SOME ASPECTS ON INTERACTIONS BETWEEN ALGEBRAIC NUMBER THEORY AND ANALYTIC NUMBER THEORY

Katsuya MIYAKE*
Department of Mathematics
Tokyo Metropolitan University
miyakek@comp.metro-u.ac.jp

1. Prehistory of Algebraic Number Theory

1.1 P. de Fermat (1601-1665)

Pierre de Fermat is the great grand father of the modern number theory. He himself published only few of his findings and proofs which he suggested to have obtained. However, what he found on numbers succeeded in attracting Euler. Even with his gifts on mathematics it was not an easy task for Euler to reconstruct what was in the wide view of Fermat. All through his life, however, he could finally obtain proofs and a few disproofs to all but 'the last theorem' which Fermat stated on numbers. Then Lagrange and Legendre followed; and Gauss founded the basic frame work of a modern science on numbers on the fertile ground. Hence it may be allowed to call Fermat the great grand father of the modern number theory and Euler its grand father.

We point out here just one of Fermat's theories which we may clearly understand as arithmetic of the quadratic field $\mathbb{Q}(\sqrt{-1})$.

◇ Determination of the numbers of form $a^2+b^2,\ a,\ b\in\mathbb{Z}$.

On the days of Fermat it has well been recognized that the numbers of form $a^2+b^2,\ a,\ b\in\mathbb{Z}$, are closed under multiplication; we may even say that Fermat and some of his contemporaries must have been familiar

*The author was partly supported by the Grant-in-Aid for Scientific Research (B) No. 11440013, Japan Society for the Promotion of Science while he prepared this work.
This paper is submitted to be published in *Number Theoretic Methods-Future Trends*, ed. by Chaohua Jia and Shigeru Kanemtisu, DEVM Series, Kluwer Academic Publishers.

with the formula

$$(a^2 + Nb^2)(c^2 + Nd^2) = (ac \pm Nbd)^2 + N(ad \mp bc)^2$$

for integers N with small absolute values.

Fermat found all the 'generators' (= 'atoms') of sums of two squares under the multiplicative structure ([Fe-1891].II.213-214,221-222);

$$\begin{aligned} &\text{a prime } p \text{ divides a primitive } a^2 + b^2,\ a,\ b \in \mathbb{Z} \\ &\iff p = a^2 + b^2,\ a,\ b \in \mathbb{Z} \\ &\iff p \equiv 1 \mod 4 \\ &\iff p \in N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\mathbb{Z}[\sqrt{-1}]). \end{aligned}$$

◇ He also handled binary quadratic forms x^2+2y^2, x^2+3y^2 ([Fe-1891].II. 313,403,431-436) and $x^2 - 2y^2$ ([Fe-1891].II.221,224-226,434,441). As for the last case, he recognized the importance of the solution $(1,1)$ of the equation $x^2 - 2y^2 = -1$ which represents the fundamental unit $\varepsilon = 1+\sqrt{2}$ of the real quadratic field $\mathbb{Q}(\sqrt{2})$ though, of course, he did not directly work with these irrational numbers; he used $(3,2)$ and $(3,-2)$, i.e. $\varepsilon^2 = 3 + 2\sqrt{2}$ and $\varepsilon^{-2} = 3 - 2\sqrt{2}$, when he needed a unit e with $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(e) = 1$.

◇ He had a firm belief that he found a *new science* on numbers in his various findings ([We-1984].118-119).

1.2 L. Euler (1707-1783)

◇ Euler investigated in binary quadratic forms $x^2 + Ny^2$ for $N = 2, 3, 5, 6, 7, 14$ and also 17 ([Eu-1911].I-2.6-17,196-199,556-575,I-3.218-239,273-275); he added an important remark that a solution (a, b) of $x^2 - Ny^2 = 1$ provides a good rational approximation a/b for $\sqrt{N}$.

As for quadratic irrational numbers, he finally introduced them into the theory of binary quadratic forms in his book *Algebra* ([Eu-1911].I-1.1-498).

◇ He was aware of the quadratic reciprocity law ([We-1984].209,218-219).

1.3 J. L. Lagrange (1736-1813)

◇ Lagrange started to handle all of the binary quadratic forms with a fixed discriminant D simultaneously, and introduced the equivalence classes,

$$\{\text{binary quadratic forms with a fixed discriminant } D\}/\mathrm{GL}_2(\mathbb{Z})$$

in his *Recherches d'Arithmetique* ([La-1867].III.697-758,759-795). This set of classes corresponds to the ideal class group of the order $\mathbb{Z}+\mathbb{Z}\sqrt{D}$ in the quadratic field $\mathbb{Q}(\sqrt{D})$.

2. Prelude to the Birth of Analytic Number Theory

2.1 L. Euler (1707-1783)

Euler found and proved important results on the infinite series

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} \cdots$$

which we now call Riemann's zeta function, and on some other related series (cf. e.g. *Introductio in Analysin Infinitorum*, [Eu-1911].I-8). One of them is the Euler product formula:

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \textit{ etc.} = \frac{1}{(1-\frac{1}{2^s})(1-\frac{1}{3^s})(1-\frac{1}{5^s})(1-\frac{1}{7^s}) \textit{ etc.}}$$

where the product on the right hand side is taken over all prime numbers.

◇ In the case of $s = 1$, we have

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \textit{ etc.} = \frac{1}{(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{7}) \textit{ etc.}}.$$

The left hand side is the harmonic series whose n-th partial sum is as large as $\log n$ as n tends to infinity. (Euler denoted it by $\log\infty$.) Hence, first of all, the Euler product shows that there exist infinitely many prime numbers. By taking the logarithm of both sides Euler pointed out, for example, that the sum of all reciprocals of primes

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \textit{ etc.}$$

has infinite magnitude as large as $\log\log\infty$ ([Eu-1911].I-14.87-100).

◇ He was also able to determine the values of $\zeta(s)$ at positive even integers;

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(2n) = \frac{1}{2}(-1)^{n-1}\frac{b_{2n}}{2n!}(2\pi)^{2n}$$

where b_{2n} is the nth Bernoulli number ([Eu-1911].I-14.434-439).

2.2 A.-M. Legendre (1752-1833)

◇ In his book *Recherches d'Analyse Indéterminée* ([Le-1785]), Legendre clearly stated the quadratic reciprocity law and tried to prove it. In the course of his trial, he used the Prime Number Theorem in Arithmetic Progressions. He had a strong belief in it. He himself, however, could not find any effective ways to go. And he could not complete his proof of the reciprocity law either. It was Gauss who first gave a full proof. He published two different proofs at the beginning of the new century; he put them in his epoch-making book *Disquisitiones Arithmeticae* ([G-1801]). A little later in 1837, Dirichlet was to give a genuine proof to the prime number theorem in arithmetic progressions in [Di-1837b]; it should be regarded as the year of the birth of analytic number theory.

◇ Legendre is the first author who used the terms 'theory of numbers' instead of 'arithmetic'. The book was published in 1798 with the title *Essai sur la théorie des nombres* ([Le-1798]). The third edition of the book appeared in 1830 in two big volumes with the simplified title *Théorie des Nombres* ([Le-1830]).

In the book, he introduced the counting function of prime numbers

$$\pi(x) = \text{the number of primes not exceeding } x,$$

and stated that $\pi(x)$ is approximately equal to $x/(\log x - 1.08366)$. (The symbol '$\pi(x)$' for the function was introduced later by N. Nielsen [Ni-1906].) He was unable to prove this. After some contributions ([Tc-1848,-52]) of P. L. Tchebychef (1821-1894), Jacques Hadamard (1865-1963) and Charles Jean de la Vallée Poussin (1866-1962) independently proved the Prime Number Theorem later at the end of the 19th century ([Ha-1896] and [VP-1896]); it states

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

In a letter with the date $\sqrt[3]{6064321219}$ (August 24, 1823) to his friend B. Holmboe, N. H. Abel wrote about the statement of Legendre on $\pi(x)$; he picked up no other than this from the Essai because he thought it the most remarkable result in mathematics ([Ab-1902], Correspondence 5).

In 1863, the second volume of Gauss' Work [G-1863] was published. It contains a letter of Gauss to Encke dated December 24,1849 (pp.444–447). According to it, he obtained Lambert's table of logarithms with a table of prime numbers as a supplement in 1792 or 1793 and was aware that the integral $\int \frac{dn}{\log n}$ numerically approximates $\pi(n)$ very well.

3. Algebraic Equations and the Fundamental Theorem of Algebra

3.1 Ars Magna

In the 16th century a monumental step toward a flourishment of algebra was taken in Italy. Scipione del Ferro (1465-1526), Professor of University of Bologna, found a formula for a root of the cubic equation $x^3 + ax = b$, $a > 0$, $b > 0$. At the time the common way to write and handle algebraic equations was the geometric one. Neither the concept nor the symbol of the 'number 0' were introduced in Europe yet. Then cubic equations were classified into several types. Scipione del Ferro succeeded in solving one of them. Challenged by Niccolò Tartaglia (1500?-1557), he selected one of his disciples, Antonio Maria Fiore, for the mathematical contest. The challenger Tartaglia worked hard for it and succeeded in finding a formula for a root of another type of cubic equations besides del Ferro's by the day of the contest, and won an overwhelming victory over Fiore who armed only with the formula of his teacher.

After a while, Girolamo Cardano (1501-1576) learned the formula for the above equation of del Ferro from Tartaglia after eager and insistent requests. Then he succeeded in solving all types of cubic equations. Moreover, one of his disciples, Lodovico Ferrari (1522-1565), was able to solve biquadratic equations. He reduced it to cubic and quadratic equations. Cardano published all of these results in *Artis Magnæ Sive de Regulis Algebraicis* [Ca-1545] (cf. [Ca-1968]).

◇ A root of the cubic equation $x^3 + ax + b = 0$ is given by the formula

$$\sqrt[3]{\frac{-b}{2} + \sqrt{(\frac{-b}{2})^2 + (\frac{a}{3})^3}} + \sqrt[3]{\frac{-b}{2} - \sqrt{(\frac{-b}{2})^2 + (\frac{a}{3})^3}}$$

if we choose the two cubic roots properly. Cardano and his disciples have already well understood that the cubic equation has three real roots if and only if the square root $\sqrt{(\frac{-b}{2})^2 + (\frac{a}{3})^3}$ is imaginary, that is, $(\frac{-b}{2})^2 + (\frac{a}{3})^3 < 0$. Then they became well acquainted with imaginary numbers, perhaps to be ready for mathematical contests. Rafael Bombelli (1526-1572) wrote up a perfect treatment of complex numbers in his book *Algebra* ([Bo-1572]).

The Ars Magna contains many cubic equations with three real roots. Cardano, however, did not use imaginary numbers nor the formula to obtain these roots. Here he handled only those equations for which one can find a real root almost at once. Then he factored out the linear term to get quadratic equations.

He introduced imaginary numbers in Chapter XXXVII *On the Rule for Postulating a Negative* with the following problem ([Ca-1968], p.219):

Divide 10 into two parts the product of which is 30 or 40.

He gave the answer $5+\sqrt{-15}$ and $5-\sqrt{-15}$ in the case of 40.

It should be noted that imaginary numbers could not have been numbers in reality for them at their time. These were not mathematical reality but something belonging to arts with which they tacitly handled cubic equations and other surely existing objects of algebra.

3.2 The Fundamental Theorem of Algebra

D. S. Smith says that Peter Roth (1580-1617) was the first author who openly stated the Fundamental Theorem of Algebra in 1608 ([Ro-1608]); cf. [Sm-1925].II.474. Then Albert Girard (1595-1632) put it forth in his book *Invention nouvelle en l'algébre* [Gi-1637]. An important step was made by J. le Rond d'Alembert (1717-1783) in his memoirs [dA-1746]. He tried hard to show that a (non-constant) polynomial with real coefficients has a root of the form $a+b\sqrt{-1}$, a, $b \in \mathbb{R}$, if it does not have any real roots; then it was not very hard for him to show by this that a polynomial has the same number of roots as its degree.

Lagrange opened the gate toward investigations in the mechanism hidden behind the relations of roots and coefficients of a polynomial in [La-1770]; there he introduced 'Lagrangian resolvents'.

C. F. Gauss (1777-1855) published his first proof to the fundamental theorem of algebra in [G-1799]. (He implicitly used the completeness of the field of real numbers.) By this, anyway, he provided not only algebra but also analysis with a rigid universal domain, the field of complex numbers.

4. The 19th Century begins

4.1 C. F. Gauss (1777-1855)

◇ The number theory of the 19th century began with the celebrated book of Gauss, *Disquisitiones Arithmeticae* ([G-1801]). He began it with the concept of the congruence relation of integers, and introduced the term 'modulus' and the symbol ≡ with numerical examples, $-16 \equiv 9 \pmod 5$ and $-7 \equiv 15 \pmod{11}$. This book contains two complete proofs to the quadratic reciprocity law, and a modern theory of cyclotomy in the last *Section Seven*. He published his papers toward biquadratic reciprocity law [G-1828] and [G-1932] 27 years later. In 1801, however, he had already prepared *Section Eight* ([G-1801*]) of *Disquisitiones Arithmeticae* which was posthumously published by Dedekind in 1863. Günther Frei recently pointed out in [Fre-2001] that "*Section Seven on Cyclotomy* served only as a preparation for Section Eight which was to contain a *Third Proof of Quadratic Reciprocity Law*, a proof Gauss planned to generalize to *Higher Reciprocity*".

Anyway Gauss introduced the ring $\mathbb{Z}[\sqrt{-1}]$ for the biquadratic case in 1828, and proposed a research problem of establishing Higher Power Reciprocity Laws though he might not have done it explicitly. Hereafter through the century or more, this became a principal motivation for developing algebraic number theory. First in 1844 Gotthold Eisenstein (1823-1852) made important contributions for the cubic case in a series of papers [Ei-1844a-e]; he had naturally to develop arithmetic in the ring $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ of the cyclotomic field of cubic roots of unity. Then Kummer, Kronecker, Dedekind, and so on, followed.

4.2 N. H. Abel (1802-1829)

We have to pick up N. H. Abel who did not leave any distinguished works on number theory but supplied important sources of ideas for the development of algebraic number theory due particularly to Kronecker, and indirectly to Zolotareff. One of his works we mention here is on algebraic equations, and the other is on elliptic functions.

Before we go into these main topics, however, we should also pay attention to his work [Ab-1826] on elliptic and hyperelliptic integrals; this indirectly motivated Zolotareff for his divisor theory in algebraic number fields (cf. Section 7.4 below). Abel studied there those hyperelliptic differential forms $\frac{\rho dx}{\sqrt{R}}$ with polynomials ρ and R in x whose integrals are given as logarithm functions of the form $\log \frac{y+\sqrt{R}}{y-\sqrt{R}}$ with a polynomial y, and characterized them in terms of the continued fraction expansion of the square root $\sqrt{R}$. His criterion is the expansion to be periodic and of a certain special form. In the last section Abel deals with elliptic integrals, that is, the case where R is a monic polynomial of degree 4. He explicitly stated that the integral

$$\int \frac{\left(x+\frac{\sqrt{5}+1}{14}\right)dx}{\sqrt{\left(x^2+\frac{\sqrt{5}-1}{2}\right)^2+\left(\sqrt{5}-1\right)^2 x}}$$

could be expressed by logarithms.

It is apparent that the work of Legendre [Le-1811] or its revised version [Le-1825] on elliptic integrals was in the background of this work of Abel.

◇ Abelian Equations

As is well known, Abel succeeded in proving that there cannot exist any algebraic formulas for roots of general polynomials of degree equal to 5 ([Ab-1824]). This is an important and essential development on algebraic equations after Lagrange opened the door by his work [La-1770] as we pointed it out above in Section 3.2. Abel left the full-scale theory of algebraic equations to Évariste Galois. His interest tended to characterization of solvable equations, and found the *Abelian criterion* because of which we now have the names *Abelian groups* and *Abelian equations*. It is Kronecker who introduced the word 'Abelian equations'. He first used it in [Kr-1853] to mean cyclic polynomials, that is, polynomials with cyclic Galois groups. Then he enlarged its use to mean polynomials with Abelian Galois groups (cf. [Kr-1857a,-1877]).

◇ Elliptic Functions

Abel developed a beautiful theory of elliptic functions in [Ab-1827], and found quite new Abelian polynomials in the work. Legendre used the word 'elliptic functions' before Abel; however, all he worked on were elliptic integrals with analysis in the real number field. In [Ab-1827] Abel started his investigation by considering inverse functions of elliptic integrals by utilizing complex analysis. Since then we have customarily been using the word 'elliptic functions' in Abel's sense. His arithmetical instinct did not miss smelling out the importance of elliptic functions with complex multiplication; and he attracted Kronecker especially with a few explicit numerical examples. The terminology 'complex multiplication' was also introduced by Kronecker who fostered 'Kronecker's dream in his youth' (see below Section 7.1 and [Kr-1857a,-1880b]). The theory of complex multiplication must also have supplied sources for Dedekind to formulate the concepts of 'modules', 'orders' and 'ideals' of an algebraic number field in [De-1871,1877a,-1879,-1893]. (See below Sections 7.2 and 7.3.)

5. Birth of Analytic Number Theory

As Euler is the father of modern number theory (cf. 1-1), then so is P. G. Lejeune Dirichlet (1805-1859) of Analytic Number Theory. It was born in his paper [Di-1837b] where he proved the Prime Number Theorem in Arithmetic Progressions conjectured by Legendre (cf. 2-2). His strategy was to follow Euler's idea of utilizing Euler product formulas. However, none of the modified harmonic series for arithmetic progressions have necessary product formulas as they are. To overcome the difficulty he brought out a brilliant idea; he utilized all of the modified harmonic series with initial terms which are relatively prime to the fixed common difference, and put them together by Dirichlet characters defined for the common difference. Then the orthogonal relations of the characters lead us to the desired end. Thus Dirichlet's L-series were sent out into the world. Let us see them more closely:

Let d be the fixed common difference; for simplicity, Dirichlet restricted himself to the case where d is an odd prime number. For each a, $0 \leq a \leq d-1$, put

$$C_a = \{a + dn \mid n = 0,\ 1,\ 2, \dots\},$$
$$\zeta(s; C_a) = \sum_{n=0}^{\infty} \frac{1}{(a+dn)^s}.$$

Let χ be a character of the Abelian group $(\mathbb{Z}/d\mathbb{Z})^\times$, that is, a homomorphism of the group to $\mathbb{C}^\times$. The values are of finite order and hence roots of unity ($\varphi(d)$-th roots of 1 where φ is the Euler function). We naturally regard χ as a map from $\mathbb{Z}$ to $\mathbb{C}$ with $\chi(m) = 0$ if m is not relatively prime to d, i.e. $(m, d) \neq 1$; thus we get Dirichlet characters modulo d which still remain multiplicative. Define Dirichlet's L-functions by

$$L(s; \chi) = \sum_{a=0}^{d-1} \chi(a) \zeta(s; C_a) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Then we have product formulas

$$L(s; \chi) = \prod_{p,\ prime} \frac{1}{1 - \chi(p) p^{-s}}.$$

Note that $L(s; \chi)$ is a multiple of Riemann's zeta function by a finite product $\prod_{p|d}(1 - p^{-s})$ for the trivial character $\chi = 1$. On one hand, therefore, we have $L(1; 1) = +\infty$ at once. Dirichlet, on the other hand, could show that $L(s; \chi)$ converges and is not equal to 0 at $s = 1$ for every non-trivial χ. Hence the value of $\log L(s; \chi)$ at $s = 1$ is $+\infty$ if $\chi = 1$ and finite if $\chi \neq 1$. Now let us consider the series

$$\lambda(s; \chi) := \sum_{p,\ prime} \frac{\chi(p)}{p^s}.$$

Then we see from the values of $\log L(s; \chi)$ at $s = 1$ that $\lambda(1; 1) = +\infty$ and $\lambda(1; \chi)$ is a finite value for each non-trivial χ. It follows from the orthogonal relations of characters that

$$\sum_{p,\ prime \in C_a} \frac{1}{p^s} = \varphi(d)^{-1} \sum_{\chi} \chi(a)^{-1} \lambda(s;\chi)$$

for every $a \in (\mathbb{Z}/d\mathbb{Z})^\times$. Therefore the values of the right hand side at $s = 1$ shows

$$\sum_{p,\ prime \in C_a} \frac{1}{p} = +\infty.$$

Hence we conclude that the set C_a of integers in an arithmetic progression contains infinitely many primes if the initial term a is relatively prime to the common difference d.

◇ Dirichlet's Class Number Formula

Dirichlet expanded his analytic method to investigate binary quadratic forms. He had already concerned the works of Fermat, Euler and Lagrange on the subject in [Di-1833,-1834]. In [Di-1834] he saw the basic structure of the solutions of a Fermat equation $x^2 - Dy^2 = 1$ with $D > 0$, i.e., that of the units of the real quadratic field $\mathbb{Q}(\sqrt{D})$.

For the first time in [Di-1838] he proved his class number formula of binary quadratic forms with a *negative* prime discriminant; he introduced Dirichlet series of the form $\sum_{n=1}^{\infty} (\frac{n}{q}) \frac{1}{n^s}$ and $\sum_{n,odd} (\frac{n}{p}) \frac{(-1)^{(n-1/2)}}{n^s}$, and also $\sum \frac{1}{(ax^2+2bxy+cy^2)^s}$ where q and p are prime numbers of the form $4\nu+3$ and $4\nu+1$, respectively, $(\frac{n}{q})$ and $(\frac{n}{p})$ are Legendre symbols for quadratic residues, and $ax^2 + 2bxy + cy^2$ is a quadratic form with discriminant $-q$ or $-p$. This time he observed and compared asymptotic behaviors of these series as s tends to 1 from the right. Then in [Di-1839] he successfully handled general binary quadratic forms in both cases with positive and negative discriminant D.

As soon as we translate his works in arithmetic of the quadratic field $\mathbb{Q}(\sqrt{D})$, we find the zeta function of the field and its decomposition into a product of Riemann's zeta function and an L-function. It would have then become a central motivation of Dedekind in number theory to seek similar results for pure cubic fields, that is, cubic fields of the form $\mathbb{Q}(\sqrt[3]{D})$.

◇ Dirichlet's Unit Theorem

This may be a suitable place to give a remark on Dirichlet's Unit Theorem. As we pointed out above, he actually found the structure of the unit group of a real quadratic field in [Di-1834] though he did not openly handle any irrational quadratic numbers. In [Di-1841] he introduced irrational numbers and norm forms of algebraic number fields as an important, interesting class of homogeneous forms of cubic and higher degree. More precisely, let $P(X)$ be a monic polynomial with rational integer coefficients:

$$P(X) = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \ldots + a_{n-1} X + a_n,\ a_1,\ a_2, \ldots,\ a_n \in \mathbb{Z};$$

suppose that $P(X)$ is irreducible over $\mathbb{Q}$, and let $\alpha = \alpha_1,\ \alpha_2, \cdots,\ \alpha_n$ be all of the roots of $P(X) = 0$ in $\mathbb{C}$. Let $X_1,\ X_2, \ldots,\ X_n$ be a set of independent variables and put

$$F(X_1, X_2, \ldots, X_n) = \prod_{j=1}^{n} (X_1 \alpha_j^{n-1} + X_2 \alpha_j^{n-2} + \ldots + X_{n-1} \alpha_j + X_n).$$

This is a homogeneous polynomial of degree n in $X_1,\ X_2, \ldots,\ X_n$ with coefficients in $\mathbb{Z}$. The favorite example of Dirichlet must be the quadratic form $X^2 - DY^2 = (X - \sqrt{D}Y)(X + \sqrt{D}Y)$ of a Fermat equation. As was classically well noticed, the solutions of the Fermat equation $X^2 - DY^2 = 1$, $D > 0$, play an important role also in solutions of $X^2 - DY^2 = m$ for an integer $m \geq 1$. Suppose, in general, that we have a solution $T_1,\ T_2, \ldots, T_n \in \mathbb{Z}$ for $F(X_1, X_2, \ldots,\ X_n) = m$ and $U_1,\ U_2, \ldots, U_n \in \mathbb{Z}$ for $F(X_1,\ X_2, \ldots,\ X_n) = 1$. Then we can construct many other solutions of the former equation by *complex numbers*

$$(T_1 \alpha^{n-1} + T_2 \alpha^{n-2} + \ldots + T_{n-1} \alpha + T_n)(U_1 \alpha^{n-1} + U_2 \alpha^{n-2} + \ldots + U_{n-1} \alpha + U_n)^N$$

$(N \in \mathbb{Z})$ in the field $\mathbb{Q}(\alpha)$ if we express them in the form

$$S_1 \alpha^{n-1} + S_2 \alpha^{n-2} + \ldots + S_{n-1} \alpha + S_n,\quad S_1,\ S_2, \ldots, S_n \in \mathbb{Z}.$$

Finally in 1846, Dirichlet stated his unit theorem in the paper *Zur Theorie der Complexen Einheiten* [Di-1846] which clarifies the structure of the solutions $U_1,\ U_2, \ldots,\ U_n \in \mathbb{Z}$ for $F(X_1, X_2, \ldots, X_n) = 1$ through units

$$U_1 \alpha^{n-1} + U_2 \alpha^{n-2} + \ldots + U_{n-1} \alpha + U_n,\quad U_1,\ U_2, \ldots, Un \in \mathbb{Z},$$

in the field $\mathbb{Q}(\alpha)$.

E. E. Kummer started his research in cyclotomic integers in 1844 ([Ku-1844]) and published his first paper on '*ideale complexe Zahlen*' in 1846 ([Ku-1846b,-1847b]). It was eventually almost in the middle of the 19th century that algebraic numbers became fully recognized as proper arithmetic objects.

6. Cyclotomic Fields

In the 1840's, the German number theorists, Gauss, Jacobi, Eisenstein, Dirichlet, Kummer, and so on, had already started their studies of algebraic numbers, mainly of cyclotomic integers, and compiled some amount of knowledges on them in their pockets. The principal motivation of them was to obtain higher power residue reciprocity laws.

E. Kummer (1810-1893) may be the first person who dared to move openly with a big stride.

◇ Divisor theory and arithmetic in cyclotomic number fields

In 1844 Kummer submitted a paper *Über die complexen Primfactoren der Zahlen, und deren Anwendung in der Kreisteilung* [Ku-1844a] to the Berlin Academy of Science. This was not published because of Kummer's request of withdrawal. The fully revised and enlarged version [Ku-1844b] was written in Latin and published in a few months; this contains a big table of data on decomposition of prime numbers up to 1000 in the cyclotomic field of the l-th root of unity for a prime l up to 23. In the first paper he erroneously stated that a prime p would be fully decomposed into a product of prime elements in $\mathbb{Q}(\zeta_l)$ if p is congruent to 1 modulo l, where ζ_l is a primitve l-th root of unity. In the table attached to the revised paper contains the smallest counter example, $l = 23$ and $p = 47$. It was Jacobi who pointed out the error in the first paper with a counter example for $l = 23$.

Kummer was, however, confident that *prime decomposition* should be uniquely done in $\mathbb{Q}(\zeta_l)$ even if it would not contain sufficiently many *prime elements*. He published an outline of his epoch-making theory in [Ku-1846b] which was republished in Journal für reine und angew. Math. as *Zur Theorie der complexen Zahlen* [Ku-1847b] together with a full scale paper [Ku-1847c] (see [We-1975, p.4, footnote]). His terminology of '*ideale complexe Zahlen*' may be misleading. What he did was to develop a divisor theory in $\mathbb{Q}(\zeta_l)$. What he needed was congruence relations modulo '*eine complex ideale Modul*'. There was a serious gap in this paper which was not realized for a while. It was finally filled almost ten years later in 1856 by the short paper [Ku-1857a] which was written up on June 5, 1856. With this indispensable result his theory was completed in the paper *Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn n eine zusammengesetzte Zahl ist* ([Ku-1856]).

◇ Fermat's Last Theorem and Bernoulli Numbers

Now Kummer picked up Fermat's Last Theorem to demonstrate the effectiveness of his divisor theory; the reason may be partly because it would not be so easy for him to get any substantial results on higher power reciprocity laws at once. Perhaps he did not think the Last Theorem itself a very serious problem in number theory if we take his words in the first letter to Dirichlet in [Ku-1847a]; he even called it 'ein Curiosum' (p.139). (This paper consists of his two letters to Dirichlet with a comment of Dirichlet on the first one.) He thought the arithmetic in cyclotomic fields he developed was much more important than the Last Theorem. In his second letter of [Ku-1847a] he analyses the ideal class number h of the cyclotomic field $\mathbb{Q}(\zeta_l)$ for an odd prime l and decomposes it into a product of the first and the second factors h_1 and h_2, respectively, where h_2 is the class number of the maximal real subfield $\mathbb{Q}(\zeta_l + \zeta_l^{-1})$. He believed that he could have showed Fermat's Last Theorem for those odd primes l which did not divide h. He also declared that l divides h if and only if l divides h_1. He states his class number formula for the first factor h_1 and from it he gives a criterion for l not to divide h_1 in terms of Bernoulli numbers $B_2, B_4, \ldots, B_{l-3}$; he believed that infinitely many prime numbers l satisfy this criterion. We now call an odd prime *regular* if it divides none of these $(l-3)/2$ Bernoulli numbers. Kummer actually showed that Fermat's Last Theorem holds for every regular prime. It is not, however, proved yet that there exist infinitely many regular primes. (K. L. Jensen [Je-1915] could prove that there exist infinitely many *irregular* primes of form $4n+3$; at the time he was a student, and then did not seem to pursue any mathematical career.) Kummer gave a precise proof for his class number formulas in [Ku-1850a] and for the criterion of the regularity in [Ku-1850b]. A full account of his results on Fermat's Last Theorem for regular primes is demonstrated in the paper [Ku-1850c]. Later in his paper [Ku-1857b] he could prove the Last Theorem also for some irregular primes. He showed in [Ku-1851b] that the prime numbers 37, 59 and 67 are the only irregular primes up to 100. Later in [Ku-1874] he showed as results of laborious calculations that 101, 103, 131, 149, 157 are consecutive irregular primes after the first three.

He also gave the following conjecture in the paper: let $\alpha(x)$ and $\beta(x)$ be the numbers of irregular primes and regular ones less than or equal to x (≥ 3), respectively; then the ratio $\nu(x) = \alpha(x)/\beta(x)$ would tend to $1/2$ as x tends to $+\infty$. Siegel [Si-1964] proposed another value in place of $1/2$ in the conjecture so that we have

Conjecture of Siegel: $\nu(x)$ would tend to $e^{1/2} - 1 = 0.648\ldots$ as x tends to $+\infty$.

◇ Higher Power Residue Reciprocity Law

In 1850 Kummer announced his prospect on the higher power residue reciprocity law for an odd prime in [Ku-1850d]; this is a letter to Dirichlet. Then a big scale paper [Ku-1852] appears; here he made an extensive study on *cyclotomic units*. The final version was published in 1859 ([Ku-1859a,b]). In 1855 he introduced a new tool, *Lagrangian Resolvents for cyclotomy*, in [Ku-1855]. In [Ku-1859b] we see his investigations in *Kummer extensions* fully demonstrated.

As we have pointed out above, he proved Fermat's Last Theorem for some irregular primes in [Ku-1857b]. He handled there such an irregular prime l for which the class number of $\mathbb{Q}(\zeta_l)$ is divisible by l but not by l^2. Therefore there exists just one unramified cyclic extension of degree l over $\mathbb{Q}(\zeta_l)$ by class field theory. It is realized as a Kummer extension $\mathbb{Q}(\zeta_l, \sqrt[l]{e})$ with some unit e in $\mathbb{Q}(\zeta_l)$ as Weil pointed out in [We-1975]. This is the background where Kronecker started his career as a number theorist.

7. Algebraic Numbers — From Divisor Theories to Class Field Theory

In this chapter we pick up mainly four mathematicians, L. Kronecker, R. Dedekind, H. Weber and E. I. Zolotareff. For a historical study on the process of the establishment of the Takagi-Artin Class Field Theory interested readers are suggested to see [Mi-1994] for example.

7.1 L. Kronecker (1823-1891)

The mathematical style of Kronecker seems very singular. It is true that he discovered at least a few profound arithmetic phenomena and could bravely formulate big research projects from them. T. Takagi once called Kronecker a prophet ([Ta-1948], footnote, p.261); he made a comment related to Tschebotareff's Density Theorem, "His speculation has turned out well here again.", and chose the terminology 'Kronecker density'.

◇ Abelian polynomials over $\mathbb{Q}$

In 1853 Kronecker stated the following proposition in [Kr-1853]:

Kronecker-Weber Theorem: Roots of every Abelian polynomial with rational integer coefficients are expressed as a rational function of a root of unity.

Here he means by an Abelian polynomial the one with a cyclic Galois group. Later in [Kr-1877] he extends it to mean the one with an Abelian Galois group. As for the proof of the theorem, H. Weber made a certain contribution in [Wb-1886]. The basic tool of both authors for their trials to prove it was Lagrangian resolvents. Both of them, however, could not give a complete proof. An error in Weber's paper did not seem to be realized for a while. He could finally give a complete proof of his own in [Wb-1909].(II). The first complete proof of the theorem was given by D. Hilbert in [Hi-1896]. Olaf Neumann gave a clear and detailed explanation on the errors in the proofs based on Lagrangian resolvents in [Ne-1981].

It must be noted that Kronecker mentions a generalization of the theorem at the end of [Kr-1853]; namely, roots of an Abelian polynomial with coefficients in the Gaussian ring $\mathbb{Z}[\sqrt{-1}]$ may be similarly treated with the division of the lemniscate. He also indicates further generalization. It is probable that, at the time, he had already studied elliptic functions with complex multiplication to some extent through Abel's works. Kronecker's dream in his youth must have appeared in these days. His words, " ... um meinen liebsten Jugendtraum ... ", appear in his letter [Kr-1880b] to Dedekind written in 1880.

◇ Elliptic functions with complex multiplication

In 1857 he published the paper *Über die elliptischen Functionen, für welche complexe Multiplication stattfindet* [Kr-1857a] on arithmetic of elliptic functions with complex multiplication. He also wrote a letter [Kr-1857b] to Dirichlet about his findings. Though the statements of the letter are not mathematically exact, we can vividly look over what he had found:

Let $\mathbb{Q}(\sqrt{-D})$, $D > 0$, be an imaginary quadratic number field. Let k be the singular modulus (in the sense of Kronecker) of an elliptic function which has complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-D})$, and H be the class number of binary quadratic forms over $\mathbb{Z}$ with discriminant $-D$ (the class number of $\mathbb{Q}(\sqrt{-D})$). His findings are as follows:

(1) the singular modulus k is a root of a polynomial of degree H (in [Kr-1857a] he gives the correct value $6H$) over $\mathbb{Q}(\sqrt{-D})$ which is algebraically solvable;

(2) the polynomial has the property which Abel treated: namely, when any one of the roots is chosen, every other root can be expressed as a rational function of it, and the Galois group is commutative;

(3) H values of singular moduli k respectively correspond to the H equivalence classes of the binary quadratic forms with discriminant $-D$;

(4) a certain rational function of the irrational number k may be regarded as the ideal complex number corresponding to each class of quadratic forms; etc. (For these statements we should take j-invariants instead of k.)

In the paper [Kr-1862] he investigated the different of the Abelian polynomial. We know that the Abelian extension $\mathbb{Q}(\sqrt{-D}, j)/\mathbb{Q}(\sqrt{-D})$ is unramified, and, corresponding to (4), we have

The Principal Ideal Theorem: Every ideal of an algebraic number field of finite degree is realized by an irrational number (i.e. becomes a principal ideal) in the maximal unramified Abelian extension field.

Kronecker formulated this theorem as 'die Frage der zu associirenden Gattungen' in [Kr-1882a]. After the Takagi-Artin class field theory was established, it was finally proved in 1930 by Ph. Furtwängler [Fw-1930] by making use of the general reciprocity law of E. Artin [Ar-1927,-1930]. (See [Mi-1988] for further developments on the subject including a historical overview.)

We state here Kronecker's dream in his youth. This is not mathematically precise. For a detailed mathematical discussion about it, we refer to Zusatz 35 of [Kr-1895, pp.510-515] written by H. Hasse.

Kronecker's Dream in his Youth: All Abelian extensions of an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ are obtained by adjoining the j-invariant of an elliptic function with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-D})$ and the values of the elliptic function at division points of the periods.

This research problem seems the principal motivation of not only H. Weber but also T. Takagi for their works on class fields. Takagi first proved Kronecker's Dream for the Gaussian field $\mathbb{Q}(\sqrt{-1})$ in his doctoral thesis [Ta-1903]. Then he finally gave a complete proof in [Ta-1920] with his class field theory after an important contribution by R. Fueter [Ft-1914]. (For a historical study of class field theory, see [Mi-1994].)

◇ Divisor theory for algebraic number fields

Kronecker had a strong opinion on Kummer's theory of 'ideale complexe Zahlen'; he thought that an important concept like 'ideale complexe Zahlen' must be given a clear mathematical description. He seemed to have his divisor theory for algebraic number fields of finite degree around 1857 if we adopt Kummer's testimony in [Ku-1859b], p.57. He published it in [Kr-1882a] later in 1882. In this paper he also formulated the Principal Ideal Theorem as we mentioned above. He uses (indefinitely) many independent variables for his theory.

Let $\tilde{\mathbb{Q}}$ be the rational function field $\mathbb{Q}(X, Y, Z, \dots)$ in independent variables X, Y, $Z, \dots$ with coefficients in $\mathbb{Q}$. We call a polynomial in $\tilde{\mathbb{Q}}$ an integral element if its coefficients are integers, and a primitive one if the g.c.d. of the coefficients is equal to 1. An element f of $\tilde{\mathbb{Q}}$ is expressed in the form

$$f = r \cdot (E_1(X, Y, Z, \dots)/E_2(X, Y, Z, \dots))$$

with $r \in \mathbb{Q}$, $r > 0$, and primitive integral elements E_1 and $E_2 \in \tilde{\mathbb{Q}}$; it is clear that the rational number r is uniquely determined by f and called the number factor of f. We also call f an *integral element* if $r \in \mathbb{Z}$ to widen the concept. Then we can introduce division among integral elements in a natural way. A divisor of 1 is a unit. An element of $\tilde{\mathbb{Q}}$ is a unit if and only if its number factor is equal to 1; hence there are many units, indeed.

Now let K be an algebraic number field of finite degree and $\tilde{K}$ be the rational function field $K(X, Y, Z, \dots)$. An element of $\tilde{K}$ is an integral element if it is a root of a monic polynomial whose coefficients are integral elements of $\tilde{\mathbb{Q}}$. Then we are able to define a unit, a prime element, etc., of $\tilde{K}$ in a natural manner. Note that there are plenty of units in $\tilde{K}$. We can also define a g.c.d. of a finite number of integral elements of $\tilde{K}$ though it is only determined up to units. Then we have

Theorem: For a finite number of integral elements of $\tilde{K}$, there exists a g.c.d. of them in $\tilde{K}$.

An algebraic integer in K is an integral element of $\tilde{K}$. It is, therefore, decomposed into a product of prime elements of $\tilde{K}$ uniquely up to units.

As for the relation with the ideal theory of Dedekind, let $\alpha_1, \alpha_2, \dots,$ α_n be algebraic integers in K, and $X_1, X_2, \dots, X_n$ be independent variables in $\tilde{K}$. Then

$$\varphi := \alpha_1 X_1 + \alpha_2 X_2 + \dots + \alpha_n X_n \in \tilde{K}$$

is a g.c.d. of $\alpha_1, \alpha_2, \dots, \alpha_n$ in $\tilde{K}$. Hence the ideal (in the sense of Dedekind) of K

$$(\alpha_1,\ \alpha_2, \dots,\ \alpha_n)$$

which is generated by $\alpha_1, \alpha_2, \dots, \alpha_n$ corresponds to φ as a g.c.d. of $\alpha_1, \alpha_2, \dots, \alpha_n$.

◇ Kronecker's density of primes

In 1880 Kronecker [Kr-1880a] introduced a kind of density of a set of (rational) prime numbers in connection with a polynomial.

Let $F(x)$ be a polynomial with integer coefficients. For a prime p, let ν_p be the number of roots of the equation $F(x) \equiv 0 \mod p$ in the finite field $\mathbb{Z}/p\mathbb{Z}$; here we count the multiplicity, of course. Then Kronecker states

Theorem: The notation being as above, the limit of the value of the series

$$\sum_{p,\ prime} \nu_p \cdot p^{-1-w}$$

as the positive w tends to 0 is proportional to the value of $\log(1/w)$ and coincides with $\log(1/w)$ multiplied by the number of irreducible factors of $F(x)$.

For each integer k, $0 \leq k \leq n := \deg F$, let us denote those primes p for which the equation $F(x) \equiv 0 \mod p$ has just k roots by p_k. Then the series become

$$\sum_{k=0}^{n} k \cdot \sum p_k^{-1-w}.$$

Assume now that the limit

$$D_k := \lim_{w \to 0+} \frac{\sum p_k^{-1-w}}{\log(1/w)} = \lim_{w \to 0+} \frac{\sum p_k^{-1-w}}{\sum p^{-1-w}}$$

exists. Then by the theorem we have

$$\sum_{k=0}^{n} k \cdot D_k = 1$$

if $F(x)$ is irreducible. This formula was so attractive that G. Frobenius finally formulated a conjecture out of it in [Fr-1896a] by means of the Galois group of the polynomial $F(x)$ and Frobenius automorphisms. N. Tschebotareff [Ts-1926] proved it in 1926; hence it is now called Tschebotareff's Density Theorem. His proof was well analyzed by O. Schreier [Sc-1927] and supplied an essential method for E. Artin to prove his General Reciprocity Law in 1927 ([Ar-1927]).

7.2 R. Dedekind (1831-1916)

There are two well known contributions of Dedekind to algebraic number theory, Theory of Ideals and Dedekind's Zeta Function. It is, however, probable that his direct and indirect influences on Frobenius, H. Weber and E. Artin do not seem to be well recognized. If we closely study his works on number theory, we find a typical model of interactions between algebraic number theory and analytic number theory.

◇ Basis of Algebraic Number Theory

His theory of ideals first appears in 1871 as Supplement X *Über die Komposition der binären quadratischen Formen* to the second edition of Dirichlet's book of number theory, *Vorlesungen über Zahlentheorie* ([De-1871]). Then his theory of algebraic numbers grew well step by step in his three works [De-1877a,-1879,-1893], and became a basic standard. His terminology and even some from his notation are still commonly used.

On the contrary, for example, we now see few of Kronecker's (except 'Abelian polynomials' or 'Abelian extensions' and 'complex multiplication').

In 1900 he published a paper [De-1900] on pure cubic fields; its title is *Über die Anzahl der Ideal-Klassen in reinen kubischen Zahlkörpern.* In the introduction he says that this is a revised version of what he prepared in nearly two years, 1871 and 1872. It seems apparent to me that his primary motivation toward algebraic number theory is to generalize Dirichlet's class number formula for a quadratic number field to that for a pure cubic field.

The first thing he had to do for this purpose is to develop a good divisor theory at least for a pure cubic field. Since it is not contained in any cyclotomic field, he could not directly use Kummer's theory of 'ideale complexe Zahlen', and so gently modified Kummer's 'ideale complexe Modul'. He did not need any ideal or imaginary objects because he was ready to introduce infinite sets as concrete mathematical objects. His Supplement X [De-1871] consists of five sections:

§159. Endlich Körper,
§160. Ganze Algebraische Zahlen,
§161. Theorie der Moduln,
§162. Ganze Zahlen eines endlichen Körpers,
§163. Theorie der Ideale eines endlichen Körpers.

After he introduces an algebraic number field K of finite degree and algebraic integers in the first two sections, he presents a 'Modul' to support congruence relation in K as an additive subgroup of K. The word 'Modul' must have been taken on account of 'modulus' of Gauss and 'ideale complexe Modul' of Kummer. For a finitely generated $\mathbb{Z}$-submodule M of K of the maximal rank, an order $\mathfrak{o}_M$ is defined as

$$\mathfrak{o}_M = \{a \in K \mid a \cdot M \subset M\}.$$

Since M is finitely generated over $\mathbb{Z}$, every element of $\mathfrak{o}_M$ is an algebraic integer. Hence $\mathfrak{o}_M$ is contained in *the maximal order* $\mathfrak{o}$ which is the ring of all the integers in K. Dedekind could observe examples of such structures in imaginary quadratic fields through complex multiplication of elliptic functions (see Section 7.3 below). In the final section he develops his divisor theory with those modules whose orders coincide with the maximal $\mathfrak{o}$.

◇ From Dedekind's Zeta Functions to Artin's L-functions

His next target was to define a zeta function $\zeta_K(s)$ for an algebraic number field K, and calculate its residue at $s = 1$ or, more precisely, the value $S = \lim_{s \to 1+}(s-1)\zeta_K(s)$. This was done in [De-1877b]. He could express the limit value by the class number, the discriminant and the regulator. Here he also handled the class numbers of non-maximal orders.

To obtain a class number formula like Dirichlet's one, he had to decompose $\zeta_K(s)$ as a product of Riemann's zeta function and some suitable L-functions. To define suitable L-functions, he needs 'characters' with orthogonal relations. This was not an easy task for him. He was, however, lucky enough to find Frobenius. Encouraged by Dedekind, Frobenius succeeded in establishing the desired theory of group characters for finite groups in [Fr-1896b]. (Cf. also Th. Hawkins [Hk-1970,-1974], and [Mi-1989].) However, neither Dedekind nor Frobenius defined L-functions with the group characters even though the latter formulated Frobenius' conjecture in [Fr-1896a]. The task was left to Artin [Ar-1923,-1924b].

In 1923 E. Artin (1898-1962) published his paper [Ar-1923] under the influence of Dedekind [De-1900]. The theme was to express the quotient $\zeta_K(s)/\zeta_k(s)$ of Dedekind's zeta functions for a finite meta-cyclic extension K/k of algebraic number fields in terms of L-functions. He must have been much encouraged by Takagi [Ta-1920]. In case of an Abelian extension, K is characterized as a congruence class field of k by Takagi's class field theory. Hence (modified) Weber's L-functions with characters of the corresponding congruence ideal class group give a perfect answer. (Weber did not consider congruence relations by archimedian primes. They were first introduced by Hilbert in his theory of relative quadratic extensions [Hi-1899]; the main theme of the paper is to show the quadratic reciprocity law in an arbitrary algebraic number field.) In 1924 Artin gave his L-functions for an arbitrary Galois extension with his conjectural general reciprocity law in [Ar-1924b]. Then he could give its proof in [Ar-1927] to complete the Takagi-Artin class field theory as we mentioned above at the end of Section 7.1.

◇ Rational Function Fields over finite fields

It may be of some interest to note Dedekind's influence on 'analytic theory' of arithmetic in function fields of one variable over a finite field.

Dedekind published a paper on the polynomial ring over a finite field in 1857 ([De-1857]). He presented here a divisor theory in the ring. It is apparent that Gauss [G-1801*] gave a direct motivation to him. The article of Gauss was posthumously published in his collected works [G-1863].II in 1863 as was mentioned in Section 4.1 above. Dedekind attached a note to it which he referred in a footnote of [De-1857]. In the article Gauss had already discussed roots of a polynomial over a finite prime field $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number, by utilizing the p-th power map. (It was Galois who first (posthumously) published a paper on finite algebraic extensions of a finite prime field $\mathbb{Z}/p\mathbb{Z}$ together with the

p-th power map in [Gal-1846]. He could not see Gauss [G-1801*] which was not yet published at the time when he prepared his paper.) Meanwhile Dedekind treated the polynomial ring *analogously* with the ring of rational integers as he clearly stated. He obtains a finite extension of the prime field by a congruence relation modulo a prime polynomial (eine (irreductibel Function order) Primfunction) and generalize Fermat's theorem. He shows, moreover, 'the quadratic reciprocity law' for the ring by means of quadratic extensions.

After 62 years later H. Kornblum [Ko-1919] picked up the polynomial ring and proved an analogue of Dirichlet's Prime Number Theorem in Arithmetic Progressions.

Then in his thesis [Ar-1924a] Artin investigated the arithmetic of quadratic extensions of the rational function field of one variable over a finite field, and for the congruence zeta functions showed the analogue of the functional equation of Riemann's zeta function, and introduced the analogue of Riemann's hypothesis.

7.3 H. Weber (1842-1913)

At the international conference on class field theory[2] held at Tokyo in 1998, P. Roquette stated that Germany was the father of class field theory and Japan the mother. H. Weber and D. Hilbert may be most paternal because both of them independently began to use the word 'class field' in different contexts ([Wb-1891] and [Hi-1897]).

Hilbert introduced the word in relation to his Theorem 94 which he thought as the first step toward the Principal Ideal Theorem.

Weber did it in his investigation on 'Kronecker's dream in his youth' which was his principal interest. He extended his concept of class fields finally to cover those Abelian extensions of an imaginary quadratic field which are constructed by the singular moduli and the values at division points of the periods of elliptic functions with complex multiplication by the base quadratic field; in [Wb-1908] he defined a class field of an imaginary quadratic field as an Abelian extension which 'canonically' corresponds to a congruence ideal class group of the base field. He was eager to determine Abelian extensions of imaginary quadratic fields generated by the special values, but not so much to see class field theory in general algebraic number fields even though he introduced congruence ideal class groups and his L-functions to show one of the two fundamental inequalities in general algebraic number fields ([Wb-1897]).

[2]The Proceedings: Class Field Theory – its Centenary and Prospect, ed. K. Miyake, Advanced Studies in Pure Math. 30, Math. Soc. Japan, Tokyo, 2001. This contains a paper of H. Suzuki which gives a most general form of the Principal Ideal Theorem.

◇ Weber and Number Theory

When he started his career as a mathematician Weber worked in some area of analysis related to partial differential equations and mathematical physics. He was also interested in Abelian functions and Abelian integrals from an analytical point of view associated, e.g., with the Dirichlet Principle. Meanwhile these Abelian functions gave him a chance to get an acquaintance with Dedekind. The latter was trying to publish the works on Abelian functions of the late colleague B. Riemann at Göttingen; Riemann died in 1866. He asked Clebsch to help him who, however, died soon in 1872. Then he decided to invite Weber for the help. Their cooperation produced the first edition of Riemann's Collected Works in 1876. (Cf. Aurel Voss [Vo-1914] and Frei [Fre-1989].) Then in 1882 they published the big work [DW-1882] on the theory of algebraic functions. Here we see clearly an analogy between algebraic number fields and algebraic function fields. For example, 'ideale Theiler' and 'Modul' were introduced in the theory. In 1882 Weber also published his first paper of number theory, *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darstellen* ([Wb-1882]); as the title shows, this is a quadratic version of Dirichlet's Prime Number Theorem. In the introduction Weber also mentioned Kronecker's papers [Kr-1857a] and [Kr-1880a]; the former is on elliptic functions with complex multiplication and the latter on the densities of sets of primes determined by congruence properties of a polynomial which also attracted Frobenius (see Section 7.1).

◇ Kronecker-Weber Theorem

In 1886 Weber published a colossal work [Wb-1886] in two parts to prove the Kronecker-Weber Theorem. As it was noted in Section 7.1, this contains a gap though it did not seem to be immediately realized. The theorem itself was, however, soon given a new proof by Hilbert [Hi-1896]; his approach, based on Minkowski's result in the Geometry of Numbers ([M-1896]), was quite new with his theory of ramification of ideals ([Hi-1894]). Weber published another paper [Wb-1909].(I) on the theorem later in 1909. Perhaps, he was stimulated by Mertens [Me-1906]. Both of them, however, contain errors. As for Weber's paper, Frobenius pointed out two errors. Then in 1911 Weber published his corrected and first perfect proof of the Kronecker-Weber Theorem in [Wb-1909].(II). For the details on the history of the theorem and a complete proof based on Lagrangian Resolvents the reader should see the interesting paper [Ne-1981] of Olaf Neumann.

◇ Congruence ideal class groups and Weber's L-functions

As we have pointed out a few times, Weber eagerly investigated extension fields of an imaginary quadratic field constructed with the singular moduli and the values at division points of an elliptic function which has complex multiplication with numbers of the base field. Through them he exstracted the concept of congruence ideal class groups and developed his analytic theory with his L-functions in an arbitrary algebraic number field in his paper [Wb-1897].

Here we explain how a congruence ideal class group comes out from division points of periods of such an elliptic function. For the sake of simplicity, we do not adhere to historical context.

Let $\varphi = \varphi(z)$ be an elliptic function; it is a meromorphic function on the complex plane $\mathbb{C}$ with two independent periods ω_1, ω_2 over $\mathbb{R}$; $\varphi(z) = \varphi(z+\omega_1) = \varphi(z+\omega_2)$, ω_1, $\omega_2 \in \mathbb{C}^\times$, $\omega_2 \notin \mathbb{R}\omega_1$. Then we have $\varphi(z) = \varphi(z+\omega)$ for each element ω of

$$\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{m\omega_1 + n\omega_2 \mid m,\ n \in \mathbb{Z}\}.$$

We may assume that the imaginary part $\mathrm{Im}(\tau)$ is positive for $\tau = \omega_1/\omega_2$ by changing ω_1 and ω_2 if necessary. If an elliptic function is not a constant, all of its periods are given as a $\mathbb{Z}$-module $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with a suitable pair ω_1 and ω_2.

Conversely, for such a pair ω_1 and ω_2, there exist those elliptic functions the set of periods of which coincides with the module $\Omega := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$; for example, the Weierstrass $\wp$-function $\wp(z) = \wp(\omega_1, \omega_2; z)$ and its derivative $\wp'(z)$ are such.

The set of all elliptic funcions that admit Ω as their periods (including constant functions) form an algebraic function field $\mathfrak{K}_\Omega$; if we take $x := \wp(z)$ and $y := \wp'(z)$, then we have $\mathfrak{K}_\Omega = \mathbb{C}(x, y)$ with the relation $y^2 = 4x^3 - g_2 x - g_3$. The discriminant $g_2^3 - 27g_3^2$ of the cubic polynomial is not equal to 0. Put $j = g_2^3/(g_2^3 - 27g_3^2)$. Then both of the numerator and the denominator are homogeneous functions of ω_1 and ω_2 of the same degree. Therefore, this may be considered as a function of $\tau = \omega_1/\omega_2$: $j = j(\tau)$, $\mathrm{Im}(\tau) > 0$. For another $\Omega' = \mathbb{Z}\omega_1' + \mathbb{Z}\omega_2'$, $\tau' = \omega_1'/\omega_2'$, two function fields $\mathfrak{K}_\Omega$ and $\mathfrak{K}_{\Omega'}$ are isomorphic over $\mathbb{C}$ if and only if $j(\tau) = j(\tau')$. The fields $\mathfrak{K}_{\Omega'}$ and $\mathfrak{K}_\Omega$ are naturally identified with the fields of all meromorphic functions on the complex tori $\mathbb{C}/\Omega'$ and $\mathbb{C}/\Omega$, respectively. Therefore, an isomorphism of the two fields corresponds to an isomorphism of these two complex tori $f : \mathbb{C}/\Omega \to \mathbb{C}/\Omega'$. Combining f with the translation on $\mathbb{C}/\Omega'$ by $-f(0)$, we may assume $f(0) = 0$. Then, as is well known, this isomorphism f is induced from the multiplication by $\alpha \in \mathbb{C}$ on $\mathbb{C}$; α must satisfy the condition $\alpha\Omega = \Omega'$. In other words, an isomorphism of the algebraic function fields $\mathfrak{K}_{\Omega'}$ and $\mathfrak{K}_\Omega$ is essentially obtained by the variable change from z to αz. If we take $\alpha = \omega_2^{-1}$ then the periods ω_1 and ω_2 are changed to 1 and τ respectively.

Let us take $\Omega = \mathbb{Z} + \mathbb{Z}\tau$. For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, put $A(\tau) = (a\tau + b)/(c\tau + d)$. Since A induces just a basis change on Ω, we have $j(A(\tau)) = j(\tau)$ by the isomorphism invariant property of j explained above.

If Ω' is a submodule of Ω, then the complex torus $\mathbb{C}/\Omega'$ is a Galois covering of $\mathbb{C}/\Omega$ with the covering group Ω/Ω'; and hence $\mathfrak{R}_{\Omega'}/\mathfrak{R}_\Omega$ is an algebraic extension of finite degree.

Suppose now that an elliptic function $\varphi(z)$ with the periods Ω has complex multiplication by $\mu \in \mathbb{C} - \mathbb{R}$. This means that two elliptic functions $\varphi(z)$ and $\varphi(\mu z)$ have an algebraic relation; in other words, we may say that the periods Ω and $\mu^{-1}\Omega$ are commensurable, i.e. that the intersection of the two modules has finite indices in both of Ω and $\mu^{-1}\Omega$. Hence we can find a positive integer N such as $N\Omega \subset \mu^{-1}\Omega$, and then we have $(\mu N)\Omega \subset \Omega$. For simplicity we may consider the case of $\mu\Omega \subset \Omega$. Then there is $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$ with $a,\ b,\ c,\ d \in \mathbb{Z}$ so that we have $\mu \begin{pmatrix} \tau \\ 1 \end{pmatrix} = A \begin{pmatrix} \tau \\ 1 \end{pmatrix}$. Hence μ is an eigenvalue of A, and is an algebraic integer in the quadratic field $\mathbb{Q}(\mu)$. We easily see $\mathbb{Q}(\mu) = \mathbb{Q}(\tau)$, and that it is an imaginary quadratic field. Thus we have a 'Modul' Ω in $k := \mathbb{Q}(\mu) = \mathbb{Q}(\tau)$ and a fractional ideal Ω of the order $\mathfrak{o}_\Omega$. It is now clear that two fractional ideals Ω and Ω' of the same order $\mathfrak{o}' := \mathfrak{o}_\Omega = \mathfrak{o}_{\Omega'}$ give isomorphic elliptic function fields $\mathfrak{R}_\Omega$ and $\mathfrak{R}_{\Omega'}$ if and only if there exists an element $\alpha \in k$ with the property $\alpha\Omega = \Omega'$. Here we have the ideal class group of an oder $\mathfrak{o}'$ of the imaginary quadratic field k. For the maximal oder $\mathfrak{o}$ of k we have the following theorem:

Theorem: Let k be an imaginary quadratic field and $\mathrm{Cl}(k)$ be the (absolute) ideal class group of k. Each class of $\mathrm{Cl}(k)$ corresponds to an isomorphism class of elliptic function fields among whose modules of periods we can choose an ideal $\mathfrak{w} = \mathbb{Z} + \mathbb{Z}\tau$, $\mathrm{Im}(\tau) > 0$, from the ideal class as is explained above. Then the extension $k(j(\tau))/k$ is Abelian and unramified, and the Galois group is isomorphic to $\mathrm{Cl}(k)$. Every ideal of k becomes a principal one if it is lifted to the ideal of $k(j(\tau))$.

All of the contents of the theorem were finally proved by Weber in [Wb-1908].

Weber further considered the field obtained by adjoining the values of elliptic functions at division points of the periods. Let d be a positive integer. Then the d-th division points of the periods are given by the set $d^{-1}\mathfrak{w}/\mathfrak{w}$ on the complex torus $\mathbb{C}/\mathfrak{w}$. Let $\varphi(z)$ be an elliptic function whose period module is $\mathfrak{w}$, and α an element of $k^\times$. We have $\varphi(\alpha d^{-1}\omega) = \varphi(d^{-1}\omega)$ for every $\omega \in \mathfrak{w}$ if and only if $\alpha d^{-1}\omega \equiv d^{-1}\omega \mod \mathfrak{w}$ for every $\omega \in \mathfrak{w}$; that is, α acts trivially on $d^{-1}\mathfrak{w}/\mathfrak{w}$. In other words, we have

$$(\alpha - 1)d^{-1}\omega \equiv 0 \mod \mathfrak{w} \quad \text{for every } \omega \in \mathfrak{w}$$

and hence $(\alpha-1)d^{-1}\mathfrak{w} \subset \mathfrak{w}$. Multiplying both sides by the ideal $d\mathfrak{w}^{-1}$, we finally have the condition

$$\alpha \equiv 1 \mod d\mathfrak{o}.$$

If we replace d by an integral ideal $\mathfrak{m}$ and consider $\mathfrak{m}$-th division points $\mathfrak{m}^{-1}\mathfrak{w}/\mathfrak{w}$, then we have a condition

$$\alpha \equiv 1 \mod \mathfrak{m}$$

on $\alpha \in k^\times$. The multiplicative subgroup $\{\alpha \in k^\times \mid \alpha \equiv 1 \mod \mathfrak{m}\}$ of $k^\times$ is the Strahl or the ray (in English) modulo $\mathfrak{m}$. Thus we have the *congruence ideal class group* $A(\mathfrak{m})/S(\mathfrak{m})$ modulo $\mathfrak{m}$ where $A(\mathfrak{m})$ is the multiplicative group of those ideals which are relatively prime to $\mathfrak{m}$ and $S(\mathfrak{m})$ is the group of principal ideals coming from the Strahl:

$$S(\mathfrak{m}) = \{(\alpha) \mid \alpha \in k^\times,\ \alpha \equiv 1 \mod \mathfrak{m}\}.$$

In [Wb-1897] Weber introduced congruence ideal class groups of the form $A(\mathfrak{m})/H(\mathfrak{m})$ where $H(\mathfrak{m})$ is an intermediate group of $A(\mathfrak{m}) \supset S(\mathfrak{m})$ in an arbitrary algebraic number field K of finite degree as well as his L-functions

$$L(s;\chi) = \sum_{C\in A(\mathfrak{m})/H(\mathfrak{m})} \chi(C)\zeta(s;C) = {\sum_{\mathfrak{a}\in A(\mathfrak{m})}}' \frac{\chi(\mathfrak{a})}{N_{K/\mathbb{Q}}(\mathfrak{a})^s}$$

through the partial zeta-functions

$$\zeta(s;C) = {\sum_{\mathfrak{a}\in C}}' \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{a})^s}$$

where C is a class in $A(\mathfrak{m})/H(\mathfrak{m})$, $\sum'$ is the summation over integral ideals and χ is a character of the abelian group $A(\mathfrak{m})/H(\mathfrak{m})$.

By the time of his article [Wb-1900], he had proved that the extension

$$k(j(\tau), \varphi(u) \mid u \in \mathfrak{m}^{-1}\mathfrak{w})/k(j(\tau))$$

is Abelian with the Galois group isomorphic to $\mathfrak{m}^{-1}\mathfrak{w}/\mathfrak{w}$. In [Wb-1908] he was able to show finally that the field $k(j(\tau), \varphi(u) \mid u \in \mathfrak{m}^{-1}\mathfrak{w})$ is Abelian over the base quadratic field k with the Galois group isomorphic to $A(\mathfrak{m})/S(\mathfrak{m})$. Then he decisively called all of these fields *class fields* of k.

Hilbert introduced sign distribution at Archimedian primes in his paper [Hi-1899] to handle quadratic extensions over an arbitrary algebraic number field and show the quadratic reciprocity law in the most general framework. Then Takagi used congruence ideal class groups for modulus including Archimedian primes to establish his class field theory in [Ta-1915,-1920].

Once the existence of the class field M/K for each congruence ideal class group $A(\mathfrak{m})/H(\mathfrak{m})$ is assured by Takagi, then Weber's L-functions supply a natural decomposition of the quotient of the Dedekind zeta functions,

$$\zeta_M(s)/\zeta_K(s) = \prod_{\chi} L(s;\chi),$$

where $\prod_\chi$ is the product over all non-trivial characters of the Abelian group $A(\mathfrak{m})/H(\mathfrak{m})$. These examples stimulated Artin to define his L-functions in [Ar-1924b] as was noted in the previous Section.

7.4 E. I. Zolotareff (1847-1878)

In this final section of the present article, we see the motivation of Zolotareff who also developed a divisor theory in an algebraic number field. Although his work is not directly related to our main purpose of this article, it may be of some interest to look into the St. Petersburg school of number theory where Tschebotareff soon came to make a big contribution toward Artin's proof of his general reciprocity law.

P. L. Tchebychef was probably the most influential Russian mathematician who raised the modern school of number theory at St. Petersburg. We have mentioned his works [Tc-1849,-1852] on distribution of prime numbers in Section 2.2. Beside them he published several papers on continued fraction expansions. And he came across Abel's paper [Ab-1826]; here Abel gave a criterion by which one can determine whether hyperelliptic integrals be expressed by logarithm functions and which depends on periodicity of the continued fraction expansions of the square roots in the integrals (cf. Section 4.2). In his paper [Tc-1861] he dealt with the elliptic case $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}}dx$ with *rational numbers* α, β, γ, δ, and gave an *effective* criterion for the case. Since Abel's criterion says that the expansion is to be periodic in a specific form, it so happened that there cannot exist any effective bounds of the periods for all of hyperelliptic integrals of the kind. Here is the point of Tchebychef's criterion; and he had to restrict himself to rational coefficients. In this case one can assume without losing generality that the coefficients are rational integers. The basic tool is Jacobi transformations. Then the integrability by logarithms is reduced to a kind of Diophantine problems which have only a finite number of solutions. In the process one cannot dispense with the Fundamental Theorem of Arithmetic. He states as one of examples that the integral function of $\frac{x+A}{\sqrt{x^4+5x^3+3x^2-x}}dx$ cannot be expressed by logarithm functions for any values of A. He did not, however, give any proofs nor brief explanations in the paper. Then Zolotareff published a detailed proof of Tchebychef's criterion in [Zo-1874].

In his paper [Zo-1880] of his divisor theory in algebraic number fields (which was posthumously published), Zolotareff says that he tried to generalize Kummer's theory to extend Tchebychef's method for any real coefficients (des valeurs réelles quelconques). He even states, after referring to Selling [Se-1865] and Dedekind [De-1871], that there have not been any theories yet which matches Kummer's. (E. Selling [Se-1865] contains a serious error.) It appears that he faithfully followed Kummer's way. To utilize it to his concrete problems, he found it best. Here he means real *algebraic* numbers by 'des valeurs réelles quelconques'. We may safely suppose that he would have liked to handle much wider integrals at least including Abel's example

$$\int \frac{\left(x+\frac{\sqrt{5}+1}{14}\right)dx}{\sqrt{\left(x^2+\frac{\sqrt{5}-1}{2}\right)^2+\left(\sqrt{5}-1\right)^2 x}}$$

with Tchebychef's method.

Zolotareff, as a young hope of Tchebychef's school at the time, obtained his degree in 1874 and was selected to be a member of St. Petersburg Academy of Science in 1876. It is probable that he was the first number theorist in the school who worked on algebraic numbers. It is, however, regrettable to say that he passed away at the age of 31 in 1878 because of blood poisoning caused by a car accident; cf. A. N. Kolmogorov and A. P. Yushkevich [KY-1992].

References

[Ab-1824] N. H. Abel. Mémoire sur les équations algébriques oú l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré, Brochure imprimée chez Grondahl, Christiania, 1824; Œuvres complètes I, 28-33.

[Ab-1826] ______. Sur l'intégration de la formule différentielle $\frac{\rho dx}{\sqrt{R}}$, R et ρ étant des fonctions entières, Jour. reine angew. Math. 1 (1826), 185-221; Œuvres complètes I, 104-144.

[Ab-1827] ______. Recherches sur les fonctions elliptiques, Jour. reine angew. Math. 2 (1827), 101-181, 3 (1828), 160-190; Œuvres complètes I, 263-388.

[Ab-1881] ______. Œuvres complètes I, II; Christiania, 1881; Reprint from Johnson Reprint, New York, 1965.

[Ab-1902] ______. Mémorial publié à l'occasion du centenaire de sa naissance, Christiania, 1902.

[dA-1746] J. le Rond d'Alembert. Réflexions sur la cause générale des vents, Mémoires de l'Académie des Sciences et Belles Lettres de Berlin, 1747.

[Ar-1923] E. Artin. Über die Zetafunktionen gewisser algebraischer Zahlkörper, Math. Ann. 89 (1923), 147-156; Collected Papers, 95-104.

[Ar-1924a] ______. Quadratische Körper im Gebiete der höheren Kongruenzen I, II, Math. Zeitschrift 19 (1924), 153-246; Collected Papers, 1-94.

[Ar-1924b] ______. Über eine neue Art von L-Reihen, Abh. Math. Sem. Univ. Hamburg, 3 (1924), 89-108; Collected Papers, 105-124.

[Ar-1927] ______. Beweis des allgemeinen Reziprozitätsgesetzes, Abh. Math. Sem. Univ. Hamburg, 5 (1927), 353-363; Collected Papers, 131-141.

[Ar-1930] ______. Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz, Abh. Math. Sem. Univ. Hamburg, 7 (1930), 46-51; Collected Papers, 159-164.

[Ar-1931] ______. Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren, Abh. Math. Sem. Univ. Hamburg, 8 (1931), 292-306; Collected Papers, 165-179.

[Ar-1965] ______. The Collected Papers, Addison Wesley, 1965.

[Bo-1572] Rafael Bombelli. L'Algebra, Opera di Rafael Bombelli da Bolognia, divisa in tre libri, per Giovanni Rossi, Bolognia, 1572.

[Ca-1545] Girolamo Cardano. Artis Magnæ Sive de Regulis Algebraicis. Lib. unus. Qui & totius operis de Arithmetica, quod OPUS PERFECTUM inscripsit, est in ordine Decimus, 1545.

[Ca-1968] ______. The Great Art or The Rules of Algebra, trasl. and ed. by T. Richard Witmer, The M.I.T. Press, Cambridge, Massachusetts and London, England, 1968.

[Co-1989] David A. Cox. Primes of the Form $x^2 + ny^2$ — Fermat, Class Field Theory, and Complex Multiplication, John Wiley & Sons, Inc., New York, 1989.

[De-1857] R. Dedekind. Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus, Jour. reine angew. Math., Bd.54 (1857), 1-26; Werke I, 40-66.

[De-1871] ______. Supplement X. Über die Komposition der binären quadratischen Formen, von Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet (2. Auflage), 423-462, (1871); Werke III, 223-261.

[De-1877a] ______. Sur la théorie des nombres entiers algébriques, Paris, Gauthier-Villars, 1877, 1-121, Bulletin des Sci. math. astron., 1er série, t. XI, 2e série, t. I, 1876, 1877; Werke III, 262-296.

[De-1877b] ______. Über die Anzahl der Ideal-Klasse in den verschiedenen Ordnungen eines endlichen Körpers, Festschrift Techn. Hochschule Braunschweig zur Säkularfeier des Geburtstages von C. F. Gauß, Braunschweig, 1877, pp.1-55; Werke I, 105-157.

[De-1878] ______. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Abhandl. kgl. Ges. Wiss. Göttingen, Bd.23 (1878), 1-23; Werke I, 202-230.

[De-1879] ______. Supplement XI. Über die Theorie der ganzen algebraischen Zahlen, von Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet (3. Auflage), 515-530, (1879); Werke III, 297-313.

[De-1882] ______. Über die Discriminanten endlicher Körper, Abhandl. kgl. Ges. Wiss. Göttingen Bd.29 (1882), 1-56; Werke I, 351-396.

[De-1882*] ______. Aus Briefen an Frobenius, Werke II, 414-442.

[De-1892] ______. Erläuterungen zu zwei Fragmenten von Riemann, B. Riemanns gesammelte math. Werke und wissenschaftlicher Nachlass, 2. Auflage, 1892, pp.466-478; Werke I, 159-172.

[De-1893] ______. Supplement XI. Über die Theorie der ganzen algebraischen Zahlen, von Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet (4. Auflage), 434-657, (1893). Reprint from Chelsea, New York, 1968.

[De-1894] ______. Zur Theorie der Ideale, Nachr. kgl. Ges. Wiss. Göttingen, Math.-phys. Klasse, 1894, 272-277; Werke II, 43-48.

[De-1900] ______. Über die Anzahl der Ideal-Klassen in reinen kubischen Zahlkörpern, Jour. reine angew. Math. 121 (1900), 40-123; Werke II, 148-233.

[De-1930] ______. Gesammelte Mathematische Werke I, II, III, Braunschweig, 1930-1932; Reprint, Chelsea, New York, 1969.

[D&W-1882] R. Dedekind and H. Weber. Theorie der algebraischen Functionen einer Veränderlichen, Jour. reine angew. Math. 92 (1882), 181-290.

[Di-1833] P.G. Lejeune Dirichlet. Untersuchungen über die Theorie der Quadratischen Formen, Abhandl. König. Preuss. Akad. Wiss. Jahrg. 1833, 101-121; Werke I, 195-218.

[Di-1834] ______. Einige Neue Sätze über Unbestimmte Gleichungen, Abhandl. König. Preuss. Akad. Wiss. Jahrg. 1834, 649-664; Werke I, 219-236.

[Di-1837a] ______. Beweis eines Satzes über die arithmetische Progression, Bericht Verhandl. König. Preuss. Akad. Wiss. Jahrg. 1837, 108-110; Werke I, 307-312.

[Di-1837b] ______. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, Abhandl. König. Preuss. Akad. Wiss. Jahrg. 1837, 45-81; Werke I, 313-342.

[Di-1838] ______. Sur l'usage des séries infinies dans la théorie des nombres, Jour. reine angew. Math. 18 (1838), 259-274; Werke I, 357-374.

[Di-1839] ______. Recherches sur diverses applications de l'analyse infinitésimale á la théorie des nombres, Jour. reine angew. Math. 19 (1839), 324-369, und 21 (1840), 1-12 und 134-155; Werke I, 411-496.

[Di-1841] ______. Einige Resultate von Untersuchungen über eine Classe homogener Functionen des dritten und der höheren Grade, Sitzung der physik.-math. Classe der Acad. Wissens. Jahrg. (1841), 280-285.

[Di-1842] ______. Recherches sur les formes quadratiques à coefficients et à indetérminées complexes, Jour. reine angew. Math. 24 (1842), 291-371; Werke I, 533 -618.

[Di-1846] ______. Zur Theorie der complexen Einheiten, Bericht König. Preuss. Akad. Wiss. Jahrg. 1846, 103-107; Werke I, 639-644.

[Di-1889] ______. G. Lejeune Dirichlet's Werke I, II, Berlin, 1889-1897; Reprint, Chelsea, New York, 1969.

[Ed-1975] H. M. Edwards. The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes, Arch. Hist. Exact Sci. 14 (1975), 219-236.

[Ed-1977] ______. Postscript to "The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes", Arch. Hist. Exact Sci. 17 (1977), 381-394.

[Ei-1844a] Gotthold Eisenstein. Beweis des Reciprocitätssatzes für die cubischen Restes in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complex Zahlen, Jour. reine angew. Math. 27 (1844), 289-310; Mathematische Werke, I, 59-80.

[Ei-1844b] ______. Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten complex Zahlen. Criterien des cubischen Characters der Zahl 3 und ihrer Theiler, Jour. reine angew. Math. 28 (1844), 28-35; Mathematische Werke, I, 81-88.

[Ei-1844c] ______. Lois de réciprocité, Jour. reine angew. Math. 28 (1844), 53-67; Mathematische Werke, I, 126-140.

[Ei-1844d] ______. Einfach Beweis und Verallgemeinerung des Fundamentaltheorems für die Biquadratischen Reste, Jour. reine angew. Math. 28 (1844), 223-245; Mathematische Werke, I, 141-163.

[Ei-1844e] ______. Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreistheilung ihre Entstehung verdanken, Jour. reine angew. Math. 28 (1844), 289-374 und 29 (1845), 19-53; Mathematische Werke, I, 167-286.

[Ei-1975] ______. MATHEMATSCHE WERKE I, II, Chelsea Publ. Comp., New York, 1975.

[Eu-1911] Leonhardi Euleri Opera omnia, sub ausp. Soc. scient. Nat. Helv. Seres I-IV A, 1911.

[Eu-1862] Leonhardi Euleri Opera Postuma Mathematica et Phisica I, Anno 1844 detecta, edd.P.-H. Fuss et Nic. Fuss, Petropoli 1862 (Reprint, Kraus 1969).

[Fe-1891] Pierre de Fermat. Œuvres de Fermat, pub. par Paul Tannery et Charles Henry, Paris, 4 vol., 1891-1912 (& Supplément, pub. par M.C. de Waard, 1 vol., 1922).

[Fe-1679] ______. Varia Opera Mathematica D·Petri de Fermat, Senatoris Tolosani, Tolosae, Apud Joannem Pech, juxta Collegium PP. Societatis Jesu M.DC.LXXIX.

[Fre-1989] Günther Frei. Heinrich Weber and the Emergence of Class Field Theory, in The History of Modern Mathematics, ed. D. E. Rowe and J. McCleary, Acad. Press, 1989, pp.425-450.

[Fre-2001] ______. Gauss' unpublished Section Eight of the Disquisitiones arithmeticae: The Beginning of the Theory of Function Fields over a Finite Field, Lecture held in Oberwolfach on June 21, 2001; Preprint, 24th of June, 2001.

[Fr-1887a] G. Frobenius. Neuer Beweis des Sylowschen Satzes, Jour. reine angew. Math. 100 (1887), 179-181; Ges. Abh. II, 301-303.

[Fr-1887b] ______. Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul, Jour. reine angew. Math. 101 (1887), 273-299; Ges. Abh. II, 304-330.

[Fr-1896a] ______. Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, Sitzungsber. König. Preuss. Akad. Wiss. Berlin (1896), 689-703; Ges. Abh. II, 719-733.

[Fr-1896b] ______. Über Gruppencharaktere, Sitzungsber. König. Preuss. Akad. Wiss. Berlin (1896), 985-1021; Ges. Abh. III, 1-37.

[Fr-1968] ______. Gesammelte Abhandlungen I, II, III, Springer-Verlag, 1968.

[Ft-1914] R. Fueter. Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern, Math. Ann. 75 (1914), 177-255.

[Fw-1930] Ph. Furtwängler. Beweis des Hauptidealsatzes für Klassenkörper algebraischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg 7 (1930), 14-36.

[Gal-1846] E. Galois. Sur la théorie des nombres, Jour. Math. pures appl. 11 (1846), 398-407; Écrite et Mémoires Mathématiques d'Évariste Galois, par R. Bourgne et J.-P. Azra, Gauthier-Villars, Paris, 1962, 113-127.

[G-1799] C. F. Gauss. Demonstratis Nova Theorematis Omnem Functionem Algebraicam Rationalem Integram Unius Variabilis in Factores Reales Primi vel Secondi Gradus Resolvi Posse (1799), Gauss Werke III, Göttingen, 1866, 1-30.

[G-1801] ______. Disquisitiones Arithmeticae, Leibzig, 1801; Gauss Werke I, Göttingen, 1863.

[G-1801*] ______. Disquisitiones Generales de Congruentiis. Analysis Residuorum Caput Octavum, Gauss Werke II, Göttingen, 1863, 212-242.

[G-1828] ______. Theoria Residuorum Biquadraticorum, Commentatio Prima, Comment. soc. reg. sci. Gottingen 1828; Werke II, 65-92.

[G-1832] ______. Theoria Residuorum Biquadraticorum, Commentatio Secunda, Comment. soc. reg. sci. Gottingen 1828; Werke II, 93-148.

[G-1863] ______. CARL FRIEDRICH GAUSS WERKE Bd.I - Bd.XII, König. Gesel. Wiss. Göttingen, 1863 - 1929; Reprint, Georg Olms Verlag, Hildesheim·New York, 1973.

[Gi-1637] Albert Girard. Invention nouvelle en l'algèbre, Amsterdam, 1629 (Reprint by Bierens de Haan, Leyde, 1884).

[Ha-1896] Jacques Hadamard. Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques, Bull. Soc. Math. France, 24 (1896), 199-228.

[Hk-1970] Th. Hawkins. The Origin of the Theory of Group Characters, Arch. History Exact Sci.7 (1970/71), 142-170.

[Hk-1974] ______. New Light on Frobenius' Creation of the Theory of Group Characters, Arch. History Exact Sci. 12 (1974), 217-243.

[Hi-1896] D. Hilbert. Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper, Nachr. Akad. Wiss. Göttingen (1896), 29-39; Ges.Abh.I, 53-62.

[Hi-1897] ______. Bericht: Die Theorie der algebraischen Zahlkörper, Jber. Deutschen Math.-Ver.4 (1897), 175-546; Ges.Abh.I, 63-363.

[Je-1915] Kaj Loechte Jensen. Om talteoretiske Egenskaber ved de Bernoulliske Ta (Danish; On number theoretic properties of the Bernoulli numbers), Nyt Tidsskrift for Matematik, Afd. B, vol. 26 (1915), pp. 73-83.

[KY-1992] A. N. Kolmogorov and A. P. Yushkevich (Edit.). Mathematics of the 19th Century, Mathematical Logic, Algebra, Number Theory, Probability Theory, Birkhäuser, Basel·Boston·Berlin, 1992.

[Kr-1853] L. Kronecker. Über die algebraisch auflösbaren Gleichungen, Monatsber. König. Preuss. Acad. Wiss. Berlin (1853), 365-374; Werke IV, 1-11.

[Kr-1857a] ______. Über die elliptischen Functionen, für welche complexe Multiplication stattfindet, Monatsber. König. Preuss. Acad. Wiss. Berlin (1857), 455-460; Werke IV, 177-183.

[Kr-1857b] ______. Brief an G. L. Dirichlet vom 17 Mai 1857, Nachr. König. Akad. Wiss. Göttingen (1885), 253-297; Werke V, 418-421.

[Kr-1862] ______. Über die complexe Multiplication der elliptischen Functionen, Monatsber. König. Preuss. Acad. Wiss. Berlin (1862), 363-372; Werke IV, 207-217.

[Kr-1874] ______. Über die congruenten Transformation der bilineiar Formen, Monatsber. König. Preuss. Acad. Wiss. Berlin (1874), 397-447; Werke I, 423-483.

[Kr-1877] ______. Über Abelsche Gleichung (Auszug aus der am 16. April 1877 gelesenen Abhandlung), Monatsber. König. Preuss. Acad. Wiss. Berlin (1877), 845-851; Werke IV, 63-72.

[Kr-1880a] ______. Über die Irreductibilität von Gleichungen, Monatsber. König. Preuss. Acad. Wiss. Berlin (1880), 155-162; Werke II, 85-93.

[Kr-1880b] ______. Auszug aus einem Briefe von L. Kronecker an R. Dedekind, 15. März, 1880, Werke V, 455-457.

[Kr-1882a] ______. Grundzüge einer arithmetschen Theorie der algebraischen Grössen, Jour. reine angew. Math. 92 (1882), 1-122; Werke II, 237-388.

[Kr-1882b] ______. Die Composition Abelscher Gleichungen, Sitzungsber. Acad. Wiss. Berlin (1882), 1059-1064; Werke IV, 115-121.

[Kr-1895] ______. Mathematische Werke I-V, Leipzig, 1895-1930; Reprint, Chelsea, New York, 1968.

[Ku-1844a] Ernst Eduard Kummer. Über die complexen Primfactoren der Zahlen, und deren Anwendung in der Kreisteilung, April, 1844, Appendix 1 to [Ed-1977], pp.388-393.

[Ku-1844b] ______. De numeris complexis, qui radicibus unitatis et numeris integris realibus constant, In: Gratulationsschrift d. Univ. Breslau zur Jubelfeier d. Univ. Königisberg 1844, pp.28; Jour. pures et appl. 12 (1847), 185-212; Collected Papers I, 165-192.

[Ku-1846a] ______. Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung entstehen, Jour. reine angew. Math. 30 (1846), 107-116; Collected Papers I, 193-202.

[Ku-1846b] ______. Vervollständigung der Theorie der complexen Zahlen, Monatsber. König. Preuss. Wiss. Berlin (1846), 87-96.

[Ku-1847a] ______. Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren, Jour. reine angew. Math. 35 (1847), 327-367; Collected Papers I, 211-251.

[Ku-1847b] ______. Zur Theorie der complexen Zahlen (Republ. of [Ku-1846a]), Jour. reine angew. Math. 35 (1847), 319-326; Collected Papers I, 203-210.

[Ku-1847c] ______. Beweis des Fermat'schen Satzes der Unmöklivhkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen λ, Monatsber. König. Preuss. Akad. Wiss. Berlin, 1847, 132-141, 305-319; Collected Pares I, 274-283, 283-297.

[Ku-1850a] ______. Bestimmung der Anzahl nicht äquivalenter Classen für die aus λten Wurzel der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben, Jour. reine angew. Math. 40 (1850), 93-116; Collected Pares I, 299-322.

[Ku-1850b] ______. Zwei besondere Untersuchngen über die Classen-Anzahl und über die Einheiten der aus λten Wurzel der Einheit gebildeten complexen Zahlen, Jour. reine angew. Math. 40 (1850), 117-129; Collected Papers I, 323-335.

[Ku-1850c] ______. Allgemeiner Beweis des Fermat'schen Satzes, dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zahlen der ersten $(\lambda - 3)/2$ Bernoulli'schen Zahlen als Factoren nicht vorkommen, Jour. reine angew. Math. 40 (1850), 368-372; Collected Papers I, 336-344.

[Ku-1850d] ______. Allgemeine Reciprocitätsgesetze für beliebig hohe Potenzreste, Monatsber. König. Preuss. Akad. Wiss. Berlin, 1850, 154-165; Collected Papers I, 345-357.

[Ku-1851a] ______. Über eine allgemeine Eigenschaft der rationalen Entwiklungscoefficienten einer bestimmten Gattung analytischer Funktionen, Jour. reine angew. Math. 41 (1851), 130-138; Collected Papers I, 358-362.

[Ku-1851b] ______. Mémoire sur la théorie des nombres complexes composés de raciness de unité et de nombres entiers, Jour. math. pures et appl. 16 (1851), 377-498; Collected Papers I, 363-484.

[Ku-1852] ______. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, Jour. reine angew. Math. 44 (1852), 93-146; Collected Papers I, 485-538.

[Ku-1855] ______. Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke, Jour. reine angew. Math. 50 (1855), 212-232; Collected Papers I, 552-572.

[Ku-1856] ______. Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine Zusammengesetzte Zahl ist, Math. Abhandl. König. Preuss. Akad. Wiss. Berlin (1856), 1-47; Collected Papers I, 583-629.

[Ku-1857a] ______. Über die den Gaussischen Perioden der Kreistheilung entsprechenden Congruenzwurzeln, Jour. reine angew. Math. 53 (1857), 142-148; Collected Papers I, 573-580.

[Ku-1857b] ______. Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildete complexen Zahlen, für den Fall, dass die Klassenzahl durch λ teilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes, Monatsber. König. Preuss. Akad. Wiss. Berlin, 1857, 275-282; Collected Papers I, 631-638.

[Ku-1857c] ______. Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildete complexen Zahlen, für den Fall, dass die Klassenzahl durch λ teilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes, Math. Abhandl. König. Preuss. Akad. Wiss. Berlin, 1857, 41-74; Collected Papers I, 639-672.

[Ku-1858] ______. Über die allgemeinen Reciprocitätsgesetze, Monatsber. König. Preuss. Akad. Wiss. Berlin, 1858, 158-171; Collected Papers I, 673-687.

[Ku-1859a] ______. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, Jour. reine angew. Math. 56 (1859), 270-279; Collected Papers I, 688-697.

[Ku-1859b] ______. Über die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist, Math. Abhandl. König. Preuss. Akad. Wiss. Berlin (1859), 19-159; Collected Papers I, 699-839.

[Ku-1874] ______. Über diejenigen Primzahlen λ, für welche die Klassenzahl der aus λten Einheitswurzeln gebildeten complexen Zahlen durch λ teilbar ist, Monatsber. König. Preuss. Akad. Wiss. Berlin, 1874, 239-248; Collected Papers I, 945-954.

[Ku-1887] ______. Zwei neue Beweise der allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist, Jour. reine angew. Math. 100 (1887), 10-50; Collected Papers I, 842-882.

[Ku-1975] ______. Collected Papers I, II; Springer-Verlag, 1975.

[La-1770] J. L. Lagrange. Réflexions sur la Résolution Algébraique des Équations, Nouveaux Mémoires de l'Académie des Sciences et Belles Lettres de Berlin, Année 1770 et 1771; Œuvres de Lagrange III, 203-421.

[La-1867] ______. Œuvres de Lagrange, pub. par M. J.-A. Serret et M. Gaston Darboux, Paris, 14 vol., 1867-1892.

[Le-1785] A.-M. Legendre. Recherches d'Analyse Indéterminée, Histoire de l'Acad. Royale des Sci., Paris, 1785; Mémoires de Mathématique et de Physique de l'Imprimerie Royale, Paris, 1788, 465-559.

[Le-1792] ______. Mémoire sur les Transcendantes elliptiques, Académie Sciences 1792, Paris, l'an deuxième de la Répablique.

[Le-1798] ______. Essai sur la Théorie des Nombres, Chez Duprat, Libraire pour Mathématiques, quai des Augustins, An VI, Paris, 1798; 2nd ed., Courcier, Paris, 1808.

[Le-1811] ______. Exercices de calcul intégral, 3 vol., Paris, 1811-17.

[Le-1825] ______. Traité des fonctions elliptiques, 3 vol., Paris, 1825-1828.

[Le-1830] ______. Théorie des Nombres, troisième édition, 2 vol., Firmin-Didot, 1830.

[Mi-1988] Katsuya Miyake. The capitulation problem, Sugaku Expositions Vol.1 (1988), No.2, 175-194, Amer. Math. Soc.

[Mi-1989] ______. A Note on the Arithmetic Background to Frobenius' Theory of Group Characters, Expo. Math. 7 (1989), 347-358.

[Mi-1994] ______. The establishment of the Takagi-Artin class field theory, in The Intersection of History and Mathematics (ed. J.W.Dauben et al), Birkhäuser Verlag, Basel·Boston·Berlin, 1994, pp.109-128.

[Na-1990] Władysław Narkiewicz. Elementary and Analytic Theory of Algebraic Numbers, Second Edit., Springer-Verlag, Berlin ·Heidelberg·New York·London·Paris ·Tokyo·Hong Kong, 1990.

[Ne-1981] Olaf Neumann. Two proofs of the Kronecker-Weber theorem "according to Kronecker, and Weber", Jour. reine angew. Math. 323 (1981), 105-126.

[Ni-1906] N. Nielsen. Theorie des Integrallogarithmus und verwandter Transzendenten, Taubner, 1906; Chelsea reprint, 1965.

[Ro-1608] Peter Roth. Arithmetica philosophica, order schöne, neue, wohlgegründete, überaus künstliche Rechnung der Coss oder Algebra, Nürnberg, 1608.

[Sc-1927] O. Schreier. Über eine Arbeit von Herrn Tschebotareff, Abh. Math. Sem. Univ. Hamburg, 5 (1927), 1-6.

[Se-1865] E. Selling. Über die idealen Primfactoren der complexen Zahlen, welche aus den wurzeln einer beliebigen irreductibeln Gleichung rational gebildet sind, Schlömilch's Zeitschr. für Math. u. Phys. 10 (1865), 17-47.

[Si-1964] C. L. Siegel. Zu zwei Bemerkungen Kummers, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Klasse, 1964, Nr.6, 51-57; Gesammelte Abhandlungen III, 436-442.

[Ta-1903] Teiji Takagi. Über die im Bereiche der rationalen complexen Zahlen Abel'scher Zahlkörper, J. Coll. Sci. Tokyo 19 (1903), 1-42; Collected Papers, 13-39.

[Ta-1915] ______. Zur Theorie der relativ-Abel'schen Zahlkörper I, Proc. Phys.-Math. Soc. Japan, Ser.II, 8 (1915), 154-162; II, 243-254; Collected Papers, 43-50, 51-60.

[Ta-1920] ______. Ueber eine Theorie des relativ Abel'schen Zahlkörpers, J. Coll. Sci. Tokyo 41 (1920), 1-133; Collected Papers, 73-167.

[Ta-1948] ______. Algebraic Number Theory (in Japanese), Iwanami Shoten, Tokyo, 1948.

[Ta-1973] ______. The Collected Papers, Iwanami Shoten, 1973; the 2nd edit., Springer-Verlag, 1990.

[Tc-1849] P. L. Tchebychef. Sur la fonction qui détermine la totalité des nombres premiers inférieures à une limite donnée, Jour. math. pures et appl. I sérei, 17 (1852), 341-365; Œuvres I, 27-48.

[Tc-1852] ______. Mémoire sur les nombres premiers, Jour. math. pures et appl. I sérei, 17 (1852), 366-390; Œuvres I, 49-70.

[Tc-1861] ______. Sur l'intégration de la différentielle $\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}}$; Bull. l'Acad. Impér. sci. St.-Pétersbourg, T. III (1861), 1-12 = Œuvres I, 517-530.

[Tc-18**] ______. Œuvres I, II; Reprint, Chelsea, New York, 1962.

[Ts-1926] N. G. Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen substitutionsklasse gehören, Math. Ann. 95 (1926), 191-228.

[VP-1896] C. de la Vallée Poussin. Recherches analytiques sur la théorie des nombres, Annal. de la Soc. Bruxells, 20 (1896), 183-256, 281-397.

[Vo-1914] Aurel Voss. Heinrich Weber, Jahresbericht der DMV 23 (1914), 431-444.

[Wb-1882] H. Weber. Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darstellen fähig ist, Math. Ann. 20 (1882), 301-329.

[Wb-1884] ______. Ueber die Galois'sche Gruppe der Gleichung 28^{ten} Grades, von welcher die Doppeltangenten einer Curve vierter Ordnung abhängen, Math. Ann. 23 (1884), 489-503.

[Wb-1886] ______. Theorie der Abelschen Zahlkörper I, Acta Math. Stokh. 8(1886), 193-263; II, 9 (1887), 105-130.

[Wb-1891] ______. Elliptischen Functionen und algebraischen Zahlen, Braunschweig, 1891.

[Wb-1894] ______. Lehrbuch der Algebra, Vol. I - II, Braunschweig, 1894, 1896.

[Wb-1897] ______. Ueber Zahlengruppen in algebraischen Körpern I, Math. Ann. 48 (1897), 433-473; II, 49 (1897), 83-100; III, 50(1898), 1-26.

[Wb-1900] ______. Komplexe Multiplikation, in: Encyklopödie der Mathematischen Wissenschaften, Leibzig, 1900-1904, I.2.C. Zahlentheorie, 6, pp.718-732.

[Wb-1908] ______. Lehrbuch der Algebra, Vol. III, Braunschweig, 1908; (the second edition of [W-1891]).

[Wb-1909] ______. Zur Theorie der zyklischen Zahlkörper (I), Math. Ann. 67 (1909), 32-60; (II), 70 (1911), 459-470.

[We-1975] André Weil. Introduction of "Ernst Eduard Kummer Collected Papers I", Springer-Verlag, 1975.

[We-1984] ______. Number Theory, An approach through history, From Hammurapi to Legendre, Birkhäuser, Boston·Basel·Stuttgart, 1984.

[Zo-1874] E. I. Zolotareff. Sur la méthode d'intégration de M. Tchebychef, Jour. de Math. pures appl. 2e série, 16 (1874), 161-188.

[Zo-1880] ______. Sur la théorie des nombres complexes, Jour. de Math. pures appl. 3e série, 6 (1880), 51-84, 129-166.