2x^2 - 2x - 1 = 0$$

resp.

$$x^5 - x^4 + x^3 + x^2 - 2x_{+1} = 0$$

are given as resolvents of the class equation for the discriminant $d = -47$.

[2] Hasse's student, PhD Hamburg 1959, dissertation: *Einige Sätze aus der komplexen Multiplikation.*

[3] H. Hasse, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*, Abh. Deutsche Akad. Wiss. Berlin 1948, Nr. 2 (1950). Cited in the following by GK.

[4] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akad. Verlag, Berlin 1952. Cited in the following by KAZ.

B.1.1 Ascent to Generation of N^3/Ω^3

The cyclic extension of 3rd degree N/Ω can be generated by a radical, after the adjunction of a third root of unity (indicated by superscript 3):

$$N^3 = \Omega^3\left(\sqrt[3]{\omega}\right).$$

To be precise, the radicand ω is a singular 3-primary number of Ω^3, that is, a third divisor power number [5] which is 3-primary (i.e. a third power residue mod $3\sqrt{-3}$). In short, [6]

$$\omega \underset{3}{\cong} 1, \quad \omega \underset{3}{\equiv} 1 \mod 3\sqrt{-3}.$$

In the sense of $\underset{3}{=}$, it is uniquely determined, up to choice of $\omega^{\pm 1}$ (i.e. up to third number power factors [7]).

In order to investigate ω, we will first determine the fundamental unit ε and class number h of the bicyclic biquadratic number field

$$\Omega^3 = \mathbb{Q}(\sqrt{-3}, \sqrt{d}).$$

That can be done, following KAZ §26, in the following way.

The real quadratic subfield

$$\Omega_0^3 = \mathbb{Q}(\sqrt{-3d})$$

has the fundamental unit

$$\varepsilon_0 = \frac{(27 \mp 2) + 3\sqrt{-3d}}{2}$$

with the norm

$$N(\varepsilon_0) = 1$$

and the class number

$$h_0 = 1.$$

The two imaginary quadratic subfields

$$\Omega = \mathbb{Q}(\sqrt{d}), \quad \mathbb{Q}^3 = \mathbb{Q}(\sqrt{-3})$$

---

[5] That is, a number whose divisor is a third power.

[6] Hasse's notation in which a number n is set beneath an equivalence relation $=$, $\cong$, or $\equiv$ means that the relation holds up to an n^{th} power factor. That is, there exists a number or a divisor such that the relation will hold if one side is multiplied by its n^{th} power. The relation $\alpha \cong \beta$ means that α and β have the same divisor, if α, β are numbers; if β is a divisor then it means that β is the divisor of α.

[7] That is, up to a factor which is the third power of a number.

have the class numbers

$$h_1 = 3, \quad h_2 = 1.$$

Following KAZ, §26, (6) - (8), one has in general that

$$\varepsilon = \begin{cases} \varepsilon_0 & \text{if} \quad Q = 1 \\ \sqrt{-\varepsilon_0} & \text{if} \quad Q = 2 \end{cases}$$

and

$$h_1 = \frac{1}{2} Q h_0 h_1 h_2, \quad h^* = \frac{1}{2} Q h_1 h_2,$$

where Q is the unit index [8] and h^* is the relative class number of Ω^3/Ω_0^3. The unit index is by definition

$$Q = \left\{ \begin{array}{ll} 1 & \text{if} - \varepsilon_0 \underset{2}{\neq} 1 \\ 2 & \text{if} - \varepsilon_0 \underset{2}{=} 1 \end{array} \right\} \quad \text{in} \quad \Omega^3.$$

Already, since the relative class number is integral (KAZ §§19, 27), we must have $Q = 2$ in the present case, where $h^* = \frac{1}{2} Q \cdot 3$. One can see this in the following way, without having to appeal to the rather deep-lying integrality of h, and thereby at the same time determine ε.

The criterion (11_I) for $Q = 2$ from KAZ, §26, (12_I) is satisfied:

$$\mp\sqrt{-3}^2 = \pm 3 = aa'$$

with

$$a = \frac{9 + \sqrt{-3d}}{2}$$

from Ω_0^3. Since the prime 3 is ramified in Ω_0^3, one therefore has

$$a \cong a', \quad \text{so that} \quad a \cong \sqrt{-3}.$$

Therefore

$$\varepsilon = \frac{a}{\sqrt{-3}} = \frac{-3\sqrt{-3} + \sqrt{d}}{2}$$

is a unit in Ω^3, with

$$\varepsilon^2 = \frac{a^2}{-3} = \frac{(-27 + d)/2 - 3\sqrt{-3d}}{2} = \frac{-(27 \mp 2) - 3\sqrt{-3d}}{2} = -\varepsilon_0.$$

[8] The terms *unit index*, and *relative class number* are defined in Hasse's monograph (Hasse 1952).

But this says that $Q = 2$ and ε is the fundamental unit of Ω^3. Therewith we get that

$$h = h^* = 3.$$

From class field theory it follows that in Ω^3 there is essentially only one singular 3-primary number ω. The two postulates on ω are now satisfied for the fundamental unit ε, the first trivially, since actually $\varepsilon \cong 1$; the second considering that

$$\varepsilon^{-1} \underset{3}{=} \varepsilon^2 = -\varepsilon_0 \equiv \frac{d \mp 2}{2} \equiv \pm 1 \underset{3}{\equiv} 1 \mod 3\sqrt{-3}.$$

Then one can normalize by setting

$$\omega = \varepsilon$$

so that we get for N^3/Ω^3 the representation

$$N^3 = \Omega^3 \left(\sqrt[3]{\varepsilon}\right).$$

Remark: One notes that in the present cases $d = -23$ and $d = -31$, the singular 3-primary number ω is not, as one would have assumed at the outset, formed by normalization of the third divisor power number already existing in Ω,

$$w = \frac{(2 \pm 1) + \sqrt{d}}{2} \underset{3}{\cong} 1 \quad \text{with} \quad N(w) = 2^3$$

by means of a unit of Ω^3. In the following treatment, the case $d = -47$ will turn out accordingly.

B.1.2 Descent to Generation of $K/\mathbb{Q}$

For the present purpose it is crucial that the singular 3-primary number ω in Ω^3 can be normalized as a number already in the maximal real subfield Ω_0^3 of Ω^3. That is achieved either by the normalization

$$\omega^{-1} \underset{3}{=} \varepsilon^2 \underset{3}{=} \varepsilon_0 = \frac{(27 \mp 2) + 3\sqrt{-3d}}{2}$$

just now given, or better, since – as will be seen – it leads to a lower fundamental equation, [9] the normalization

$$\omega \underset{3}{=} \frac{\varepsilon}{\sqrt{-3}^3} = \frac{\alpha}{9} = \frac{1}{9} \cdot \frac{9 + \sqrt{-3d}}{2}.$$

[9] By a fundamental equation for a field, Hasse means the equation $f(x) = 0$ in which $f(x)$ is the minimal polynomial of a primitive or generating element of the field. By lower he means lower height, i.e. smaller coefficients.

Since the (real) radical $\sqrt[3]{\alpha/9}$ already lies in the maximal real subfield N_0^3 of N^3, one therefore has for N_0^3/Ω_0^3 the representation

$$N_0^3 = \Omega_0^3\left(\sqrt[3]{\frac{\alpha}{9}}\right).$$

The generating automorphism of N_0^3/K sends the radical $\sqrt[3]{\alpha/9}$ to $\sqrt[3]{\alpha'/9}$ (again meaning the real root). Therefore the trace of N_0^3/K in K is the radical sum

$$A = \sqrt[3]{\frac{\alpha}{9}} + \sqrt[3]{\frac{\alpha'}{9}}$$

and this generates K over $\mathbb{Q}$, since it is different from both its complex conjugates. For the generator A one has

$$A^3 = \left(\frac{\alpha}{9} + \frac{\alpha'}{9}\right) + 3\sqrt[3]{\frac{\alpha}{9}}\sqrt[3]{\frac{\alpha'}{9}}\left(\sqrt[3]{\frac{\alpha}{9}} + \sqrt[3]{\frac{\alpha'}{9}}\right).$$

Considering that $\alpha + \alpha' = 9$ and $\alpha\alpha' = \pm 3$, this becomes

$$A^3 = 1 \pm A.$$

Therewith the stated goal is reached:

RESULT. *The maximal real subfield K of the class field N of an imaginary quadratic number field $\Omega = \mathbb{Q}(\sqrt{d})$ with $d = -27 \pm 4$ has the representation*

$$K = \mathbb{Q}(A)$$

with the minimal equation

$$A^3 \mp A - 1 = 0.$$

The generator A is arithmetically characterized as the radical sum

$$A = \sqrt[3]{\frac{\alpha}{9}} + \sqrt[3]{\frac{\alpha'}{9}},$$

whose radicand

$$\frac{\alpha}{9} = \frac{1}{9}\cdot\frac{9 + \sqrt{-3d}}{2}$$

is related to the fundamental unit

$$\varepsilon_0 = \frac{(27 \mp 2) + 3\sqrt{-3d}}{2}$$

of the maximal real subfield $\Omega_0^3 = \mathbb{Q}(\sqrt{-3d})$ *of* $\Omega^3 = \mathbb{Q}(\sqrt{-3}, \sqrt{d})$*, and to the prime number* 3 *by*

$$\frac{\alpha}{\alpha'} = \pm\varepsilon_0, \quad \alpha\alpha' = \pm 3.$$

Remark. Using the aforementioned, more obvious normalization $\omega^{-1} \underset{3}{=} \varepsilon_0$ of the radicands we get for the generator

$$B = \sqrt[3]{\varepsilon_0} + \sqrt[3]{\varepsilon_0'}$$

the higher fundamental equation

$$B^3 - 3B - (27 \mp 2) = 0.$$

B.2 The Case $d = -47$

For the sake of uniformity with the afore-handled cases, although here d has only the one value -47, the notation $\sqrt{d}$ will be retained (and we will not write $\sqrt{-47}$).

B.2.1 Ascent to Generation of N^5/Ω^5

The cyclic extension of 5th degree N/Ω can be generated by a radical, after the adjunction of a fifth root of unity (indicated by superscript 5):

$$N^5 = \Omega^5\left(\sqrt[5]{\omega}\right),$$

where the radicand ω is a singular 5-primary number of Ω^5, that is, [10] a 5th divisor power number, which is 5-primary (i.e. a fifth power residue mod $5\sqrt{-e\sqrt{5}}$). In short,

$$\omega \underset{5}{\cong} 1, \quad \omega \underset{5}{\equiv} 1 \mod 5\sqrt{-e\sqrt{5}}.$$

Up to choice of $\omega^{\pm 1}$, $\omega^{\pm 2}$, it is uniquely determined in the sense of $\underset{5}{=}$ (i.e. up to 5th number power factors).

In order to investigate ω, we will first, by the method laid out in full in GK, determine the relative fundamental unit ε_0, unit index Q_0 and class number h_0 of the cyclic biquadratic maximal real subfield

$$\Omega_0^5 = \mathbb{Q}\left(\sqrt{-e\sqrt{5}\cdot d}\right)$$

[10] We note that in a diagram that we have not reproduced in this translation, Hasse defines $e = (1+\sqrt{5})/2$, noting that it is the fundamental unit of $\mathbb{Q}_0^5$.

of Ω^5 and thence the unit index Q, and furthermore the fundamental unit ε and class number h of the imaginary Abelian number field

$$\Omega^5 = \mathbb{Q}\left(\sqrt{-e\sqrt{5}}, \sqrt{d}\right)$$

of Type $(4, 2)$.

Relative fundamental unit ε_0, unit index Q_0 and class number h_0 of Ω_0^5

The determination is based on the representation of the integers of Ω_0^5 in the canonical form

$$\frac{1}{2}\left(\frac{x_0 + x_1\tau(\psi)}{2} + y_0\frac{\tau(\chi) + \tau(\overline{\chi})}{2} + y_1\frac{i\tau(\chi) - i\tau(\overline{\chi})}{2}\right)$$

with congruence conditions mod 4 for the rational integer coordinates x_0, x_1, y_0, y_1 (GK, §8, (2), (3) and Theorem 14). Here $\chi, \overline{\chi}$ are the two conjugate biquadratic characters mod $5 \cdot 47$, $\psi = \chi^2$ the quadratic character mod 5, and $\tau(\chi), \tau(\overline{\chi}), \tau(\psi)$ the corresponding Gauss sums. The forms appearing in this representation are given, following GK, §8, (21), by

$$\tau(\psi) = \sqrt{5}, \quad \frac{\tau(\chi) + \tau(\overline{\chi})}{2} = e'\sqrt{-e\sqrt{5} \cdot d}, \quad \frac{i\tau(\chi) - i\tau(\overline{\chi})}{2} = \sqrt{-e\sqrt{5} \cdot d}.$$

The relative units of $\Omega_0^5/\mathbb{Q}_0^5$ (units with relative norm ± 1) are characterized in this canonical representation, following GK, §12, (2), by the coordinate equations

$$\frac{(x_0^2 \mp 16)/5 + x_1^2}{2 \cdot 47} = y_0^2 + y_1^2, x_0x_1 = -(y_0^2 - y_1^2) - 4y_0y_1,$$

and the relative unit ε_0 corresponds to the essentially uniquely determined solution with minimal $y_0^2 + y_1^2$. As minimal solution one quickly finds here, using the systematic testing procedure in GK, §12, A1,

$$x_0 = 47, \quad x_1 = -5, \quad y_0 = -1, \quad y_1 = -2,$$

with positive sign in the first equation on the left, which means relative norm -1; y_0, y_1 are thereby negatively normalized, for entirely irrelevant reasons, not to be discussed here. Therefore $\Omega_0^5/\mathbb{Q}_0^5$ has the relative fundamental unit

$$\varepsilon_0 = \frac{1}{2}\left(\frac{47 - 5\sqrt{5}}{2} - e'\sqrt{-e\sqrt{5} \cdot d} - 2\sqrt{-e\sqrt{5} \cdot d}\right)$$

or

$$\varepsilon_0 = \frac{1}{2}\left(\frac{47-5\sqrt{5}}{2} - \frac{-5+\sqrt{5}}{2}\sqrt{-e\sqrt{5}\cdot d}\right)$$

with the relative norm

$$n(\varepsilon_0) = \varepsilon_0\varepsilon_0'' = -1.$$

Since $x_1 = -5$ thus proves not to be divisible by 47, we finally get, using GK, §12, A2, the unit index of $\Omega_0^5/\mathbb{Q}_0^5$ as

$$Q_0 = 1.$$

Accordingly, the unit group of Ω_0^5 will be generated by the units

$$e, \varepsilon_0, \varepsilon_0' \quad \text{with} \quad N(e) = -1, n(\varepsilon_0) = -1.$$

In order to at last determine the class number h_0 of Ω_0^5, one has to compute the reduced relative cyclotomic unit [11]

$$\eta_0 = \theta\theta'$$

(GK, §19, (11)). That can be done using the Bergström product formula for the 23-factor product

$$\theta = \prod_a \left((-\zeta)^a - (-\zeta)^{-a}\right)$$

(GK, §14), where ζ is a primitive $5\cdot 47$-th root of unity, and a runs over an odd normalized subsystem of the rational congruence group mod $5\cdot 47$ assigned to Ω_0^5 (KAZ, §10), say, the smallest positive

$$1, 19, 21, 29, 39, 51, 61, 69, 71, 81, 99, 101, 109,$$

$$111, 121, 129, 131, 139, 179, 191, 199, 219, 229.$$

For this calculation one has to turn to the Schema in GK, §19, B 3, a 2, Type 3 (p. 86). Without mechanical or electronic computational means this could not have been carried out successfully. By means of the Hamburg electronic computer TR 4 we obtained the agreement

$$\eta_0 = \frac{1}{2}\left(\frac{47-5\sqrt{5}}{2} - \frac{-5+\sqrt{5}}{2}\sqrt{-e\sqrt{5}\cdot d}\right) = \varepsilon_0$$

[11] On cyclotomic units, see e.g. (Hilbert 1897, §98).

with the afore-determined relative fundamental unit ε_0. Following GK, §19, Theorem 37 implies, in light of $Q_0 = 1$, that $\Omega_0^5/\mathbb{Q}_0^5$ has the relative class number

$$h_0^* = 1.$$

Since $\mathbb{Q}_0^5 = \mathbb{Q}(\sqrt{5})$ has the class number 1, therefore Ω_0^5 also has the class number

$$h_0 = 1.$$

Unit index Q, another fundamental unit ε, and class number h of Ω^5

By KAZ, §33, (p. 98) Ω^5/Ω_0^5 has the unit index

$$Q = 2.$$

A unit ε therefore existing in Ω^5 by KAZ, §20, Theorem 14 and ($4a_0$), with the property

$$\overline{\varepsilon} = -\varepsilon,$$

will arise by the generating automorphism of Ω^5/Ω_0^5 (complex conjugation), from the number θ underlying the reduced relative cyclotomic unit $\eta_0 = \theta\theta'$ – and generally all cyclotomic units – which indeed in the present case (a composite conductor $f = 5 \cdot 47$) is a unit in Ω^5, and as product of an odd number of pure-imaginary factors with the property

$$\overline{\theta} = -\theta$$

satisfies:

$$\varepsilon = \theta.$$

For this number θ we found during the aforementioned electronic computation of η_0 the value

$$\theta = \frac{1}{2}\left((2-\sqrt{5})\sqrt{d} + \frac{25-11\sqrt{5}}{2}\sqrt{-e\sqrt{5}}\right).$$

As one also easily computes, the relative norm of this unit of $\mathbb{Q}(\sqrt{5},\sqrt{d})$ is

$$n(\theta) = \theta\theta' = e' = -e^{-1}$$

and therefore its complete norm is

$$N(\theta) = \theta\theta'\theta''\theta''' = N(e) = -1.$$

By the salient points demonstrated thus far, the unit group of Ω^5 must be generated by a primitive $5 \cdot 47$th root of unity ζ, the real units e, ε_0, ε_0', and the imaginary unit θ. According to the norm relations just given and the earlier relation

$$\varepsilon_0 = \eta_0 = \theta\theta'$$

one can instead simply take

$$\zeta \quad \text{and the conjugates} \quad \theta, \theta', \theta''$$

as generators.

By KAZ, §33, Theorem 34, we compute finally, in light of $Q = 2$, the relative class number of Ω^5/Ω_0^5 as

$$h^* = 2 \cdot 10 \cdot N_\chi(\theta(\chi))N_\psi(\theta(\psi))N_{\hat{\psi}}(\theta(\hat{\psi})),$$

where, as earlier, χ denotes a biquadratic character mod $5 \cdot 47$, $\psi = \chi^2$ the quadratic character mod 5, and $\hat{\psi}$ the quadratic character mod 47, and $\theta(\chi)$, $\theta(\psi)$, $\theta(\hat{\psi})$ are the character sums formed according to KAZ, §27, (2), of which the norms N_χ, N_ψ, $N_{\hat{\psi}}$ are taken in the field of the respective characters. The calculation of these character sums and their norms can without great effort be carried out by hand. They give as relative class number

$$h^* = 2 \cdot 5.$$

In view of $h_0 = 1$, Ω^5 therefore also has the class number

$$h = 2 \cdot 5.$$

Therefore by class field theory there is in Ω^5 essentially only *one* singular 5-primary number ω.

Determination of the singular 5-primary number ω

The singular 5-primary number ω we seek must comprise units of Ω^5, and the essentially unique 5th divisor power number already existing in Ω,

$$w = \frac{9 + \sqrt{d}}{2} \underset{5}{\cong} 1 \quad \text{with} \quad N(w) = 2^5$$

In order to reach it by a suitable product of powers of w and the fundamental units ζ, θ, θ', θ'' of Ω^5, one determines the exponents mod 5 in the representation of these numbers by a

basis of the π-adic principal unit group [12] of Ω^5, only considered mod π^5, where for short we write

$$\pi = \sqrt{-e\sqrt{5}} \quad \text{with} \quad \pi^4 \cong 5,\ \pi^5 \cong 5\pi$$

for the prime divisor of 5 in Ω^5. This analysis can be made without great difficulty, by an incremental procedure, through rising powers $\pi, \pi^2, \pi^3, \pi^4, \pi^5$ as modulus. The result is assembled in the following table, in whose heading the chosen basis is given; blank spaces indicate exponents 0 mod 5:

	$1+\pi$	$1+\pi\sqrt{d}$	$1+\sqrt{5}$	$1+\sqrt{5}\sqrt{d}$	$1+\pi\sqrt{5}$	$1+\pi\sqrt{5}\sqrt{d}$	$1+5$	$1+5\sqrt{d}$	
w								3	
ζ	3		3		4		4		
θ			2			2	1		2
θ'			3			1	4		3
θ''			2			3	1		1

Between the five exponent lines there is clearly, as there must be, a linear dependence mod 5, namely with the coefficients given in the column on the far right. Therefore the unit

$$\omega = \theta^2\theta'^3\theta'' \underset{5}{\equiv} 1 \mod 5\pi,$$

is 5-primary. By carrying out the formation of conjugates and the multiplication, which is easiest in the association

$$\omega = (\theta\theta')^2(\theta'\theta'') = \eta_0^2\eta_0' = \varepsilon_0^2\varepsilon_0',$$

one obtains for ω the value

$$\omega = \frac{1}{2}\left(\frac{9353+4225\sqrt{5}}{2} - \frac{715+325\sqrt{5}}{2}\sqrt{-e\sqrt{5}\cdot d}\right).$$

For use later let us also note the value

$$\varepsilon_0\varepsilon_0' = \frac{1}{2}\left(\frac{521+235\sqrt{5}}{2} - (20+9\sqrt{5})\sqrt{-e\sqrt{5}\cdot d}\right).$$

With the radicands ω so determined, one then has for N^5/Ω^5 the representation

$$N^5 = \Omega^5\left(\sqrt[5]{\omega}\right) = \Omega^5\left(\sqrt[5]{\varepsilon_0^2\varepsilon_0'}\right).$$

Remark. One notes that also in the present case $d = -47$ by construction the 5th divisor power number w in Ω does not divide the singular 5-power number, entirely analogously to the afore-handled cases $d = -23$ and $d = -31$.

[12] See (Hensel 1908, Ch. 4 § 7).

B.2.2 Descent to Generation of $K/\mathbb{Q}$

The afore-determined singular 5-primary number $\omega = \varepsilon_0^2\varepsilon_o'$ of Ω^5 is here already so normalized that it lies in the maximal real subfield Ω_0^5 of Ω^5. Since the (real) radical $\sqrt[5]{\omega} = \sqrt[5]{\varepsilon_0^2\varepsilon_0'}$ lies in the maximal real subfield N_0^5 of N^5, one thus has for N_0^5/Ω_0^5 the representation

$$N_0^5 = \Omega_0^5(\sqrt[5]{\omega}) = \Omega_0^5(\sqrt[5]{\varepsilon_0^2\varepsilon_0'}).$$

Descent from N_0^5/Ω_0^5 to $K_0^5/\mathbb{Q}_0^5$.

The generating automorphism of N_0^5/K_0^5 sends the radical $\sqrt[5]{\omega}$ to $\sqrt[5]{\omega''}$ (again, the real radical understood). In view of

$$\omega\omega'' = n(\varepsilon_0)^3 = -1$$

one also has

$$\sqrt[5]{\omega}\sqrt[5]{\omega''} = -1.$$

We have then the radical sum

$$B = \sqrt[5]{\omega} + \sqrt[5]{\omega''} = \sqrt[5]{\omega} - \frac{1}{\sqrt[5]{\omega}}$$

as the trace for N_0^5/K_0^5 in the subfield K_0^5, and this generates this subfield over $\mathbb{Q}_0^5$, since it is different from its four complex conjugates:

$$K_0^5 = \mathbb{Q}_0^5(B).$$

In order to find the equation that the B in this representation satisfies, one goes to the identities

$$\left(x - \frac{1}{x}\right)^5 = \left(x^5 - \frac{1}{x^5}\right) - \left(x^3 - \frac{1}{x^3}\right) + 10\left(x - \frac{1}{x}\right),$$
$$\left(x - \frac{1}{x}\right)^3 = \left(x^3 - \frac{1}{x^3}\right) - 3\left(x - \frac{1}{x}\right),$$

thus

$$\left(x - \frac{1}{x}\right)^5 + 5\left(x - \frac{1}{x}\right)^3 + 5\left(x - \frac{1}{x}\right) = x^5 - \frac{1}{x^5},$$

and puts $x = \sqrt[5]{\omega}$ therein. This gives:

$$B^5 + 5B^3 + 5B = \omega - \frac{1}{\omega} = \omega + \omega'' = \frac{9353 + 4225\sqrt{5}}{2}.$$

The norm of the absolute term of this equation is the prime number 443629.

Descent from $K_0^5/\mathbb{Q}_0^5$ to $K/\mathbb{Q}$.

The generating automorphism of K_0^5/K sends the radical $\sqrt[5]{\omega}$ to $\sqrt[5]{\omega''}$ (again, the real radical understood). In view of

$$\omega' = \varepsilon_0'^2\varepsilon_0'' = \frac{\varepsilon_0^5\varepsilon_0'^2\varepsilon_0''}{\varepsilon_0^5} = -\frac{\varepsilon_0^4\varepsilon_0'^2}{\varepsilon_0^5} = -\frac{\omega^2}{\varepsilon_0^5}$$

one also has

$$\sqrt[5]{\omega'} = -\frac{\sqrt[5]{\omega}^2}{\varepsilon_0}.$$

We have then the radical sum

$$A = B + B' = \sqrt[5]{\omega} + \sqrt[5]{\omega'} + \sqrt[5]{\omega''} + \sqrt[5]{\omega'''} = \left(\sqrt[5]{\omega} - \frac{1}{\sqrt[5]{\omega}}\right) - \left(\frac{\sqrt[5]{\omega}^2}{\varepsilon_0} - \frac{\varepsilon_0}{\sqrt[5]{\omega}^2}\right)$$

as the trace for K_0^5/K in the subfield K, and this generates this subfield over $\mathbb{Q}$, since it is different from its four complex conjugates:

$$K = \mathbb{Q}(A).$$

In order to finally find the equation which the A in this representation satisfies, one may regard the last given representation of A as a representation by the basis $\sqrt[5]{\omega}^{-2}$, $\sqrt[5]{\omega}^{-1}$, 1, $\sqrt[5]{\omega}$, $\sqrt[5]{\omega}^2$ of N_0^5/Ω^5, and compute from that the corresponding basis representations of A^2, A^3, A^4, and A^5. For carrying out this computation, which was indeed somewhat troublesome, yet to be dealt with entirely by hand, I thank Klaus Alber (Hamburg). The equation obtained was

$$A^5 + 10A^3 - 5T(\varepsilon_0)A^2 + 5\left(1 + T\left(\frac{\omega}{\varepsilon_0}\right)\right)A - T(\omega) = 0.$$

One computes the traces appearing therein from the afore-given numerical values of ε_0, $\omega/\varepsilon_0 = \varepsilon_0\varepsilon_0'$, $\omega = \varepsilon_0^2\varepsilon_0'$ to be

$$T(\varepsilon_0) = 47, \quad T\left(\frac{\omega}{\varepsilon_0}\right) = 521, \quad T(\omega) = 9353.$$

Therewith is the stated goal reached:

RESULT. *The maximal real subfield K of the class field N of the imaginary quadratic number field $\Omega = \mathbb{Q}(\sqrt{-47})$ has the representation*

$$K = \mathbb{Q}(A)$$

with the fundamental equation

$$A^5 + 10A^3 - 235A^2 + 2610A - 9353 = 0.$$

The generator A is arithmetically characterized as the radical sum

$$A = \sqrt[5]{\omega} + \sqrt[5]{\omega'} + \sqrt[5]{\omega''} + \sqrt[5]{\omega'''},$$

whose radicand is formed by

$$\omega = \varepsilon_0^2 \varepsilon_0'$$

out of the relative fundamental unit ε_0 of the cyclic biquadratic maximal real subfield $\Omega_0^5 = \mathbb{Q}\left(\sqrt{-e\sqrt{5}\cdot d}\right)$ of $\Omega^5 = \mathbb{Q}\left(\sqrt{-e\sqrt{5}}, \sqrt{d}\right)$, where $e = (1+\sqrt{5})/2$ is the fundamental unit of $\mathbb{Q}_0^5 = \mathbb{Q}(\sqrt{5})$.

Closing remark. Whether in the present case $d = -47$ the disproportionately high fundamental equation can be reduced to a lower one by dividing out of the radicand $\omega = \varepsilon_0^2 \varepsilon_0'$ an appropriate 5th power, as was possible in the cases $d = -23$ and $d = -31$ by dividing the radicand ε by $\sqrt{-3}^3$, and whether one can perhaps reduce the equation found here to those coming out of the transformation theory of modular functions (see footnote 1), remains to be seen in a further investigation.

Appendix C

The Legendre-Germain computation

Below we reproduce the MAPLE code we used to compute all the data discussed by Hasse and Taussky on the Legendre-Germain criterion, as we saw in Chapter 5. Comments in the code indicate how it works.

```
# Build list P of primes less than 25,000, and list R containing
# one primitive residue for each prime in list P.

with(numtheory):
n := 1:
p := 2:
while(p < 25000) do
  R[n] := primroot(p):
  P[n] := p:
  n := n+1:
  p := nextprime(p):
od:


N := nops(P);
```

```
# Both lists P and R run from index 1 to N.

# We will consider l equal to each odd prime less than 100,
# which are primes P[2] through P[25].
# For each l, we will consider only those p that are greater than l,
# since for p less than l we must have (p-1,l) = 1, in which case
# every residue mod p is an lth power.
# Meanwhile, when p > l, then l odd says p >= l + 2, so p - 1 > l,
# and then (p-1,l) > 1 is equivalent to l dividing p - 1, since
# l is prime.

checklAsnthPrime := proc(n)
 T := 0:
 for k from n+1 to N do
  p := P[k]:
  r := R[k]:
  m := p-1:
  # If l mod p-1 does not divide p-1, then /every/ residue
  # mod p is an lth power, so we need not check.
  if irem(m,l) <> 0 then next fi:
  # Compute list of all lth powers mod p, together with
  # their index w.r.t. r.
  q := m/l:
  L := [seq([Power(r,a*l) mod p, a*l], a=0..q-1)]:
  L := sort(L):
  # Search for l, and for a pair of consecutive residues.
  lind := -1:
  cons := -1: consInd := -1: last := -1:
  for i from 1 to nops(L) do
   x := L[i]:
   # Look for l.
   if x[1] = l then
    lind := x[2]:
```

```
      if cons > 0 then break: fi:
    fi:
    # Look for consecutive residues.
    if cons = -1 and x[1] = last + 1 then
      cons := last:
      consInd := L[i-1][2]:
      if lind >= 0 then break: fi:
    fi:
    last := x[1]:
  od:
  if lind >= 0 then
    printf("%2d %5d %5d %5d %4d ***\n",l,p,l,lind,k);
  fi:
  if cons >= 0 then
    printf("%2d %5d %5d %5d %4d\n",l,p,cons,consInd,k);
  fi:
  if lind = -1 and cons = -1 then
    printf("%2d %5d           %4d\n",l,p,k);
  fi:
  T := T+1:
 od:
 printf("Considered %d primes p.\n",T);
end proc:

bst := time():
for n from 2 to 25 do
 printf("################################################\n");
 l := P[n]:
 printf("# l = %d\n",l);
 st := time():
 checklAsnthPrime(n);
 dt := time()-st:
 printf("Elapsed time: %.2f.\n",dt);
```

```
od:
bdt := time()-bst:
printf("Total time: %.2f.\n",bdt);
```

Bibliography

Artin, Emil (1923). "Über eine neue Art von L-Reihen". In: *Hamb. Abh.* Pp. 89–108 (cit. on p. 89).

Artin, Emil (1927). "Beweis des allgemeinen Reziprozitätsgesetzes". In: *Hamb. Abh.* 5, pp. 353–363 (cit. on p. 89).

Artin, Emil and Helmut Hasse (1925). "Über den zweiten Egänzungssatz zum Reziprozitätsgesetz der ℓ-ten Potenzreste im Körper k_ζ der ℓ-ten Einheitswurzeln und in Oberkörpern von k_ζ". In: *J. f. reine angew. Math.* Pp. 143–148 (cit. on pp. 89, 91).

— (1928). "Die beiden Egänzungssätze zum Reziprozitätsgesetz der ℓ^n-ten Potenzreste im Körper der ℓ^n-ten Einheitswurzeln". In: *Hamb. Abh.* 6, pp. 146–162 (cit. on p. 92).

Aspray, William (1990). *John von Neumann and the Origins of Modern Computing*. The MIT Press (cit. on p. 169).

Atkin, A. O. L. and B. J. Birch, eds. (1971). *Computers in Number Theory*. Proceedings of the Science Research Council Atlas Symposium No. 2 held at Oxford, from 18 - 23 August, 1969. Academic Press (cit. on p. 235).

Avigad, Jeremy (2006). "Methodology and metaphysics in the development of Dedekind's theory of ideals". In: *The Architecture of Modern Mathematics*. Ed. by José Ferreirós and Jeremy Gray. Oxford University Press, pp. 159–186 (cit. on pp. 8, 30).

Bachmann, Paul (1905). *Zahlentheorie*. Vol. V. B.G. Teubner (cit. on p. 3).

Bauer, Friedrich L. (1998). "Olga Taussky-Todd 30.8.1906 - 7.10.1995". In: *Linear Algebra and its Applications* 280, pp. 9–12 (cit. on pp. 97, 154).

Bergström, Harald (1944). "Die Klassenzahlformel für reelle quadratische Zahlkörper mit zusammengesetzter Diskriminante als Produkt verallgemeinerter Gaußscher Summen". In: *J. Reine Angew. Math.* 186, pp. 91–115 (cit. on p. 138).

Berlekamp, Elwyn R. (1967a). "Factoring Polynomials Over Finite Fields". In: *The Bell System Technical Journal* 46, pp. 1853–1859 (cit. on p. 200).

Berlekamp, Elwyn R. (Apr. 7, 1967b). *On the Factorization of Polynomials over Finite Fields*. Technical report. Bell Telephone Laboratories Inc. Murray Hill, New Jersey (cit. on p. 200).

— (Aug. 9, 1968a). *How to Find the Factorization of Polynomials over Very Large Finite Fields*. Technical report. Bell Telephone Laboratories Inc. Murray Hill, New Jersey (cit. on p. 200).

— (June 25, 1968b). *On the Factorization of Polynomials over Very Large Finite Fields*. Technical report. Bell Telephone Laboratories Inc. Murray Hill, New Jersey (cit. on p. 200).

— (1970). "Factoring Polynomials Over Large Finite Fields". In: *Mathematics of Computation* 24.111 (cit. on p. 200).

Berwick, William Edward Hodgson (1927). *Integral Bases*. Cambridge Tracts in Mathematics and Mathematical Physics 22. Cambridge University Press (cit. on pp. 195–197).

Brillhart, John (1992). "Derrick Henry Lehmer". In: *Acta Arithmetica* LXII.3, pp. 207–220 (cit. on p. 113).

Cantor, David G. and Hans Zassenhaus (1981). "A New Algorithm for Factoring Polynomials Over Finie Fields". In: *Mathematics of Computation* 36.154 (cit. on p. 199).

Cantor, Georg (1874). "Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen". In: *J. Reine Angew. Math.* 77, pp. 258–262 (cit. on p. 39).

Cassels, J.W.S. and A. Fröhlich, eds. (1967). Washington: Thompson (cit. on pp. 89, 94–95).

Cohen, Henri (1993). *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics 138. Springer (cit. on pp. 17, 168, 239, 241).

— (2000). *Advanced Topics in Computational Number Theory*. Graduate Texts in Mathematics 193. Springer (cit. on p. 168).

Cohn, Harvey (1962). "Some Illustrative Computations in Algebraic Number Theory". In: *Survey of Numerical Analysis*. Ed. by John Todd. McGraw-Hill, pp. 543–549 (cit. on p. 148).

— (1978). *A Classical Invitation to Algebraic Numbers and Class Fields*. Springer (cit. on pp. 98, 240–241).

Collatz, L., G. Meinardus, and H. Unger, eds. (1967). *Funktionalanalysis Approximationstheorie Numerische Mathematik*. Vol. 7. International Series of Numerical Mathematics. Birkhäuser (cit. on p. 190).

Corry, Leo (1996). *Modern Algebra and the Rise of Mathematical Structures*. Vol. 17. Science Networks Historical Studies. Birkhäuser (cit. on pp. 5, 30, 33, 103, 204–205, 231).

Corry, Leo (2007). "From *Algebra* (1895) to *Moderne Algebra* (1930): Changing Conceptions of a Discipline – A Guided Tour Using the *Jahrbuch über die Fortschritte der Mathematik*". In: *Episodes in the History of Modern Algebra (1800 - 1950)*. Ed. by Jeremy J. Gray and Karen Hunger Parshall. Vol. 32. History of Mathematics. American Mathematical Society. Chap. 10, pp. 221–243 (cit. on p. 204).

— (2008a). "FLT Meets SWAC: Vandiver, the Lehmers, Computers and Number Theory". In: *IEEE Annals for History of Computing* 30.1, pp. 38–49 (cit. on pp. 167, 242).

— (2008b). "Number Crunching vs. Number Theory: Computers and FLT, from Kummer to SWAC (1850-1960), and beyond". In: *Archive for History of Exact Science* 62.1, pp. 393–455 (cit. on pp. 167, 242).

Curtiss, John H., ed. (1956). *Numerical Analysis*. Vol. VI. Proceedings of Symposia in Applied Mathematics. Held at the Santa Monica City College, August 26-28, 1953. Cosponsored by the National Bureau of Standards. (cit. on p. 140).

Dade, E.C., O. Taussky, and H. Zassenhaus (1962). "On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field". In: *Mathematische Annalen* 148, pp. 31–64 (cit. on p. 184).

Dade, E.C. and H. Zassenhaus (1963). "How Programming Difficulties Can Lead to Theoretical Advances". In: *Experimental Arithmetic, High Speed Computing and Mathematics*. Ed. by N.C. Metropolis et al. Vol. XV. Proceedings of Symposia in Applied Mathematics, pp. 87–94 (cit. on pp. 184–185).

Davis, Chandler (1997). "Remembering Olga Taussky Todd". In: *The Mathematical Intelligencer* 19.1, pp. 15–17 (cit. on pp. 97–98, 102, 139, 174).

Dedekind, Richard (1878). "Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen". In: *Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen* 23. Repr. in (Dedekind 1930-1932c), vol. 1, pp. 202-232, pp. 1–23 (cit. on p. 127).

— (1930-1932c). *Gesammelte mathematische Werke*. Ed. by R. Fricke, E. Noether, and O. Ore. 3 vols. Braunschweig: Vieweg (cit. on p. 294).

— (1930-1932b). *Gesammelte mathematische Werke*. Ed. by R. Fricke, E. Noether, and O. Ore. Vol. I. Braunschweig: Vieweg (cit. on p. 247).

— (1930-1932a). *Gesammelte mathematische Werke*. Ed. by R. Fricke, E. Noether, and O. Ore. Vol. III. Braunschweig: Vieweg (cit. on pp. 1, 28–30).

Dedekind, Richard (1996). *Theory of Algebraic Integers*. Trans. by John Stillwell. Orig. pub. 1877. Cambridge University Press (cit. on p. 11).

Dedekind, Richard and Peter Gustav Lejeune Dirichlet (1871). *Vorlesungen über Zahlentheorie*. 2nd ed. Vieweg (cit. on pp. 30, 249).

— (1894). *Vorlesungen über Zahlentheorie*. 4th ed. Corrected reprint of the edition published in Braunschweig by F. Vieweg und Sohn in 1894. Chelsea Pub. Co. 1968. (cit. on pp. 8, 30, 249, 253–254).

Dickson, L. E. (1910). "Hensel's Theory of Algebraic Numbers". In: *Bull. Amer. Math. Soc.* 17, pp. 23–36 (cit. on pp. 119, 247).

— (1919). *History of the theory of numbers*. 3 vols. Carnegie institution of Washington (cit. on p. 127).

— (1925). "Review: Robert Fricke, Lehrbuch der Algebra, verfasst mit Benutzung von Heinrich Webers gleichnamigem Buche". In: *Bulletin of the American Mathematical Society* 31.7, pp. 372–373 (cit. on p. 204).

— (1928). "Review: Robert Fricke, Lehrbuch der Algebra". In: *Bulletin of the American Mathematical Society* 34.4, p. 531 (cit. on p. 205).

Dold, A. and B. Eckmann, eds. (1973). *Proceedings of the Conference on Orders, Group Rings and Related Topics*. Vol. 353. Lecture Notes in Mathematics. Springer (cit. on p. 194).

Edwards, Harold, Olaf Neumann, and Walter Purkert (1982). "Dedekinds "Bunte Bemerkungen" zu Kroneckers "Grundzüge"". In: *Archive for History of Exact Sciences* 27, pp. 49–85 (cit. on pp. 6, 23, 50, 245).

Edwards, Harold M. (1977). *Fermat's Last Theorem: A Genetic Introcution to Algebraic Number Theory*. Springer-Verlag (cit. on pp. 4, 74, 247, 271).

— (1980). "The Genesis of Ideal Theory". In: *Archive for History of Exact Sciences* 23, pp. 321–378 (cit. on pp. 3, 30, 249, 254).

— (1990). *Divisor Theory*. Birkhäuser (cit. on pp. 4, 6, 24, 118–119).

— (2008a). "Hasse, Helmut". In: *Complete Dictionary of Scientific Biography*. Ed. by Charles Gillispie. Charles Scribner's Sons, pp. 385–387 (cit. on pp. 17, 95).

— (2008b). "Takagi, Teiji". In: *Complete Dictionary of Scientific Biography*. Ed. by Charles Gillispie. Charles Scribner's Sons, pp. 890–892 (cit. on p. 85).

Eisenstein, Gotthold (1850). "Über ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze". In: *J. f. rein. angew. Math.* 39, pp. 351–364 (cit. on p. 92).

Euler, L. (1915). *Opera Omnia*. Vol. II. I. Leipzig/Berlin (cit. on p. 137).

Ewald, William (2005). *From Kant to Hilbert. A Source Book in the Foundations of Mathematics*. Vol. II. Oxford University Press (cit. on pp. 6, 117).

Frei, Günther (1989). "Heinrich Weber and the Emergence of Class Field Theory". In: *The History of Modern Mathematics. Ideas and Their Reception*. Ed. by David E. Rowe and John McCleary. Vol. 1. Academic Press, pp. 425–450 (cit. on p. 78).

— (2007). "The Unpublished Section Eight: On the Way to Function Fields over a Finite Field". In: *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*. Ed. by Catherine Goldstein, Norbert Schappacher, and Joachim Schwermer. Springer. Chap. II.4, pp. 159–198 (cit. on pp. 42–43, 199).

Freudenthal, Hans (2008). "Hilbert, David". In: *Complete Dictionary of Scientific Biography*. Ed. by Charles Gillispie. Charles Scribner's Sons, pp. 388–395 (cit. on pp. 68–69).

Furtwängler, Philipp (1903a). "Die Konstruktion des Klassenkörpers für solche algebraischen Zahlkörper, die eine ℓ-te Einheitswurzel enthalten, und deren Idealklassen eine zyklische Gruppe vom Grad ℓ^h bilden". In: *Göttinger Nachrichten*, pp. 203–217 (cit. on p. 65).

— (1903b). "Über die Konstruktion des Klassenkörpers für beliebige algebraische Zahlkörper, die eine ℓ-te Einheitswurzel enthalten". In: *Göttinger Nachrichten*, pp. 282–303 (cit. on p. 65).

— (1904). "Die Konstruktion des Klassenkörpers für beliebige algebraische Zahlkörper". In: *Göttinger Nachrichten*, pp. 173–195 (cit. on p. 65).

— (1906). "Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers". In: *Mathematische Annalen* 63, pp. 1–37 (cit. on pp. 65, 74, 81).

— (1930). "Beweis des Haptidealsatzes für die Klassenkörper algebraischer Zahlkörper". In: *Abh. Hamburg* 7, pp. 14–36 (cit. on pp. 77, 99).

Gallian, Joseph A. (1998). *Contemporary Abstract Algebra*. Fourth. Houghton Mifflin (cit. on p. 253).

Gauss, C. F. (1801). *Disquisitiones Arithmeticae*. Leipzig (cit. on p. 69).

Geddes, Keith O., Stephen R. Czapor, and George Labahn (1992). *Algorithms for Computer Algebra*. Kluwer Academic Publishers (cit. on p. 230).

Grier, David Alan (2001). "The Rise and Fall of the Committee on Mathematical Tables and Other Aids to Computation". In: *IEEE Annals* 23.2, pp. 38–49 (cit. on p. 110).

Hasse, Helmut (1923). "Über die Darstellbarkeit von Zahlen durch Quadratische Formen im Körper der rationalen Zahlen". In: *J. Reine Angew. Math.* 152, pp. 129–148 (cit. on pp. 17, 88).

— (1924). "Das allgemeine Reziprozitätsgesetz und seine Ergänzungssätze in beliebigen algebraischen Zahlkörpern für gewisse, nichtprimäre Zahlen". In: *J. Reine Angew. Math.* 153, pp. 192–207 (cit. on p. 91).

— (1925a). "Das allgemeine Reziprozitätsgesetz der ℓ-ten Potenzreste für beliebige, zu ℓ prime Zahlen in gewissen Oberkörpern des Körpers der ℓ-ten Einheitswurzeln". In: *J. Reine Angew. Math.* 154, pp. 199–214 (cit. on p. 91).

— (1925b). "Der zweite Ergänzungssatz zum Reziprozitätsgesetz der ℓ-ten Potenzreste für beliebige, zu ℓ prime Zahlen in gewissen Oberkörpern des Körpers der ℓ-ten Einheitswurzeln". In: *J. Reine Angew. Math.* 154, pp. 215–218 (cit. on p. 91).

— (1925c). "Über das allgemeine Reziprozitätsgesetz der ℓ-ten Potenzreste im Körper k_ζ der ℓ-ten Einheitswurzeln und in Oberkörpern von k_ζ". In: *J. Reine Angew. Math.* 154, pp. 96–109 (cit. on p. 91).

— (1926). "Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil I, Klassenkörpertheorie". In: *Jahresbericht D. M.-V.* 35 (cit. on p. 124).

— (1927). "Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil Ia, Beweise zu Teil I". In: *Jahresbericht D. M.-V.* 36 (cit. on p. 124).

— (1929). "Zum expliziten Reziprozitätsgesetz". In: *Abh. Math. Sem. Univ. Hamburg* 7, pp. 52–63 (cit. on p. 86).

— (1930). "Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil II, Reziprozitätsgesetez". In: *Jahresbericht D. M.-V.* Supplementary vol. 6 (cit. on pp. 93, 124).

— (1940). "Produktformel für verallgemeinerte Gaußsche Summen und ihre Anwendung auf die Klassenzahlformel für reelle quadratische Zahlkörper". In: *Mathematische Zeitschrift* 46, pp. 303–314 (cit. on p. 138).

— (1948). "Existenz und Mannigfaltigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers I-III". In: *Mathematische Nachrichten* 1, pp. 40–61, 213–217, 277–283 (cit. on p. 144).

Hasse, Helmut (1949). *Zahlentheorie*. Akademie-Verlag (cit. on pp. 119, 121).

— (1950a). "Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern". In: *Abhandlungen der Deutschen Akademie der Wissenschaften Berlin, Math.-Nat. Kl.* 2, pp. 3–95 (cit. on pp. 138, 141, 148, 172, 207, 209, 222, 237).

— (1950b). "Kurt Hensel zum Gedächtnis". In: *J. f. reine angew. Math.* 187, pp. 1–13 (cit. on p. 73).

— (1952). *Über die Klassenzahl abelscher Zahlkörper*. Akademie-Verlag (cit. on pp. 5, 8–9, 13, 123–126, 128–129, 131, 134, 136, 138, 172, 276).

— (1961). "Zum expliziten Reziprozitätsgesetz". In: *Arch. Math.* 13, pp. 479–485 (cit. on pp. 87, 92).

— (1964). "Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante -47". In: *Acta Arithmetica* IX, pp. 420–433 (cit. on pp. 148, 205–206, 210–211).

— (1965). *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*. Reprint of Jahres. d. Deutsch. Math.-Verein. Supplement 6, 1930. Physica-Verlag (cit. on p. 77).

— (1967). "History of Class Field Theory". In: *Algebraic Number Theory*. Ed. by J.W.S. Cassels and A. Fröhlich. Washington: Thompson. Chap. XI (cit. on pp. 79, 136).

— eds. (1975). *Mathematische Abhandlungen*. Vol. 1. de Gruyter (cit. on pp. 74, 88, 120).

— (1980). *Number Theory*. Springer (cit. on pp. 120–121).

— (1981). "Zu Hilberts algebraisch-zahlentheoretischen Arbeiten". In: *Hilberts Gesammelte Abhandlungen. Zahlentheorie*. Ed. by Wilhelm Magnus, Olga Taussky, and Helmut Ulm. 4th ed. Vol. 1. Orig. pub. 1932. New York: Chelsea (cit. on pp. 68–69, 71).

Hasse, Helmut and Joseph Liang (1969). "Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante -47". In: *Acta Arithmetica* XVI, pp. 89–97 (cit. on pp. 202, 205, 211–213, 215–217, 222).

Hawkins, Thomas (2008). "Berwick, William Edward Hodgson". In: *Complete Dictionary of Scientific Biography*. Ed. by Charles Gillispie. Charles Scribner's Sons, p. 90 (cit. on p. 195).

Hecke, Erich (1923). *Vorlesungen über die Theorie der algebraischen Zahlen*. Leipzig: Akademische Verlagsgesellschaft (cit. on pp. 3, 173).

Hecke, Erich (1981). *Lectures on the Theory of Algebraic Numbers*. English. Trans. from the German by George U. Brauer, Jay R. Goldman, and R. Kotzen. Graduate Texts in Mathematics 77. Springer (cit. on pp. 3, 173).

Heilbronn, H. (1934). "On the class-number in imaginary quadratic fields". In: *The Quarterly Journal of Mathematics, Oxford Series* 5, pp. 150–160 (cit. on p. 109).

Heilbronn, H. and E. H. Linfoot (1934). "On the imaginary quadratic corpora of class-number one". In: *The Quarterly Journal of Mathematics, Oxford Series* 5, pp. 293–301 (cit. on p. 109).

Hensel, Kurt (1884). "Arithmetische Untersuchungen über Discriminanten und ihre ausserwesentlichen Theiler". PhD thesis. Friedrich-Wilhelms-Universität zu Berlin (cit. on pp. 27, 246).

— (1894). "Untersuchung der Fundamentalgleichung einer Gattung für eine relle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante". In: *J. Reine Angew. Math.* 113, pp. 61–83 (cit. on p. 2).

— (1897a). "Über die Bestimmung der Discriminante eines algebraischen Körpers". In: *Göttinger Nachrichten*, pp. 247–253 (cit. on p. 73).

— (1897b). "Über die Fundamentalgleichung und die außerwesentlichen Discriminantenteiler eines algebraischen Körpers". In: *Göttinger Nachrichten*, pp. 254–260 (cit. on p. 73).

— (1897c). "Über eine neue Begründung der Theorie der algebraischen Zahlen". In: *Jahresbericht der Deutschen Mathematiker-Vereinigung*, pp. 83–88 (cit. on pp. 2, 71–72).

— (1904a). "Neue Grundlagen der Arithmetik". In: *J. Reine Angew. Math.* 127, pp. 51–84 (cit. on pp. 2, 8, 42).

— (1904b). "Über eine neue Begründung der Theorie der algebraischen Zahlen". In: *J. Reine Angew. Math.* 128, pp. 1–32 (cit. on p. 42).

— (1905). "Über die arithmetischen Eigenschaften der algebraischen und transzendenten Zahlen". In: *Jahresber. Deutsche Math.-Ver.* 14, pp. 545–558 (cit. on p. 65).

— (1908). *Theorie der algebraischen Zahlen*. B.G. Teubner (cit. on pp. 5, 8, 11–12, 21–22, 39, 50–51, 56, 119, 246, 284).

— (1913). *Zahlentheorie*. G. J. Göschen (cit. on pp. 64, 119, 231).

— (1918). “Eine neue Theorie der algebraischen Zahlen”. In: *Mathgematische Zeitschrift* 2, pp. 433–452 (cit. on pp. 228, 231).

Hensel, Kurt and Adolf Fraenkel (1927). “Das Mathematische Institut der Universität 1866-1927”. In: *Die Philipps-Universität zu Marburg 1527-1927*. Marburg, pp. 753–756 (cit. on p. 17).

Hensel, Kurt and Georg Landsberg (1902). *Theorie der algebraischen Funktionen einer Variabeln und ihre Anwendung auf algebraische Kurven und Abelsche Integrale*. Teubner (cit. on p. 73).

Hilbert, David (1894). “Über den Dirichletschen biquadratischen Zahlkörper”. In: *Mathem. Annalen* 45, pp. 309–340 (cit. on p. 137).

— (1896). “Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper”. In: *Nachrichten der Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse*, pp. 29–39 (cit. on pp. 78, 137).

— (1897). “Die Theorie der algebraischen Zahlkörper”. In: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 4, pp. 175–535 (cit. on pp. 5, 124, 246–247, 262, 264, 281).

— (1898). “Über die Theorie der relativ-Abelschen Zahlkörper”. In: *Nachrichten der Gesellschaft der Wissenschaften zu Göttingen*, pp. 370–399 (cit. on pp. 65, 71, 75, 81).

— (1899). “Über die Theorie des relativquadratischen Zahlkörpers”. In: *Mathematische Annalen*, pp. 1–127 (cit. on pp. 75, 83–84).

— (1981a). “Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper”. In: *Gesammelte Abhandlungen. Zahlentheorie*. Ed. by Wilhelm Magnus, Olga Taussky, and Helmut Ulm. 4th ed. Vol. 1. Orig. pub. 1932. New York: Chelsea. Chap. 6 (cit. on pp. 78, 137).

— (1981b). “Über die Theorie der relativequadratischen Zahlkörper”. In: *Gesammelte Abhandlungen. Zahlentheorie*. Ed. by Wilhelm Magnus, Olga Taussky, and Helmut Ulm. 4th ed. Vol. 1. Orig. pub. 1932. New York: Chelsea. Chap. 8 (cit. on p. 80).

— (1998). *The theory of algebraic number fields. With an introd. by Franz Lemmermeyer and Norbert Schappacher*. English. Trans. from the German by Iain T. Adamson. Springer (cit. on pp. 5, 179).

Hlawka, Edmund (1997). “Renewal of the Doctorate of Olga Taussky Todd”. In: *The Mathematical Intelligencer* 19.1, pp. 18–20 (cit. on pp. 97–98, 100, 102).

Huber, A. (1940). “Philipp Furtwängler”. In: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 50, pp. 167–178 (cit. on p. 76).

Ince, E.L. (1934). "Cycles of Reduced Ideals in Quadratic Fields". In: *British Association Mathematical Tables IV*. London (cit. on p. 176).

Jackson, Allyn (2004). "Comme Appelé du Néant – As If Summoned from the Void: The Life of Alexandre Grothendieck". In: *Notices of the AMS* 51.10, pp. 1196–1212 (cit. on p. 182).

Jacobi, Carl Gustav Jacob (1839a). *Canon Arithmeticus*. Berolini (cit. on p. 148).

— (1839b). "Ueber die complexen Primzahlen, welche in der Theorie der Reste der 5^{th}, 8^{th} and 12^{th} Potenzen zu betrachten sind". In: *J. f. Rein. Angew. Math.* Pp. 314–318 (cit. on p. 74).

Kisilevsky, H. (1997). "Olga Taussky-Todd's Work in Class Field Theory". In: *Pacific J. Math.* 181.3, pp. 219–224 (cit. on pp. 97–100).

Kleiner, Israel (2012). *Excursions in the History of Mathematics*. Birkhäuser (cit. on p. 154).

Knuth, Donald Ervin (1981). *The Art of Computer Programming. Seminumerical Algorithms*. Second ed. Vol. 2. Addison-Wesley (cit. on p. 199).

Kronecker, Leopold (1882). "Grundzüge einer arithmetischen Theorie der algebraischen Grössen". In: *J. Reine Angew. Math.* 92. (Kronecker 1968, 237-387)., pp. 1–122 (cit. on pp. 5–6, 23, 27, 245).

— (1968). *Leopold Kronecker's Werke*. Kurt Hensel, ed. Chelsea Pub. Co. (cit. on p. 301).

Kühne, Hermann (1903). "Angenäherte Auflösung von Congruenzen nach Primmodulsystemen in Zusammenhang mit den Einheiten gewisser Körper". In: *J. Reine Angew. Math.* 3126, pp. 102–115 (cit. on p. 43).

Kummer, Ernst Eduard (1847a). "Extrait d'une Lettre de M. Kummer à M. Liouville". In: *Journal de mathématiques pures et appliquées* 12, p. 136 (cit. on p. 4).

— (1847b). "Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren". In: *J. Reine Angew. Math.* 35, pp. 327–367 (cit. on pp. 4, 8–10, 244–245, 271).

— (1847c). "Zur Theorie der complexen Zahlen". In: *J. Reine Angew. Math.* 35, pp. 319–326 (cit. on p. 4).

— (1859). "Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist". In: *Math. Abh. König. Akad. Wiss. Berlin*, pp. 19–158 (cit. on p. 246).

— (1975). *Collected Papers*. Vol. 1, Contributions to Number Theory. André Weil, ed. Springer-Verlag (cit. on pp. 4, 246).

Lagrange, J. L. (1796). "Sur la solution des problèmes indéterminée du second degré". In: *Mem. Acad. R. Sci. Berlin* 23 (cit. on p. 69).

Lang, Serge (1970). *Algebraic Number Theory*. Springer (cit. on pp. 77, 94–95).

— (1995). "Mordell's Reivew, Siegel's Letter to Mordell, Diophantine Geometry, and 20th Century Mathematics". In: *Notices Amer. Math. Soc.* 42.3, pp. 339–350 (cit. on p. 242).

Legendre, A.-M. (1798). *Essai sur la théorie des nombres*. Paris (cit. on p. 69).

Lehmer, D. H. (1933a). "A Photo-Electric Number Sieve". In: *The American Mathematical Monthly* 40.7, pp. 401–406 (cit. on pp. 106, 108).

— (1933b). "On imaginary quadratic fields whose class number is unity". In: *Bulletin of the American Mathematical Society* 39, p. 360 (cit. on p. 109).

— ed. (1941). *Bulletin of the National Research Council, Washington, D.C.* (105): *Guide to Tables in the Theory of Numbers* (cit. on pp. 107, 110–111, 113, 133, 148, 169).

— (1969). "Computer Technology Applied to the Theory of Numbers". In: *Studies in Number Theory*. Ed. by W. J. LeVeque. Vol. 6. Studies in Mathematics. Mathematical Association of America, pp. 117–151 (cit. on p. 239).

— (1971). "The Economics of Number Theoretic Computation". In: *Computers in Number Theory*. Ed. by A. O. L. Atkin and B. J. Birch. Academic Press (cit. on p. 239).

Lehmer, Emma (1956). "Number Theory on the SWAC". In: *Numerical Analysis*. Ed. by John H. Curtiss. Vol. VI. Proceedings of Symposia in Applied Mathematics. Held at the Santa Monica City College, August 26-28, 1953. Cosponsored by the National Bureau of Standards., pp. 103–108 (cit. on p. 141).

Lejeune Dirichlet, Peter Gustav (1840). "Sur la théorie des nombres". In: *C.R. Acad. Sci. Paris* 10. (Lejeune Dirichlet 1969, 619-623)., pp. 285–288 (cit. on p. 1).

— (1841). "Einige Resultate von Untersuchungen über eine Klasse homogener Funktionen des dritten und der höheren Grade." In: *Ber. K. Preuss. Akad. Wiss.* (ibid., 625-632)., pp. 280–285 (cit. on p. 1).

— (1842). "Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen". In: *Ber. K. Preuss. Akad. Wiss.* (ibid., 633-638)., pp. 93–95 (cit. on p. 1).

— (1969). *G. Lejeune-Dirichlet's Werke*. Vol. 1. Leopold Kronecker, ed. Chelsea Pub. Co. (cit. on p. 302).

Lemmermeyer, Franz (2000). *Reciprocity Laws: From Euler to Eisenstein*. Springer (cit. on pp. 74, 83, 86, 173).

Leopoldt, Heinrich Wolfgang (1973). "Zum wissenschaftlichen Werk von Helmut Hasse". In: *Journal für die Reine und Angewandte Mathematik* 262/263, pp. 1–17 (cit. on pp. 120, 214).

Liang, Joseph Jen (1969). "On Interrelations of Arithmetical Invariants in Algebraic Number Fields". PhD thesis. The Ohio State University (cit. on p. 197).

Luchins, Edith H. and Mary Ann McLoughlin (1996). "In Memoriam: Olga Taussky-Todd". In: *Notices of the American Mathematical Society* 43.8, pp. 838–847 (cit. on pp. 97–99, 102, 140, 154, 174, 177).

Mancosu, Paolo, ed. (2008). *The Philosophy of Mathematical Practice*. Oxford University Press (cit. on pp. 30, 137).

Marcus, Daniel A. (1977). *Number Fields*. Springer (cit. on p. 223).

Mehrtens, Herbert (1987). "Ludwig Bieberbach and "Deutsche Mathematik"". In: *Studies in the history of mathematics*. Vol. 26. Mathematical Association of America Studies in Mathematics. Mathematical Association of America, pp. 195–241 (cit. on p. 96).

Metropolis, N., J. Howlett, and Gian-Carlo Rota, eds. (1980). *A History of Computing in the Twentieth Century*. Academic Press (cit. on p. 106).

Metropolis, N.C. et al., eds. (1963). *Experimental Arithmetic, High Speed Computing and Mathematics*. Vol. XV. Proceedings of Symposia in Applied Mathematics. American Mathematical Society (cit. on p. 185).

Mignotte, M. (1982). "Some Useful Bounds". In: *Compter Algebra – Symbolic and Algebraic Computation*. Ed. by B. Buchberger, G.E. Collins, and R. Loos. Springer, pp. 259–263 (cit. on p. 230).

Mordell, L. J. (1964). "Book review: *Diophantine Geometry*". In: *Bull. Amer. Math. Soc.* 70, pp. 491–498 (cit. on p. 242).

Neumann, J. von and H. H. Goldstine (1953). "A Numerical Study of a Conjecture of Kummer". In: *Mathematical Tables and Other Aids to Computation* 7.42, pp. 133–134 (cit. on p. 169).

Neumann, Olaf (2007). "Divisibility Theories in the Early History of Commutative Algebra and the Foundations of Algebraic Geometry". In: *Episodes in the History of Modern Algebra (1800-1950)*. Ed. by Jeremy J. Gray and Karen Hunger Parshall. Vol. 32. History of Mathematics. American Mathematical Society. Chap. 4, pp. 73–105 (cit. on pp. 79, 246–247).

O'Connor, J. J. and E. F. Robertson (2004). *Derrick Norman Lehmer*. URL: `http://www-history.mcs.st-and.ac.uk/Biographies/Lehmer_Derrick_N.html` (cit. on p. 108).

Petri, Birgit (2011). "Perioden, Elementarteiler, Transzendenz – Kurt Hensels Weg zu den p-adischen Zahlen". PhD thesis. Technischen Universität Darmstadt (cit. on pp. 2, 17).

Piazza, Paola (2007). "Zolotarev's Theory of Algebraic Numbers". In: *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*. Ed. by Catherine Goldstein, Norbert Schappacher, and Joachim Schwermer. Springer. Chap. VII.2, pp. 453–462 (cit. on pp. 3, 127, 246).

Pohst, M. and H. Zassenhaus (1989). *Algorithmic algebraic number theory*. Cambridge University Press (cit. on pp. 17, 103, 168, 182).

Pohst, Michael (1994). "In Memoriam Hans Zassenhaus (1912 - 1991)". In: *Journal of Number Theory* 47, pp. 1–19 (cit. on pp. 20, 103–104, 168, 174, 178–180, 182–183, 200, 202, 243).

Purkert, W. (1971). "Zur Genesis des abstrakten Körperbegriffs". In: *Schriftenreihe für Geschichte der Naturwiss. Technik und Medizin* 10.2, pp. 8–20 (cit. on p. 33).

Reid, Constance (1970). *Hilbert*. Springer (cit. on pp. 69, 111, 116).

— (1976). *Courant in Göttingen and New York*. Springer (cit. on p. 95).

Reuschle, K. G. (1875). *Tafeln complexer Primzahlen welche aus Wurzeln der Einheit gebildet sind*. Berlin (cit. on pp. 133–134, 148).

Rohrbach, Hans (1973). "The Logogryph of Euler". In: *J. Reine Angew. Math.* 262/263, pp. 392–399 (cit. on p. 96).

— (1998). "Helmut Hasse and Crelle's Journal". In: *J. Reine Angew. Math.* 500, pp. 5–13 (cit. on pp. 96, 146).

Rüdenberg, L. and H. Zassenhaus, eds. (1973). *Briefe an David Hilbert*. Springer (cit. on p. 69).

Schneider, Hans (1998). "Some personal reminischences of Olga Taussky-Todd". In: *Linear Algebra and its Applications* 280, pp. 15–19 (cit. on pp. 97, 102, 146).

Schoeneberg, Bruno (2008). "Artin, Emil". In: *Complete Dictionary of Scientific Biography*. Ed. by Charles Gillispie. Charles Scribner's Sons, pp. 306–308 (cit. on p. 89).

Schönemann, Theodor (1846). "Von denjenigen Moduln, welche Potenzen von Primzahlen sind". In: *J. Reine Angew. Math.* 32, pp. 93–105 (cit. on p. 43).

Schwermer, Joachim (2007). "Minkowski, Hensel, and Hasse: On The Beginnings of the Local-Global Principle". In: *Episodes in the History of Modern Algebra (1800-1950)*.

Ed. by Jeremy J. Gray and Karen Hunger Parshall. Vol. 32. History of Mathematics. American Mathematical Society. Chap. 7, pp. 153–177 (cit. on p. 87).

Shallit, Jeffrey, Hugh C. Williams, and François Morain (1995). "Discovery of a lost factoring machine". In: *The Mathematical Intelligencer* 17.3, pp. 41–47 (cit. on p. 106).

Sommer, J. (1907). *Vorlesungen über Zahlentheorie. Einführung in die Theorie der algebraischen Zahlkörper*. Leipzig: B.G. Teubner (cit. on pp. 133–134).

Steinitz, Ernst (1910). "Algebraische Theorie der Körper". In: *Journal für die Reine und Angewandte Mathematik* 137, pp. 167–309 (cit. on pp. 30, 231).

Takagi, Teiji (1920). "Über eine Theorie des relativ Abelschen Zahlkörpers". In: *Journal of the College of Science, Imperial University of Tokyo* 41, pp. 1–133 (cit. on p. 77).

Taussky, Olga (1932). "Über eine Verschärfung des Hauptidealsatzes für algebraische Zahlkörper". In: *J. reine angew. Math.* 168, pp. 193–210 (cit. on p. 99).

— (1952). "Arnold Scholz zum Gedächtnis". In: *Mathematische Nachrichten* 7, pp. 379–386 (cit. on pp. 100–101).

— (1953). "Some Computational Problems in Algebraic Number Theory". In: *Numerical Analysis*. Ed. by John H. Curtiss. Vol. VI. Proceedings of Symposia in Applied Mathematics. Pub. 1956, pp. 187–193 (cit. on pp. 107, 113, 140–141, 167, 169–170, 172–173, 239).

— (1969). "A remark concerning Hilbert's Theorem 94". In: *J. Reine Angew. Math.* 239/240, pp. 435–438 (cit. on p. 176).

— (1977). "Olga Taussky-Todd". In: *Number Theory and Algebra. Collected Papers Dedicated to Henry B. Mann, Arnold E. Ross, and Olga Taussky-Todd*. Ed. by Hans Zassenhaus. Academic Press, pp. xxxv–xlvi (cit. on pp. 97–98, 100).

— (1985). "An autobiographical essay". In: *Mathematical People: Profiles and Interviews*. Ed. by Donald J. Albers and G. L. Alexanderson. Birkhäuser, pp. 309–336 (cit. on pp. 97–98).

Todd, John, ed. (1962). *Survey of Numerical Analysis*. McGraw-Hill (cit. on pp. 168, 237, 240).

Ullrich, Peter (1998). "The genesis of Hensel's p-adic numbers". In: *Charlemagne and his Heritage: 1200 Years of Civilization and Science in Europe*. Turnhout: Brepols Publishers (cit. on pp. 17, 65, 73–74).

unknown (July 12, 1931). "Machine Solves Intricate Tasks of Mathematics". In: *Herald Tribune, New York* (cit. on p. 108).

von zur Gathen, Joachim (2006). "Who was Who in polynomial factorization". In: *Proceedings of ISSAC 2006*. ACM Press, p. 2 (cit. on p. 199).

Vostokov, S. V. (1978). "On an Explicit Form of the Reciprocity Law". In: *Dokl. Akad. Nauk SSSR* 238.6, pp. 198–201 (cit. on p. 87).

Weber, Heinrich (1886). "Theorie der Abel'schen Zahlkörper I". In: 8, pp. 193–263 (cit. on p. 78).

— (1891). *Elliptische Funktionen und algebraische Zahlen*. Braunschweig: F. Vieweg (cit. on pp. 78, 204).

— (1895). *Lehrbuch der Algebra*. Vol. I. Braunschweig: F. Vieweg (cit. on p. 204).

— (1896). *Lehrbuch der Algebra*. Vol. II. Braunschweig: F. Vieweg (cit. on p. 204).

— (1897). "Über Zahlengruppen in algebraischen Zahlkörpern, I, II, III". In: *Mathematische Annalen* 48,49,50, pp. 433–473,83–100,1–26 (cit. on p. 78).

— (1908). *Lehrbuch der Algebra*. Vol. III. Braunschweig: F. Vieweg (cit. on p. 204).

Weyl, Hermann (1940). *Algebraic Theory of Numbers*. Princeton University Press (cit. on pp. 5, 14, 117–119, 149, 187, 201, 246–247, 266).

Williams, Michael R. (1985). *A History of Computing Technology*. Prentice-Hall (cit. on pp. 106, 141–143, 233).

Wussing, Hans (1984). *The Genesis of the Abstract Group Concept*. English. Trans. from the German by Abe Shenitzer. Orig. pub. 1969. The MIT Press (cit. on p. 137).

Zassenhaus, H. and J. Liang (1969). "On a Problem of Hasse". In: *Mathematics of Computation* 23.107, pp. 515–519 (cit. on pp. 202, 212, 215–217, 224, 227).

Zassenhaus, Hans (1949a). *The Theory of Groups*. Chelsea (cit. on p. 103).

— (1949b). "Über die Existenz von Primzahlen in arithmetischen Progressionen". In: *Comment. Math. Helv.* 22, pp. 232–259 (cit. on p. 104).

— (1954). "Über eine Verallgemeinerung des Henselschen Lemmas". In: *Archiv der Mathematik* 5, pp. 317–325 (cit. on p. 228).

— (1964). "Emil Artin, his life and work". In: *Notre Dame J. Formal Logic* 5, pp. 1–9 (cit. on p. 103).

— (1965). "On the Hensel lemma for Lie algebras". In: *Mathematische Zeitschrift* 86, pp. 396–409 (cit. on p. 228).

— (1966). "Experimentelle Mathematik in Forschung und Unterricht". In: *Math. Phys. Semesterber. n.F.* 13, pp. 135–152 (cit. on p. 192).

— (1967). "Zahlentheoretische Experimente im Unterricht". In: *Funktionalanalysis Approximationstheorie Numerische Mathematik*. Ed. by L. Collatz, G. Meinardus, and H. Unger. Vol. 7. International Series of Numerical Mathematics. Birkhäuser, pp. 104–108 (cit. on pp. 181, 192).

Zassenhaus, Hans (1969). "On Hensel Factorization, I". In: *Journal of Number Theory* 1.3, pp. 291–311 (cit. on pp. 199, 202, 215, 228–229, 231).

— (1972). "On the Second Round of the Maximal Order Program". In: *Applications of Number Theory to Numerical Analysis*. Ed. by S.K. Zaremba. Academic Press, pp. 389–431 (cit. on pp. 195, 197, 200–201).

— ed. (1977). *Number Theory and Algebra. Collected Papers Dedicated to Henry B. Mann, Arnold E. Ross, and Olga Taussky-Todd*. Academic Press (cit. on pp. 177, 180, 243).

Zimmer, Horst G. (1972). *Computational Problems, Methods, and Results in Algebraic Number Theory*. Lecture Notes in Mathematics 262. Springer (cit. on pp. 99, 168–169, 189, 235–236, 238).

Zolotarev, Egor Ivanovič (1880). "Sur la théorie des nombres complexes". In: *Journal de mathématiques*. 3rd 6, pp. 51–94, 129–166 (cit. on p. 3).

Zuse, Konrad (1980). "Some Remarks on the History of Computing in Germany". In: *A History of Computing in the Twentieth Century*. Ed. by N. Metropolis, J. Howlett, and Gian-Carlo Rota. Academic Press (cit. on pp. 106, 142–143).