BOOK REVIEWS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 44, Number 4, October 2007, Pages 647–652
S 0273-0979(07)01152-4
Article electronically published on April 19, 2007

Reciprocity laws, from Euler to Eisenstein, by Franz Lemmermeyer, Springer-Verlag, Berlin, 2000, xix+516 pp., US$123.00, ISBN 978-3-540-66957-9

The attempts to understand and generalize the law of quadratic reciprocity, which was also part of Hilbert's 9th problem, immensely influenced the development of number theory. The study of higher reciprocity laws was the central theme of 19th-century number theory and, with the efforts of Gauss, Eisenstein, Kummer, Dedekind and others, led to the theory of algebraic number fields. Abelian extensions of algebraic number fields had been studied extensively by Kronecker, Weber and Hilbert in the second half of the 19th century. In the hands of Hilbert, Furtwängler, Takagi, Artin and Hasse the subject turned into what we now call "class field theory", also related to Hilbert's 12th problem, which asks for a generalization of Kronecker's Jugentraum.

So what is a reciprocity law? The answer to this question can take a different form whether seen from the perspective of Gauss, Dirichlet, Hilbert, or Artin, and, as Franz Lemmermeyer notes in the preface of his book, the connection between these answers is "not of the kind that springs to one's eye at first glance."

We begin with a short and obviously incomplete historical summary related to the book under review.

For an integer n and a prime number p with $(p, n) = 1$, the Legendre symbol is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv n \mod p \text{ has a solution;} \\ -1 & \text{otherwise.} \end{cases}$$

Note that $x^2 \equiv n \mod p$ has a solution if and only if $n \in (\mathbb{F}_p^*)^2$ where $\mathbb{F}_p = \mathbb{Z}/\mathbb{Z}_p$. Hence we have a homomorphism $\mathbb{F}_p^* \longmapsto \{\pm 1\}$ given by $n \longmapsto \left(\frac{n}{p}\right)$ whose kernel is $(\mathbb{F}_p^*)^2$. In particular the symbol $\left(\frac{n}{p}\right)$ is multiplicative in n. The question, how does $\left(\frac{n}{p}\right)$ vary with p for fixed n, is answered by quadratic reciprocity.

Writing the prime decomposition of $n = \pm 2^{t_0} q_1^{t_1} \cdots q_r^{t_r}$ reduces the problem to the cases $n = -1, n = 2, n = q$ for an odd prime q, and the answer in these cases is given by the

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

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right). \tag{1}$$

2000 *Mathematics Subject Classification.* Primary 11RXX; Secondary 11A15, 11-03.

Moreover,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \textit{and} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

It is an easy consequence of quadratic reciprocity that $\left(\frac{n}{p}\right)$ depends on the residue class of $p \mod 4n$.

This fact was already noted by Euler, who, following Fermat, in his investigations of representing primes by quadratic forms seems to be the first to discuss the problem whether a given prime p is a square modulo another prime q. Euler also observed the multiplicative properties of $\left(\frac{n}{p}\right)$ as a function of p, and, in modern language, his formulation of quadratic reciprocity says that there exists a group homomorphism

$$(\mathbb{Z}/4n\mathbb{Z})^* \longmapsto \{\pm 1\}$$

which for any prime p not dividing $4n$ is given by

$$p \mod 4n \longmapsto \left(\frac{n}{p}\right).$$

The quadratic reciprocity law in a more familiar form was first announced by Legendre [11] in 1788 and in a similar form to the one given in (1) was published in 1798 in [12], where the "Legendre symbol" was also introduced. Legendre was able to give only partial proofs of the law, but, in his attempts to prove the quadratic reciprocity, he proved another theorem which played an essential role in the discovery of the Local-Global principle by Hasse.

The first complete proof of the quadratic reciprocity law was given by Gauss in 1801 in *Disquisitiones Arithmeticae* [7]. After the two different proofs he had given in [7], Gauss proceeded to give a total of eight proofs in search of the extension of the law to higher power residues. He noticed that properly stating cubic or biquadratic laws requires the fields of cube or fourth roots of unity. In his work on biquadratic residues his introduction of the Gaussian integers $\mathbb{Z}[i]$ is regarded by many as the inauguration of algebraic numbers.

Even though Jacobi [8] published several theorems on cubic residues in 1827 and announced a reciprocity law for them in 1837 [9], the first complete proofs of cubic and quartic laws were given by Eisenstein [3], [4] in 1844 using the method of Gauss sums and the arithmetic of cyclotomic fields. To generalize his results to other higher residues, Eisenstein could not circumvent the major difficulty, the absence of unique factorization. In 1845 Kummer introduced his "ideal numbers" to restore unique factorization in cyclotomic fields, and in 1850 he published his reciprocity law without proof [10]. Shortly afterwards, making use of Kummer's ideal numbers, Eisenstein [5] proved a special case of what we now call Eisenstein's reciprocity law.

For an odd prime l, K a number field that contains a primitive l-th root of unity, ζ_l, and $\mathfrak{p}$ a prime ideal not dividing l, let the l-th power residue $\left(\frac{\alpha}{\mathfrak{p}}\right)_l$ be the unique l-th root of unity such that $\left(\frac{\alpha}{\mathfrak{p}}\right)_l \equiv \alpha^{(N\mathfrak{p}-1)/l} \mod \mathfrak{p}$. Then we have

Eisenstein's Reciprocity Law. *Suppose that $\alpha \in \mathbb{Z}[\zeta_l]$ is congruent to a rational integer modulo $(1-\zeta_l)^2$. Then for all integers $a \in \mathbb{Z}$ prime to l we have*

$$\left(\frac{\alpha}{a}\right)_l = \left(\frac{a}{\alpha}\right)_l. \tag{2}$$

Nine years after Eisenstein's proof of this special case, Kummer proved the general reciprocity law for a regular prime p (i.e. p does not divide the class number) in the ring $\mathbb{Z}[\zeta_p]$ of the p-th cyclotomic field $\mathbb{Q}[\zeta_p]$. The extension of ideal theory to all algebraic number fields was done by Dedekind, who also attached a zeta function to them generalizing that of Riemann. He recognized the importance of his zeta functions and obtained their Euler product as a consequence of his ideal theory.

One should also mention that, in the meantime, Eisenstein gave remarkable proofs of quadratic, cubic and biquadratic laws using the circular and elliptic (lemniscatic) functions.

As pointed out by A. Weil in his introduction of Kummer's collected papers, using the ideas in Kummer's work, one can state the reciprocity law in another and in some sense more natural way. This was not pursued by Kummer but was taken up by Hilbert, who reinterpreted and generalized the quadratic law to arbitrary algebraic number fields in terms of the "Hilbert symbol".

Let $\mathbb{Q}_p$ be the field of p-adic numbers, the completion of $\mathbb{Q}$ with respect to the p-adic norm, $|\cdot|_p$, where $|a|_p = p^{-v_p(a)}$ and $v_p(a)$ is the exponent to which p appears in the prime factorization of a. For $a, b \in \mathbb{Q}_p$, the Hilbert symbol is defined as

$$\left(\frac{a,b}{p}\right) = \begin{cases} +1 & \text{if } ax^2 + by^2 - z^2 \text{ has a solution } (x,y,z) \in \mathbb{Q}_p^3, \\ -1 & \text{otherwise.} \end{cases}$$

The Hilbert symbol can also be defined for the "infinite prime" as $\left(\frac{a,b}{\infty}\right) = +1$ if and only if $ax^2 + by^2 - z^2$ has a solution $(x,y,z) \in \mathbb{R}^3$. Now Hilbert's quadratic reciprocity law for $\mathbb{Q}$ reads as

Hilbert's Quadratic Reciprocity Law. *For $a, b \in \mathbb{Q}^*$ we have*

$$\prod_p \left(\frac{a,b}{p}\right) = 1 \tag{3}$$

where the product runs over all primes including the infinite one.

Hilbert showed that for p an odd prime and a not divisible by p, his symbol satisfies

$$\left(\frac{a,b}{p}\right) = \left(\frac{a}{p}\right)^{v_p(b)}. \tag{4}$$

Upon taking a, b to be two distinct odd primes p, q, the quadratic reciprocity as in (1) follows from that of Hilbert's (3) after using (4) and the easily verifiable identity $\left(\frac{p,q}{2}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

In his famous ICM address in 1900, Hilbert asked for a proof of the most general reciprocity law for lth power residues as part of his 9th problem. Four years after Hilbert's address and fifty years after Kummer's proof in the regular case, Kummer's reciprocity law in $\mathbb{Q}[\zeta_p]$ for irregular primes was proven by Furtwängler [6] in 1904. During the period 1920–1922 Takagi [13] showed that Kummer's results follow from his remarkable development of class field theory. It was Artin [1] who in 1923 conjectured a "general reciprocity law" which contained all past reciprocity laws of Gauss, Kummer, Eisenstein, Takagi and others as special cases. Artin succeeded in proving his conjecture in 1927 [2], using a key idea provided by Tchebotarev's paper [14] on the density of primes.

It can be seen that Euler's formulation of quadratic reciprocity mentioned above is essentially a special case of

Artin's Reciprocity Law. *Let k be an algebraic number field, K/k a finite abelian extension, C_k the idèle class group of k, $N_{K/k} : C_K \to C_k$ the norm homomorphism, and $\mathfrak{p}$ a finite prime of k. Then the map sending $\mathfrak{p}$ to the Frobenius automorphism $\sigma_{K/k}(\mathfrak{p})$ induces an isomorphism*

$$\mathbb{C}_k/N_{K/k}C_K \cong \mathrm{Gal}(K/k).$$

When k contains the m-th roots of unity and $K = k(\alpha^{1/m})$, it follows from the definitions that $\sigma_{K/k}(\mathfrak{p})$ is essentially the power residue symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$, and Artin's theorem implies that, for fixed α, the value $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ depends only on the class $[\mathfrak{p}]$ of $\mathfrak{p}$. Making this dependence explicit in the case $m = 2$ yields quadratic reciprocity.

Artin was led to his reciprocity law in his investigations of a new kind of L-functions, now called Artin L-functions, and indeed his reciprocity law can also be stated in terms of factorization of the Dedekind zeta function of K in terms of L-functions attached to the field k. This form of the law in the quadratic case is already apparent in the work of Dirichlet and in what we might call Dirichlet's quadratic reciprocity law.

Let $\zeta_K(s) = \sum_{\mathfrak{a}\in \mathrm{O}_K} \frac{1}{(N\mathfrak{a})^{-s}}$ be the Dedekind zeta function of a number field K, $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ the Riemann zeta function and $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}$ the Dirichlet L-function attached to a quadratic character $\chi \mod q$; i.e. $\chi : \mathbb{Z} \to \mathbb{C}$ is a homomorphism which is periodic with period q such that $\chi(n) \in \{\pm 1\}$ if $(n,q) = 1$ and $\chi(n) = 0$ if $(n,q) \neq 1$. Then we have

Dirichlet's Quadratic Reciprocity Law. *Let χ be a non-trivial primitive quadratic character $\mod q$, $K = \mathbb{Q}(\sqrt{\chi(-1)q})$. Then the zeta function of the field K satisfies*

$$\zeta_K(s) = \zeta(s)L(s,\chi). \tag{5}$$

To see why (5) is equivalent to (1) we first note that if $K/\mathbb{Q}$ is a quadratic extension of discriminant D, basic algebraic number theory shows that the Legendre symbol $\left(\frac{D}{p}\right)$ determines how a prime ideal (p) of $\mathbb{Z}$ decomposes in K– i.e. whether it remains prime (inert), becomes a product of two distinct prime ideals (split) or becomes a square of a prime ideal (ramifies). More precisely

$$p \text{ is } \begin{cases} \text{ramified} & \text{if and only if } p|q, \\ \text{split} & \text{if and only if } \left(\frac{D}{p}\right) = 1, \\ \text{inert} & \text{if and only if } \left(\frac{D}{p}\right) = -1. \end{cases} \tag{6}$$

On the other hand, using the Euler product expansion for the ζ_K together with its factorization in (5) gives

$$p \text{ is } \begin{cases} \text{ramified} & \text{if and only if } \chi(p) = 0 \text{ if and only if } p|q, \\ \text{split} & \text{if and only if } \chi(p)) = 1, \\ \text{inert} & \text{if and only if } \chi(p) = -1. \end{cases} \tag{7}$$

Finally, if q is an odd prime, there is a unique quadratic character modulo q, given by $\chi(n) = \left(\frac{n}{q}\right)$. Now it is easy to see that a comparison of the two characterizations of the splitting of primes in (6) and (7) gives the quadratic reciprocity as in (1).

Artin's reciprocity law answers Hilbert's 9th problem in the case of Abelian extensions. The formulations given above can be thought of as describing the splitting of primes in the field K in terms of data attached to the base field k. Similar questions can be raised for general extensions. The answer in that case is still open and belongs to the theory of Artin L-functions and Langland's conjectures.

Clearly a book covering the latest developments from Artin till today could be the subject of a third volume after the promised and to be welcomed second volume discussing "the contributions of Kummer, Hilbert, Furtwängler, Takagi, Artin and Hasse." With that remark we now turn to Lemmermeyer's book at hand, which is an excellent account of the history and development of reciprocity laws from Euler to Eisenstein, written with the hindsight of more recent developments.

The book starts with a very informative chapter on the genesis of quadratic reciprocity, moves quickly in the next two chapters to quadratic and cyclotomic fields, and gives a modern account of different proofs of the quadratic reciprocity law together with some applications to primality tests. Power residues, higher and rational reciprocity laws, and their various proofs are the subject of the next seven chapters which form the bulk of the book. In Chapter 10 the author skillfully uses Gauss' last entry to indicate the connection between biquadratic reciprocity, elliptic curves, zeta functions and Weil conjectures. Prime ideal factorization of Gauss sums is the central theme of the last chapter, where their applications to proofs of Eisenstein reciprocity law and properties of ideal class groups, together with some recent refinements and generalizations, are given. Except for the two chapters (favorites of this reviewer!), Chapter 8 about Eisenstein's analytic proofs and Chapter 10 on Gauss' last entry, the treatment remains almost completely algebraic. In fact the rarity of analytic methods and ideas might be the only serious criticism that I have for this otherwise comprehensive treatment of reciprocity laws.

The mathematical prerequisites call for acquaintance with fundamentals of algebraic number fields, Galois theory and complex function theory. As also pointed out by the author, the book is not meant to be a textbook, although each chapter can form a basis for a seminar course or independent study. There are illuminating historical notes and additional references, together with several complementing and interesting exercises at the end of each chapter.

With its comprehensive treatment of the subject, extensive references, historical notes, three appendices on dramatis personae, chronology of proofs, and open problems, Lemmermeyer's book fulfills "its intention to serve as a source of information on the history of reciprocity laws" with flying colors.

References

[1] E. Artin, *Über eine nee Art von L-Reihen*, Bah. Math. Sem. Hamburg **3** (1923) 89–108.
[2] E. Artin, *Bowes der allgemeinen Rezirozitätsgesetzes* , Bah. Math. Sem. Hamburg **5** (1927) 353–363.
[3] G. Eisenstein, *Bowes des Reciprocitätessatzes föur die cubischen reste in der Theorie der aus den dritten Wurzeln der Einheit zusammengesetzten Zahlen*, J. Reine Angew. Math. **27** (1844), 289–310.

[4] G. Eisenstein, *Nachtrag zum cubischen Reciprocitätessatzes für die aus den dritten Wurzeln der Einheit zusammengesetzten Zahlen, Criterien des cubischen Charaters der Zahl 3 und ihrer Teiler*, J. Reine Angew. Math. **28** (1844), 28–35.
[5] G. Eisenstein, *Beweis der allgemeinsten Reciprocit—ätessatzeszwischen reellen und komplexen Zahlen*, Monatsber. Akad. Wiss. Berlin, 1850, 189–198.
[6] Ph. Furtwängler, *Über die Reziprozitatsgesetze zwischen l-ten Potenzresten in algebraischen Zahlkorper, wenn l eine ungerade Primzahl beduetet*, Math. Ann. **58** (1904), 1–50. MR1511227
[7] C. F. Gauss, *Disquisitiones Arithmeticae*, reprint, Springer-Verlag (1986). MR837656 (87f:01105)
[8] C. G. J. Jacobi, *De residuis cubicis commentatio numerosa*, J. Reine Angew. Math. **2** (1827), 66–69.
[9] C. G. J. Jacobi, *Über die Kreisheilung und ihre Anwendung auf die Zahlentheorie*, Berliner Akad. Ber. (1837), 127–136.
[10] E.E. Kummer, *Allgemeine reciprocitätsgesetze für beliebig ohe Potenzreste*, Monatsber. Akad. Wiss. Berlin (1850), 154–165.
[11] A.M Legendre, *Recherches d'analyse indetérminée*, Histoire de de l'Academie Royale des Sciences de Paris (1785), 465–559.
[12] A.M Legendre, *Essai sur la theorie des nombres*, 1st edition, Paris, 1798.
[13] T. Takagi, *Collected Papers*, Springer-Verlag, Tokyo, 1990. MR1129240 (93b:01049)
[14] N. Tcheboratev, *Die Bestimmung der Dichtigkeit einer Menge von Rpimzahlen, welche zu einer gegebenen Substitutionklasse gehoren*, Math. Ann. **95** (1926), 191–228. MR1512273

Özlem Imamoğlu
ETH Zürich
E-mail address: ozlem@math.ethz.ch