*Springer Monographs in Mathematics*

Springer-Verlag Berlin Heidelberg GmbH

Franz Lemmermeyer

# Reciprocity Laws

## From Euler to Eisenstein

Springer

*Franz Lemmermeyer*
http://www.rzuser.uni-heidelberg.de/~hb3/
e-mail: hb3@ix.urz.uni-heidelberg.de

Library of Congress Cataloging-in-Publication Data
Lemmermeyer, Franz, 1962 -
Reciprocity laws : from Euler to Eisenstein / Franz Lemmermeyer.
p. cm. -- (Springer monographs in mathematics)
Includes bibliographical references and index.
ISBN 978-3-642-08628-1 ISBN 978-3-662-12893-0 (eBook)
DOI 10.1007/978-3-662-12893-0
1. Reciprocity theorems I. Title II. Series

QA241 .L56 2000 00-026905
512'74--dc21

Mathematics Subject Classification (1991): 11A15

Cover design: *Erich Kirchner, Heidelberg*
Typesetting by the author using a Springer TEX macro package
Printed on acid-free paper SPIN 10734033 41/3143AT-5 4 3 2 1 0

# Preface

The history of reciprocity laws is a history of algebraic number theory. This is a book on reciprocity laws, and our introductory remark is placed at the beginning as a warning: in fact a reader who is acquainted with little more than a course in elementary number theory may be surprised to learn that quadratic reciprocity does – in a sense that we will explain – belong to the realm of algebraic number theory. Hecke ([348, p. 59]) has formulated this as follows:

> Von der Entdeckung des Reziprozitätsgesetzes kann man die moderne Zahlentheorie datieren. Seiner Form nach gehört es noch der Theorie der rationalen Zahlen an, es läßt sich aussprechen als eine Beziehung lediglich zwischen rationalen Zahlen; jedoch weist es seinem Inhalt nach über den Bereich der rationalen Zahlen hinaus. [...] 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.[1]

Naturally, along with these higher methods came generalizations of the reciprocity law itself. It is no exaggeration to say that this generalization changed our way of looking at the reciprocity law dramatically; Emma Lehmer ([509, p. 467]) writes

> It is well known that the famous Legendre law of quadratic reciprocity, of which over 150 proofs[2] are in print, has been generalized

[1] Modern number theory dates from the discovery of the reciprocity law. By its form it still belongs to the theory of rational numbers, as it can be formulated entirely as a simple relation between rational numbers; however its contents points beyond the domain of rational numbers. [...] 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.

[2] She is apparently referring to Gerstenhaber's article [305]; in his email [306], he writes "The origin of the title was not a list but a statement of André Weil in a

> over the years to algebraic fields by a number of famous mathematicians from Gauss to Artin to the extent that it has become virtually unrecognizable.

These quotations show that a thorough command of the techniques of algebraic number theory is indispensable for understanding reciprocity laws; given the wealth of well written introductions to algebraic number theory, it seemed reasonable to assume that the readers are familiar with the basic arithmetic of number fields, in particular that of quadratic and cyclotomic fields. Galois theory is also a conditio sine qua non, and occasionally $\mathfrak{p}$-adic numbers or, e.g. for Chapter 8, elliptic functions are needed.

So what is a reciprocity law, anyway? Euler's way of looking at it was the following: the quadratic character of $a \bmod p$ only depends on the residue class of $p \bmod 4a$. For Legendre (who coined the term reciprocity), the reciprocity law was a statement to the effect that an odd prime $p$ is a quadratic residue modulo another odd prime $q$ if and only if $q$ is a quadratic residue modulo $p$, except when $p \equiv q \equiv 3 \bmod 4$; more exactly, Legendre defined, for odd primes $q$, a symbol $(p/q)$ with values in $\{-1, +1\}$ by demanding $(p/q) \equiv p^{(q-1)/2} \bmod q$ and announced the

**Quadratic Reciprocity Law.** *Let $p, q \in \mathbb{N}$ be different odd primes; then*

$$\Big(\frac{p}{q}\Big) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\Big(\frac{q}{p}\Big).$$

*Moreover, we have*

$$\Big(\frac{-1}{p}\Big) = (-1)^{\frac{p-1}{2}} \quad \text{and} \quad \Big(\frac{2}{p}\Big) = (-1)^{\frac{p^2-1}{8}};$$

*these are called the first and the second supplementary law, respectively.*

This is where our story begins; as we have noted above, the most transparent proofs of the quadratic reciprocity law are embedded into the theory of algebraic number fields, and already Gauss noticed that in order to formulate the fundamental theorem of biquadratic residues, one needs an "infinite enlargement" of the integers, namely the ring $\mathbb{Z}[i]$ of Gaussian integers. In fact, the biquadratic residue symbol $[\pi/\lambda]$, where $\pi, \lambda \in \mathbb{Z}[i]$ are primes not dividing 2, is the unique element in $\{\pm 1, \pm i\}$ such that the congruence $[\pi/\lambda] \equiv \pi^{(N\lambda-1)/4} \bmod \lambda$ holds. The reciprocity law discovered by Gauss then reads

Seminar at the Institute for Advanced Study in Princeton: he said that he knew 50 proofs of the law, and that for each he had seen there were two he had not. So that made 150 proofs. Then he called my attention to Kubota's, which would have been the 151st. So mine had to be the 152nd!"

At about the same time, Hasse [342, p. 100] wrote that there were more than 50 proofs, with some of them differing only marginally from each other. The tables in Appendix B suggest that Weil's estimate was pretty good.

**Quartic Reciprocity Law.** *Let $\pi, \lambda \in \mathbb{Z}[i]$ be different primary primes, i.e. assume that $\pi \equiv \lambda \equiv 1 \bmod (2+2i)$; then*

$$\left[\frac{\pi}{\lambda}\right] = (-1)^{\frac{N\pi-1}{4}\cdot\frac{N\lambda-1}{4}}\left[\frac{\lambda}{\pi}\right].$$

There are also analogues of the first and second supplementary laws; see Chapter 6 for details. A similar (though simpler) formula holds for the cubic residue symbol and 'primary' primes in $\mathbb{Z}[\rho]$, where $\rho$ is a primitive cube root of unity.

The first complete proofs for the cubic and quartic laws were published 1844 by Eisenstein, who also gave the corresponding supplementary laws; Jacobi, however, had given proofs as early as 1837 in his Königsberg lectures [402]. Jacobi was working on a generalization of the cubic and quartic reciprocity law using cyclotomy, but it turned out that the failure of unique factorization was a major stumbling block. Only after Kummer had introduced his ideal numbers (with the intention of applying the theory to find a general reciprocity law) did it become possible to do arithmetic in cyclotomic fields $\mathbb{Q}(\zeta_p)$. Eisenstein, who had before favored the language of forms, quickly acknowledged the superiority of Kummer's approach and succeeded in finding a special case of the general reciprocity law called

**Eisenstein's Reciprocity Law.** Let $\ell$ be an odd prime and suppose that $\alpha \in \mathbb{Z}[\zeta_\ell]$ is primary, i.e. congruent to a rational integer modulo $(1-\zeta_\ell)^2$. Then

$$\left(\frac{\alpha}{a}\right)_\ell = \left(\frac{a}{\alpha}\right)_\ell$$

for all integers $a \in \mathbb{Z}$ prime to $\ell$.

Here the $\ell^{th}$ power residue symbol $(\alpha/\mathfrak{p})_\ell$ is the unique $\ell^{th}$ root of unity such that $(\alpha/\mathfrak{p})_\ell \equiv \alpha^{(N\mathfrak{p}-1)/\ell} \bmod \mathfrak{p}$.

The quintic case had to wait for Kummer, who created the theory of *ideal numbers* along the way and finally produced a reciprocity theorem valid in all regular cyclotomic fields.

In order to define a residue symbols for ideals coprime to $\ell$ in the case of regular primes $\ell$ we observe that $\mathfrak{a}^h = \alpha\mathcal{O}_K$ is principal. Kummer showed that we can choose $\alpha$ primary, that is, in such a way that the congruences

$$\alpha\overline{\alpha} \equiv a \bmod \ell, \qquad \alpha \equiv b \bmod (1-\zeta_\ell)^2$$

hold for some integers $a$ and $b$. Moreover he proved that the residue symbol $\left(\frac{\alpha}{\mathfrak{b}}\right)_\ell$ does not depend on the choice of $\alpha$, as long as $\alpha$ is primary. Provided that $(\ell, h) = 1$, we can now define the residue symbol $\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)_\ell$ by

$$\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)_\ell^h = \left(\frac{\alpha}{\mathfrak{b}}\right)_\ell.$$

**Kummer's Reciprocity Law.** *Let $K = \mathbb{Q}(\zeta_\ell)$ and suppose that $\ell$ is regular, i.e., that $\ell$ does not divide the class number $h$ of $K$. Then*

$$\left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)_\ell = \left(\frac{\mathfrak{b}}{\mathfrak{a}}\right)_\ell,$$

*where $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime integral ideals prime to $\ell$.*

Kummer also gave explicit formulas for the supplementary laws that look rather complicated at first sight.

Hilbert did the next step forward by returning to the quadratic case: he discovered that there is a quadratic reciprocity law in every number field with odd class number, and he outlined how to include fields with even class number as well. Moreover, Hilbert showed that the quadratic reciprocity laws in algebraic number fields could be given a very simple form by using the norm residue symbol, and conjectured the following generalization:

**Hilbert's Reciprocity Law.** *Let $k$ be an algebraic number field containing the $m$-th roots of unity; then for all $\mu, \nu \in k^\times$, we have*

$$\prod_{\mathfrak{p}} \left(\frac{\mu,\nu}{\mathfrak{p}}\right) = 1.$$

*Here $\left(\frac{\cdot\,,\,\cdot}{\mathfrak{p}}\right)$ is Hilbert's $m$-th power norm residue symbol mod $\mathfrak{p}$, and the product is extended over all prime places $\mathfrak{p}$ of $k$.*

In this formulation of a reciprocity law, the power residue symbol does not even occur: in order to derive the classical formulation from Hilbert's one essentially has to compute certain Hilbert symbols which is rather straightforward though extremely technical. Actually, even the definition of the norm residue symbol is far from being obvious when $m > 2$.

Hilbert's conjectured reciprocity law was a part of the program he devised when he formulated the ninth problem in his famous address at the Congress of Mathematicians in Paris (1900):[3]

> **Beweis des allgemeinsten Reziprozitätsgesetzes.** *Für einen beliebigen Zahlkörper soll das Reziprozitätsgesetz der $\ell$-ten Potenzreste bewiesen werden*, wenn $\ell$ eine ungerade Primzahl bedeutet, und ferner, wenn $\ell$ eine Potenz von 2 oder eine Potenz einer ungeraden Primzahl ist. Die Aufstellung des Gesetzes, sowie die wesentlichen

[3] See e.g. Faddeev [227], Kantor [416] or Tate [792].

> Hilfsmittel zum Beweis desselben werden sich, wie ich glaube, ergeben, wenn man die von mir entwickelte Theorie des Körpers der $\ell$-ten Einheitswurzeln und meine Theorie des relativ-quadratischen Körpers in gehöriger Weise verallgemeinert.[4]

The first sentence of this problem asks for a generalization of Kummer's reciprocity law to fields $\mathbb{Q}(\zeta_\ell)$ for *irregular* primes $\ell$. This was accomplished by Furtwängler, who succeeded in showing the existence of the Hilbert class field and used it to prove a quite general reciprocity law. Takagi created a sensation when he found that Furtwängler's results were just a special case of what we call class field theory today. As an application of his theory, Takagi derived a reciprocity law for $\ell$-th powers in $\mathbb{Q}(\zeta_\ell)$ that contained Kummer's results for regular primes $\ell$ as a special case.

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. One of the less complicated formulas they found is the following:

**The Weak Reciprocity Law of Hasse.** *Let $\ell$ be an odd prime, $K = \mathbb{Q}(\zeta_\ell)$, and suppose that $\alpha, \beta \in \mathcal{O}_K$ satisfy $(\alpha, \beta) = 1$, $\alpha \equiv 1 \bmod \ell$, and $\beta \equiv 1 \bmod \lambda$. Let* Tr *denote the trace for $K/\mathbb{Q}$. Then*

$$\left(\frac{\alpha}{\beta}\right)_\ell \left(\frac{\beta}{\alpha}\right)_\ell^{-1} = \zeta^{\operatorname{Tr}\left(\frac{\alpha-1}{\ell}\cdot\frac{\beta-1}{\lambda}\right)}.$$

Hasse considered this as an approximation to the full reciprocity law since the assumption that $\alpha \equiv 1 \bmod \ell$ is quite strong (in particular, it doesn't contain Kummer's law). Artin and Hasse succeeded in giving more exact formulations, but the price they had to pay was the introduction of $\ell$-adic logarithms into their formulas.

The next break-through was Artin's discovery that all the reciprocity laws of Gauss, Kummer, Hilbert, and Takagi could be subsumed into a *general reciprocity law.* The connection between these laws is, as is demonstrated by E. Lehmer's quote cited above, not of the kind that springs to one's eye at first glance. Using the idèle class group $C_k$ of a number field $k$, Artin's reciprocity law takes the following simple form:

**Artin's Reciprocity Law.** *Let $k$ be an algebraic number field and let $K/k$ be a finite extension. Then the global norm residue symbol $\left(\frac{K/k}{\cdot}\right)$ induces an*

[4] **Proof of the most general reciprocity law.** *For an arbitrary number field, to prove the most general reciprocity law for $\ell$-th power residues*, when $\ell$ denotes an odd prime, and moreover, when $\ell$ is a power of 2 or a power of an odd prime. The formulation of the law, as well as the essential means for proving it will, I believe, result through a proper generalization of the theory of the field of $\ell$-th roots of unity that I have developed, and of my theory of relative quadratic fields.

*isomorphism*

$$C_k/N_{K/k}C_K \simeq \mathrm{Gal}\,(K/k)^{\mathrm{ab}},$$

*where* $G^{\mathrm{ab}} = G/G'$ *is* $G$ *made abelian.*

In its ideal theoretic formulation, Artin's reciprocity law basically states that the power residue symbol $(\frac{\alpha}{\mathfrak{p}})_m$ only depends on the residue class of $\alpha$ modulo some multiple of $\mathfrak{p}$; in the case $m = 2$, this is basically Euler's formulation of the quadratic reciprocity law, while for prime values of $m$ already Eisenstein had shown how to derive the reciprocity law from such a statement.

Immediately after Artin had proved his own four-year old conjecture in 1927 (using methods of Chebotarev), Hasse devoted the second part of his Zahlbericht to the derivation of the known explicit reciprocity laws from Artin's. Moreover, Artin's reciprocity law allowed Hasse to define a norm residue symbol $(\frac{\mu, K/k}{\mathfrak{p}})$ for any number field $k$ and an abelian extension $K/k$, not only for those $k$ containing the appropriate roots of unity; moreover he noticed that a product formula similar to Hilbert's holds. Finally, in the special case $\zeta_m \in k$ and $K = k(\sqrt[m]{\nu})$, Hasse found $(\frac{\mu, K/k}{\mathfrak{p}}) = (\frac{\mu,\nu}{\mathfrak{p}})$.

Hasse's investigation of the norm residue symbol (which is of a central importance in the second part of his Bericht) eventually suggested the existence of a "local class field theory", that is a theory of abelian extensions of local fields. This allowed him to find the local counterpart of Artin's reciprocity law and prove it by deducing it from the global result:

**Artin's Reciprocity Law for Local Fields.** *Let $k$ be a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers and let $K/k$ be a finite extension. Then the local norm residue symbol induces an isomorphism*

$$k^\times/N_{K/k}K^\times \simeq \mathrm{Gal}\,(K/k)^{\mathrm{ab}}.$$

Hasse immediately suggested that to look for direct proofs for the local case and build global class field theory on the simpler local one. This program was carried out essentially by him, F.K. Schmidt and Chevalley.

The classical formulation of class field theory in terms of ideal groups was abandoned by Chevalley who introduced idèles in order to describe the class field theory of infinite extensions. It soon became clear that idèles could also be used to reverse the classical approach and to deduce the global class field theory from the (easier) local one. Another revolution was the cohomological formulation of class field theory; using Tate's cohomology groups, the reciprocity law takes the following form:

**Tate's Formulation of Artin's Reciprocity Law.** *Let $K/k$ be a normal extension, and let $\mathrm{u}_{K/k} \in \mathrm{H}^2(\mathrm{Gal}\,(K/k), C_K)$ be the fundamental class of*

*$K/k$. Then the cup product with $\mathrm{u}_{K/k}$ induces, for every $q \in \mathbb{Z}$, an isomorphism*

$$\mathrm{u}_{K/k} \smile: \mathrm{H}^q(\mathrm{Gal}\,(K/k), \mathbb{Z}) \longrightarrow \mathrm{H}^{q+2}(\mathrm{Gal}\,(K/k), C_K).$$

The background necessary for understanding Tate's formulation will be given in Part II; here we only note that the special case $q = -2$ is nothing but Artin's reciprocity law, since $\mathrm{H}^{-2}(\mathrm{Gal}\,(K/k), \mathbb{Z}) \simeq \mathrm{Gal}\,(K/k)^{\mathrm{ab}}$ and $\mathrm{H}^0(\mathrm{Gal}\,(K/k), C_K) = C_k/N_{K/k}C_K$.

If, at this point, you have the feeling that we've come a long way, you might be surprised to hear that Weil [828] claimed that there was hardly any progress at all from Gauss to Artin:

> on peut dire que *tout* ce qui a été fait en arithmétique depuis Gauss jusqu'à ces dernières années consiste en variations sur la loi de réciprocité: on est parti de celle de Gauss; on aboutit, couronnement de tous les travaux de Kummer, Dedekind, Hilbert, à celle d'Artin, et *c'est la même.*[5]

Although Artin's reciprocity law (the decomposition law for abelian extensions) is not very far away from the quadratic reciprocity law (viewed as the decomposition law for quadratic extensions of $\mathbb{Q}$), unless when measured in terms of the technical difficulties involved in their proofs, I feel that Weil is being too modest here.

In a way, Artin's reciprocity law closed the subject (except for the subsequent work on explicit formulas, not to mention the dramatic progress into non-abelian class field theory that is connected in particular with the names of Shimura and Langlands or the recent generalization of class field theory to "higher dimensional" local fields), and the decline of interest in the classical reciprocity laws was a natural consequence. Nevertheless, two of the papers that helped shape the research in number theory during the second half of this century directly referred to Gauss's work on biquadratic residues: first, there's Weil's paper from 1949 ([We3] in Chapter 10) on equations over finite fields in which he announced the Weil Conjectures and which was inspired directly by reading Gauss:

> In 1947, in Chicago, I felt bored and depressed, and, not knowing what to do, I started reading Gauss's two memoirs on biquadratic residues, which I had never read before. The Gaussian integers occur in the second paper. The first one deals essentially with the number of solutions $ax^4 - by^4 = 1$ in the prime field modulo $p$, and with the connection between these and certain Gaussian sums; actually the method is exactly the same that is applied in the last section

[5] it can be said that *everything* which has been done in arithmetic from Gauss to these last years consists of variations on the law of reciprocity: one started with Gauss's law and arrived, thereby crowning all the works of Kummer, Dedekind and Hilbert, at Artin's reciprocity law, and *it is the same.*

> of the Disquisitiones to the Gaussian sums of order 3 and the equations $ax^3 - by^3 = 1$. Then I noticed that similar principles can be applied to all equations of the form $ax^m + by^n + cz^r + \ldots = 0$, and that this implies the truth of the "Riemann hypothesis" [...] for all curves $ax^n + by^n + cz^n = 0$ over finite fields, and also a "generalized Riemann hypothesis" for varieties in projective space with a "diagonal" equation $\sum a_i x_i^n = 0$. This led me in turn to conjectures about varieties over finite fields, ...

namely the Weil Conjectures, now Deligne's theorem (see Chapter 10).

The other central theme in number theory during the last few decades came into being in two papers by Birch & Swinnerton-Dyer: while studying the elliptic curves $y^2 = x^3 - Dx$ they were led to an amazing conjecture that linked local and global data of elliptic curves via their Hasse-Weil $L$-function; in these papers, the quartic reciprocity plays a central role in checking some instances of their conjectures – for the relation between $y^2 = x^3 - Dx$ and quartic residues, see Chapter 10 again. As a matter of fact, even the explicit formulas of Artin-Hasse were resurrected (and generalized) by Iwasawa, Coates and Wiles in order to make progress on the Birch–Swinnerton-Dyer conjecture.

After reciprocity had disappeared from textbooks[6] in number theory around 1950 (excepting, of course, the ubiquitous quadratic reciprocity law), the renaissance of reciprocity laws began with their inclusion in the influential book [386] of Ireland & Rosen. Gauss and Jacobi sums (not to mention Eisenstein sums) shared a similar fate; in [616], Neumann writes

> H. Weber räumte den Gaußschen Summen in seinem "Lehrbuch der Algebra" noch einen beträchtlichen Platz ein, während in unserm Jahrhundert dieser Teil der Kreisteilungstheorie in den Hintergrund gedrängt wurde.[7]

One of the reasons why Gauss sums came back with a vengeance was the growing interest in finite fields in general due to their applications in primality testing, cryptography and coding theory. Also, Jacobi sums provide a simple means of counting solutions of certain congruences, thus giving a well-motivated introduction to problems around the Weil conjectures (see

[6] Compare the role of reciprocity in the books of Bachmann [*Die Lehre von der Kreistheilung*, 1872; *Niedere Zahlentheorie I.*, 1902], Sommer [*Vorlesungen über Zahlentheorie*, 1907], Hecke [*Vorlesungen über die Theorie der algebraischen Zahlen*, 1923], Fueter [*Synthetische Zahlentheorie*, 1917] or Landau [*Vorlesungen über Zahlentheorie*, 1927], with those that appeared in the second part of this century, in particular Hardy & Wright, [An introduction to the theory of numbers; 1938] or Borevich & Shafarevich [Number Theory; 1964], to mention only two of the best known books.

[7] H. Weber devoted a considerable part of his textbook "Lehrbuch der Algebra" to Gauss and Jacobi sums, whereas this part of cyclotomy was thrust into the background in our century.

Chapter 10). Finally, Kolyvagin's Euler systems of Gauss sums make sure that they're here to stay.

Apart from the reciprocity laws given above, which have been of central importance for the development of algebraic number theory up to the 1930s, so-called *rational reciprocity laws* (linking the power residue character of some algebraic number modulo a rational prime $p$ to the representation of $p$ by binary quadratic forms) have been studied extensively by many mathematicians; the subject started with Euler's conjectures on the cubic and quartic residuacity of 2, and was largely neglected after Gauss, Dirichlet and Jacobi had supplied proofs. Only recently there has been a revival of interest in rational reciprocity. Parts of the sometimes confusing history of discoveries and rediscoveries of results on rational reciprocity can be found in the Notes to Chapter 5. Which brings us to the question of what this book is all about.

To begin with I should mention that it was conceived as a one-volume text on the development of reciprocity laws from Euler to Artin, but eventually it seemed more reasonable to split it into two. This first part deals with reciprocity laws from Euler to Eisenstein (including topics such as rational reciprocity that originated with Dirichlet but had a renaissance during the 1970s), while the second will discuss the contributions of Kummer, Hilbert, Furtwängler, Takagi, Artin and Hasse, in other words: it will present the connection between reciprocity laws and class field theory, and in particular with explicit reciprocity laws. Whether the writing of the second part can be completed will however depend on my being in a position to do so.

Although this book is intended to serve as a source of information on the history of reciprocity laws, it cannot claim to be a substitute for Vol. 4 of Dickson's trilogy on the history of number theory;[8] such a fourth volume (on quadratic reciprocity) had actually been planned, as Dickson himself writes on page 3 of his third volume:

> Euler stated many special empirical theorems on the representability of primes by $x^2 \pm Ny^2$, where $x$ and $y$ are relatively prime (in connection with empirical theorems on the linear forms of the prime divisors of $x^2 \pm Ny^2$, to be quoted und the quadratic reciprocity law in vol IV).

For more in this connection, see I. Kaplansky's letter [425] and D. Fenster's article [231]. It seems that A. Cooper's thesis [136] on the history of quadratic residues was meant to be a part of it. Apparently, Cooper also planned to publish a history of quadratic residues and reciprocity law, but this never

[8] In particular, this is not a book on the history of mathematics: I do not hesitate to use the language of finite fields when explaining results of Fermat, and in the presentation Eisenstein's proofs of reciprocity laws using elliptic functions I do *not* follow the original proof line by line but rather present his ideas in a modern setting. The advantage of this approach should become clear upon comparing e.g. Eisenstein's 84pp article on the division of the lemniscate with our 4 pages in Chapter 9.

happened. From what I gleaned from [231], at least parts of the manuscript seem to have survived in an archive at the University of Texas – unfortunately I have not yet had the chance to read them.

This book is likewise not meant to be a textbook (courses on reciprocity laws are a rare breed anyway), but it do hope that it contains plenty of stuff with which to pep up lectures on number theory: Section 5.1 contains an approach to rational reciprocity laws using nothing beyond the quadratic reciprocity law, introductions to algebraic number theory may be seasoned with the genus theory presented in Sections 2.2 and 2.3, and those lecturing on elliptic functions may find parts of Chapter 8 attractive. I also found it appropriate to include a number of exercises. One purpose that they serve is to present material that didn't fit in the text; the main reason for having exercises, however, is that the rocky road to research is paved with interesting questions and problems. It is my hope that readers will find some problems in this book that make them get out pencil and paper. In a similar vein, the many bibliographical references were provided not only as a service to those who are interested in studying reciprocity laws and their history, but also in the hope that they may entice readers to take the dusty volumes of the collected works of Abel, Eisenstein, Kummer etc. from the shelves and start browsing through them.

The proofs up to Chapter 9 are essentially complete, although occasionally exercises are invoked to fill in some details. In Chapters 10 and 11, however, I try to tie up the material with topics that cannot be presented in detail here, and in these places the exposition acquires the character of a survey. In general, I have indicated the lack of a proof by closing the theorem with a box □.

One problem when dealing with different power residue symbols in number fields is the choice of notation; even in a case as simple as the biquadratic reciprocity law we have to distinguish four different symbols, namely the quadratic and the biquadratic residue symbols in $\mathbb{Z}[i]$, the Legendre symbol in $\mathbb{Z}$, and the rational quartic residue symbol in $\mathbb{Z}$. In order to keep the notation as simple as possible I did *not* invent a globally consistent notation but instead tried to make sure that the meaning of the symbols employed is locally constant. The same remark applies to the notion of primary and semi-primary integers: the sheer multitude of definitions prohibits the introduction of a globally consistent notion of primariness.

Appendix B contains a table of references to published proofs of the quadratic reciprocity law. I tried to make the list as complete as possible, not counting, of course, the innumerable standard proofs given in textbooks. A closer examination of these proofs will reveal that not all of them can be counted as different; on the other hand, a thorough classification (continuing the work of Baumgart [38] and Bachmann [26] from more than a century ago) would have required a book of its own (not to mention the time for writing it).[9]

The bibliography at the end of this book contains lots of references to books and articles connected with reciprocity laws; citations by acronyms like [Has] refer to additional references given at the end of each chapter which treat reciprocity only marginally or not at all. The separation of these two groups of references is of course not always clear, but I felt it was desirable to have a list of references on reciprocity that was not sparkled with entries about other issues. Occasionally, references contain a URL; these have the habit of becoming obsolete very fast – in such a case you better use a search engine or check whether the Number Theory Web maintained by Keith Matthews on

`http://www.maths.uq.oz.au:80/~krm/web_aust.html`

contains a link that works.

Finally I would like to thank all the people without whose help this book could not have been written. First of all, thanks go to my teachers Ulrich Felgner in Tübingen, who introduced me to the world of reciprocity laws, and to Albrecht Brandis, Sigrid Böge and Peter Roquette in Heidelberg. Irving Kaplansky kindly sent me Cooper's thesis on quadratic residues, and Roger Cuculière provided me with a copy of [142]. Keith Dennis made Cooke's Lecture Notes [134, 135] available to me, and Toyokazu Hiramatsu sent me a copy of his book [371] on higher reciprocity laws in Japanese. Finally, I gained access to Jacobi's Königsberg lectures [402] through the help of Herbert Pieper. A special thank you goes to Jacques Martinet, Stéphane Louboutin, Richard Mollin and Raimund Seidel for support when I needed it most. I also thank the people who helped to reduce the number of mathematical and typographical errors (mainly in the first seven chapters), namely Robin Chapman and Marinus van den Heuvel, as well as Achava Nakhash, Jim Propp, Udaï Venedem, Stefanie Vögeli-Fandel, and Felipe Zaldivar. Last not least I thank the Deutsche Forschungsgemeinschaft for their financial support over the last four years without which this book would never have seen the light of day.

I close with a quote of Kummer (letter to Kronecker, Oct. 10, 1845):

> Nicht allein in der Absicht, daß Sie meine Arbeiten kennen lernen um sie wo es sein kann bei Ihren eigenen zu benutzen, sondern besonders auch um meiner selbst Willen, um für mich etwas Ordnung und Klarheit hineinzubringen, schreibe ich Ihnen ... davon.[10]

Heidelberg, Bordeaux, Saarbrücken, Bonn, 1993–1999

[9] If this sounds like an invitation, it's because it is one.

[10] I write ... to you not only with the intention that you get to know my work so that you can use it in your own work wherever it is possible, but also for my own sake, in order to bring in some order and clarity.

# Contents