On $K(2)$ of Rings of Integers of Totally Real Number Fields (Birch-Tate, Steinberg, Class Number, Symbol, Zeta-Function).

Karl Friedrich Hettling

Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_disstheses

Recommended Citation
Hettling, Karl Friedrich, "On $K(2)$ of Rings of Integers of Totally Real Number Fields (Birch-Tate, Steinberg, Class Number, Symbol, Zeta-Function)." (1985). LSU Historical Dissertations and Theses. 4056.
https://digitalcommons.lsu.edu/gradschool_disstheses/4056

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.
INFORMATION TO USERS

This reproduction was made from a copy of a document sent to us for microfilming. While the most advanced technology has been used to photograph and reproduce this document, the quality of the reproduction is heavily dependent upon the quality of the material submitted.

The following explanation of techniques is provided to help clarify markings or notations which may appear on this reproduction.

1. The sign or “target” for pages apparently lacking from the document photographed is “Missing Page(s)”. If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting through an image and duplicating adjacent pages to assure complete continuity.

2. When an image on the film is obliterated with a round black mark, it is an indication of either blurred copy because of movement during exposure, duplicate copy, or copyrighted materials that should not have been filmed. For blurred pages, a good image of the page can be found in the adjacent frame. If copyrighted materials were deleted, a target note will appear listing the pages in the adjacent frame.

3. When a map, drawing or chart, etc., is part of the material being photographed, a definite method of “sectioning” the material has been followed. It is customary to begin filming at the upper left hand corner of a large sheet and to continue from left to right in equal sections with small overlaps. If necessary, sectioning is continued again—beginning below the first row and continuing on until complete.

4. For illustrations that cannot be satisfactorily reproduced by xerographic means, photographic prints can be purchased at additional cost and inserted into your xerographic copy. These prints are available upon request from the Dissertations Customer Services Department.

5. Some pages in any document may have indistinct print. In all cases the best available copy has been filmed.

University Microfilms International
300 N. Zeeb Road
Ann Arbor, MI 48106
Hettling, Karl Friedrich

ON K_{(2)} OF RINGS OF INTEGERS OF TOTALLY REAL NUMBER FIELDS

The Louisiana State University and Agricultural and Mechanical Col.  Ph.D.  1985

University Microfilms International  300 N. Zeeb Road, Ann Arbor, MI 48106
On $K_2$ of Rings of Integers of Totally Real Number Fields

A Dissertation
Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in
The Department of Mathematics

by
Karl Friedrich Hettling
B.S., Universität Hamburg, 1978
M.S., Universität Hamburg, 1982
May 1985
List of Tables

Table 1  The values of $|w_2(F)\zeta_p(-1)|$ for the totally real
subfields of $\mathbb{Q}(\zeta_p)$, $p < 100$, prime ........................................... 37

Table 2  The values of $|w_2(F)\zeta_m(-1)|$ for the maximal totally real
subfields of $\mathbb{Q}(\zeta_m)$, $m \leq 100$, composite ................................. 40

Table 3  The prime numbers $p < 10000$ with the property that
$q = \frac{p-1}{2}$ is prime and 2 is a primitive root of $q$ ..................................... 42
Abstract

We study the finite abelian groups $K_2(o)$, where $o$ denotes the ring of integers of a totally real number field. As a major tool we employ the Birch-Tate conjecture which states that the order of $K_2(o)$ can be computed via the Dedekind zeta-function. The odd part of this conjecture has been proved for abelian fields as a consequence of the Mazur-Wiles work on the "Main conjecture".

After the preliminaries of chapter 1, we proceed in chapter 2 by deriving a formula for $\zeta_F(-1)$, where $F$ denotes a totally real abelian number field. Using this formula we prove the congruence $\ell \equiv 1 \mod [F : Q]$ for a class of large prime divisors $\ell$ of $\#K_2(o)$. For the totally real subfields of $Q(\zeta_p)$, $p$ prime, we obtain that every prime $q \geq 5$ dividing the field degree $[F : Q]$ is a divisor of $\#K_2(o)$. Finally we show that a prime number $p$ is irregular if and only if $p$ divides the order of $K_2(o_F)$, where $F$ is the maximal totally real subfield of $Q(\zeta_p)$.

In chapter 3 we use results of J. Hurrelbrink and M. Kolster to prove the 2-part of the Birch-Tate conjecture for two families of abelian number fields, one of them being the totally real subfields of $Q(\zeta_{2k})$, $k \in \mathbb{N}$. We compute the 2-parts of $w_2(F)\zeta_F(-1)$ and show that the full cyclotomic fields involved have odd class numbers. In chapter 4 we combine recent results of J. Hurrelbrink and P. E. Conner with those of K. S. Brown on the values of the Dedekind zeta-function and obtain that the conditions $2^{[F : Q]} \parallel \#K_2(o)$ and $2^{[F : Q]} \parallel w_2(F)\zeta_F(-1)$ are equivalent. Therefore the 2-part of the Birch-Tate conjecture holds for any—not necessarily abelian—totally real number field satisfying one (and hence both) of these conditions.

Table 1 and table 2 contain the values of $|w_2(F)\zeta_F(-1)|$ for totally real subfields of $Q(\zeta_m)$, $m \leq 100$. In table 3 we list all primes $p < 10000$ with the property that $q = \frac{p-1}{2}$ is prime and $2$ is a primitive root of $q$. 
Having undergone quite a rapid development within the last twenty-odd years, algebraic K-theory has found applications in various mathematical disciplines. In the case of number fields $F$ and their rings of integers $\mathcal{O}$ the study of the various $K$-groups $K_0(\mathcal{O}), K_1(\mathcal{O}), K_2(\mathcal{O}), \ldots$ is closely related to the arithmetic of the underlying rings. So it is well known [24] that $K_0(\mathcal{O}) \cong \mathbb{Z} \times Cl$, where $Cl$ denotes the ideal class group of $F$, and $K_1(\mathcal{O}) \cong o^\times$, the unit group of $o$.

For the abelian group $K_2(\mathcal{O})$ there are no general structure theorems of this kind. A theorem of H. Garland [11] states that $K_2(\mathcal{O})$ is finite. The algebraic meaning of $K_2(\mathcal{O})$ is that it contains the "nontrivial" relations between elementary matrices with entries in $\mathcal{O}$. For rings of integers of number fields it is well known that $E(\mathcal{O})$, the group generated by elementary matrices, is equal to $SL(\mathcal{O})$, the special linear group, consisting of all matrices with determinant 1. Hence knowing $K_2(\mathcal{O})$ yields a presentation of $SL(\mathcal{O})$ in terms of generators and relations.

An important invariant for any finite abelian group is its order. A conjecture of Birch and Tate ([1], [29]) states that $\#K_2(\mathcal{O}) = |w_2(F) \cdot \zeta_F(-1)|$ for all totally real number fields, where $\zeta_F$ is the Dedekind zeta-function of $F$ and $w_2(F)$ is a factor that can be fairly easily determined. The proof of the "Main Conjecture" by Mazur and Wiles [23] implies the Birch-Tate conjecture for abelian number fields up to 2-torsion. In particular, there is an element of $K_2(\mathcal{O})$ having order $q$ for every odd prime number $q$ dividing $\wp(F)\zeta_F(-1)$. The 2-part of the Birch-Tate conjecture is still unproved except for some families of totally real abelian number fields, see [17], [18], [21], [22], [31].

In this dissertation we show the existence of certain "small" divisors of $\#K_2(\mathcal{O})$ and give congruence conditions for "large" ones. We prove the Birch-Tate conjecture for two families of abelian number fields, one of them being the totally real subfields of the cyclotomic fields $\mathbb{Q}(\zeta_{2^k})$. Our main result is the proof of the 2-part of the Birch-Tate conjecture for all totally real—not necessarily abelian—number fields $F$ with the property that $2^{|F:Q|}$ is the exact 2-power dividing $w_2(F)\zeta_F(-1)$. 
In chapter 1 we give the basic definitions and a collection of known facts about $K_2(o)$. We define the group $K_2(R)$ for arbitrary associative rings $R$ with 1 via the Steinberg group $St(R)$. For rings of integers $o$ of number fields $F$ we give an alternative definition of $K_2(o)$ in terms of an exact sequence involving $K_2(F)$ and tame symbols [25].

Throughout chapter 2 we consider totally real subfields $F$ of cyclotomic fields $Q(\zeta_m)$, where $\zeta_m = e^{2\pi i/m}$, $m \in \mathbb{N}$. Using a formula for the values of the Dedekind zeta-function that is essentially due to C. L. Siegel [27], we show that most of the large prime divisors of $\#K_2(o)$ are congruent to 1 modulo the field degree $[F : Q]$. For the real subfields $F$ of $Q(\zeta_p)$, where $p$ is a prime number, we prove that every prime $q \geq 5$ dividing $[F : Q]$ is also a divisor of the order of $K_2(o)$. Finally we derive that a prime number $p$ is irregular if and only if $p$ divides the order of $K_2(o_F)$, where $F$ is the maximal totally real subfield of the cyclotomic field $Q(\zeta_p)$.

Chapter 3 deals with the 2-part of the Birch-Tate conjecture. We narrow our attention to totally real fields with the property that $2^{[F : Q]}$ is the exact 2-power dividing $w_2(F)\chi_F(-1)$. By the 2-rank formula for $K_2(o)$ [30] and a result of Serre [26], this is the minimal power of 2 that can possibly occur. Fields of this type have the property that 2 is inert in $F/Q$ and that their $S$-class numbers are odd, where $S$ denotes the set of infinite and dyadic primes of $F$. To obtain our results we apply a theorem of J. Hurrelbrink and M. Kolster [18] that gives conditions equivalent to the Birch-Tate conjecture. We consider two families of abelian fields, namely the maximal totally real subfields of the cyclotomic fields $Q(\zeta_{3k}), k \in \mathbb{N}$, and of $Q(\zeta_{q^k})$, where $p$ is a prime number congruent to 3 modulo 8 such that $q = \frac{2^k - 1}{3}$ is a prime having 2 as a primitive root. In both cases we show first that $2^{[F : Q]} \parallel w_2(F)\chi_F(-1)$. This property implies that the Birch-Tate conjecture is equivalent to the statement that the class numbers of the full cyclotomic fields are odd. Using the analytic class number formula we determine the 2-parts of the relative class numbers of these fields, which turn out to be trivial, and the Birch-Tate conjecture follows. Moreover we can conclude from this that the maximal totally real subfields of the above fields contain systems of fundamental units with independent signs.

In chapter 4 we approach the same problem, i.e. the proof of the 2-part of the Birch-Tate conjecture, for a larger class of fields by combining recent results of J. Hurrelbrink and P. E. Conner [8] with those of K. S. Brown [5] on the values of the Dedekind zeta-function. In
particular, our result holds even in the non-abelian case. We obtain our main theorem, namely that the conditions \(2^{|F:Q|} \parallel \# K_2(o)\) and \(2^{|F:Q|} \parallel w_2(F) \zeta_p(-1)\) are equivalent. Therefore the 2-part of the Birch-Tate conjecture holds for any totally real number field satisfying either one (and hence both) of these conditions. This generalizes earlier results considerably. Except for one [31], all the families of fields for which the Birch-Tate conjecture has been proved so far are covered by this theorem.

Table 1 and 2 were produced in order to have some examples at hand that might suggest theorems. In fact, the chapter on odd divisors of \(\# K_2(o)\) originated from this computational work. Furthermore, the tables do not only illustrate the results but also contain proofs of the Birch-Tate conjecture for special cases in the sense that the Birch-Tate conjecture holds for every field mentioned in table 1 or 2 for which \(2^{|F:Q|} \parallel w_2(F) \zeta_p(-1)\). Most of the computations have been performed on a VAX 11/750 running MACSYMA. Table 1 contains the values of \(|w_2(F) \zeta_p(-1)|\) for all totally real subfields of \(Q(\zeta_p)\), \(p < 100\) prime. Table 2 lists the corresponding values of the maximal totally real subfields of \(Q(\zeta_m)\) for composite \(m \leq 100\). In table 3 we give all prime numbers \(p < 10000\) having the property that \(q = \frac{p-1}{2}\) is prime and 2 is a primitive root of \(q\). In the appendix we present a program that was used for the computation of table 1.
Chapter 1

Preliminaries

§1.1. Basic definitions

A good reference for the material of this paragraph is [24]. Let $R$ be an arbitrary associative ring with an identity element $1$, $R^*$ its group of units. We will be concerned with groups of matrices having entries in $R$. For $n \in \mathbb{N}$, denote by $GL(n, R)$ the group of invertible $n \times n$-matrices over $R$ and by $SL(n, R)$ the subgroup of $GL(n, R)$ consisting of the matrices with determinant 1. Furthermore, let $E(n, R) \subseteq SL(n, R)$ be the group generated by elementary matrices $e_{ij}(r)$, $r \in R, 1 \leq i, j \leq n, i \neq j$. Here $e_{ij}(r)$ is the matrix with $r$ in the $i$-th row, $j$-th column, 1's in the main diagonal and zeroes elsewhere. We will mainly deal with $GL(R)$, $SL(R)$, and $E(R)$, which are defined to be the direct limits as $n \to \infty$ of the finite versions of the corresponding groups. One can simply think of them as unions, with the obvious identifications $A = \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$.

Now we introduce the Steinberg group of $R$ which is defined in terms of generators and relations that are designed to imitate the behavior of elementary matrices.

**Definition 1.1.** The Steinberg group $St(R)$ is the group given by generators $x_{ij}(r), r \in R, i, j \in \mathbb{N}, i \neq j$, and relations

(i) $x_{ij}(r)x_{ij}(s) = x_{ij}(r + s)$

(ii) $[x_{ij}(r), x_{kl}(s)] = \begin{cases} 1 & \text{if } i \neq l, j \neq k \\ x_{ii}(rs) & \text{if } i \neq l, j = k. \end{cases}$

Here $[a, b] = aba^{-1}b^{-1}$ denotes the commutator of $a$ and $b$. One can check easily that
elementary matrices $e_{ij}(r)$ satisfy these relations, and hence we have a canonical epimorphism
\[ \phi : \text{St}(R) \to \mathcal{E}(R) \]
which sends $x_{ij}(r)$ to $e_{ij}(r)$.

**Definition 1.2.** $K_2(R) = \ker(\phi)$.

This means that $K_2(R)$ represents the nontrivial relations between elementary matrices over $R$, if the relations (i), (ii) are considered the trivial ones. It has been proved in [24] (Thm. 5.1) that $K_2(R)$ is the center of the Steinberg group, thus $K_2(R)$ is an abelian group for any ring $R$. Since every homomorphism between rings $R$ and $S$ induces a homomorphism $K_2(R) \to K_2(S)$, $K_2$ is a covariant functor between rings (associative with 1) and abelian groups.

If one is interested in explicitly determining elements of $K_2(R)$, one has to look around for relations between elementary matrices. Several classes of elements of $K_2(R)$ have been successfully exhibited in this way and have led to the definitions of various "symbols", e.g. Steinberg symbols, Dennis-Stein symbols, and generalizations thereof. These are all elements depending on two entries $a, b \in R$ and satisfying properties at least similar to those that one is used to for number-theoretic symbols, like quadratic residue symbols or Hilbert symbols. For instance, consider the matrix identity
\[
\begin{pmatrix}
a & 0 \\
0 & a^{-1}
\end{pmatrix}
\begin{pmatrix}
b & 0 \\
0 & b^{-1}
\end{pmatrix}
= \begin{pmatrix}
ab & 0 \\
0 & (ab)^{-1}
\end{pmatrix}, a, b \in R^*,
\]
which holds whenever $R$ is commutative and gives rise to an element of $K_2(R)$ in the following way.

**Definition 1.3.** Let $R$ be a commutative ring, $a, b \in R^*$. Let $w_{12}(a) = x_{12}(a)x_{21}(-\frac{1}{a})x_{12}(a)$, $h_{12}(a) = w_{12}(a)w_{12}(-1)$. The element $\{a, b\}$ of $\text{St}(R)$, defined by
\[
\{a, b\} = h_{12}(a) h_{12}(b) h_{12}(ab)^{-1},
\]
is called a *Steinberg symbol* with entries in $R$. 
From the above matrix identity it follows that \( \{a, b\} \in K_2(R) \) for all \( a, b \in R^* \). In fact, if \( R = F \) is a field, \( K_2(F) \) is generated by Steinberg symbols. This is by no means true for arbitrary rings. For example, if \( o \) is the ring of integers of a real quadratic field \( \mathbb{Q}(\sqrt{m}) \), \( m > 0 \) squarefree, then \( K_2(o) \) is generated by Steinberg symbols if and only if \( m = 2, 5, \) or \( 13 \) [3].

Even if we do not restrict ourselves to quadratic fields, we do not know any element of \( K_2(o) \) of prime order \( \geq 5 \) that can be expressed as a Steinberg or Dennis-Stein symbol with entries in \( o^* \). The Dennis-Stein symbols \( <a, b> \in K_2(R) \), given by

\[
< a, b > := x_{21} \left( \frac{-b}{1 + ab} \right) x_{12}(a) x_{21}(b) x_{12} \left( \frac{-a}{1 + ab} \right) h_{12}(1 + ab)^{-1},
\]

are defined whenever \( 1 + ab \in R^* \) and arise from the matrix identity

\[
\begin{pmatrix}
1 & 0 \\
-\frac{b}{c} & 1
\end{pmatrix}
\begin{pmatrix}
1 & a \\
0 & 1
\end{pmatrix}
\begin{pmatrix}
1 & 0 \\
b & 1
\end{pmatrix}
\begin{pmatrix}
1 & -\frac{a}{c} \\
0 & 1
\end{pmatrix}
= 
\begin{pmatrix}
c & 0 \\
0 & c^{-1}
\end{pmatrix},
\]

with \( c := 1 + ab \) (see [9]). Every Steinberg symbol is a Dennis-Stein symbol; they are related to each other by

\[
< a, b >= \begin{cases}
\{ -a, 1 + ab \} & \text{if } a \in R^*, \\
\{ 1 + ab, b \} & \text{if } b \in R^*.
\end{cases}
\]

It is not known whether the Dennis-Stein symbols suffice for the generating of \( K_2 \) of rings of integers.

§1.2. \( K_2 \) of rings of integers

From now on let \( F \) be a number field, i.e. a finite extension of \( \mathbb{Q} \), \( o = o_F \) its ring of integers, and \( \zeta_F \) the Dedekind zeta-function associated to \( F \). Denote by \( r_1(F) \) and \( r_2(F) \) the number of real and pairs of complex embeddings of \( F \), respectively. Every abelian number field is contained in a cyclotomic field \( \mathbb{Q}(\zeta_m) \) for some \( m \in \mathbb{N} \). Here \( \zeta_m \) denotes a primitive \( m \)-th root of unity. If, in addition, \( F \) is totally real, \( F \) is contained in the maximal totally real subfield \( \mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1}) \) of \( \mathbb{Q}(\zeta_m) \). We give an alternative definition of \( K_2(o) \), see [25].
Definition 1.4.

a) Let $p$ be a finite prime of $F$, $\nu$ the valuation corresponding to $p$ with residue class field $\mathcal{F} = \mathbb{O}/p$. The map

$$r_p : F^* \times F^* \rightarrow \mathcal{F}^*$$

$$(x, y) \rightarrow (-1)^{\nu(x)\nu(y)} \frac{x^{\nu(y)}}{y^{\nu(x)}} \pmod{\mathcal{F}^*},$$

is called the $p$-adic tame symbol on $F$.

b) The group $K_2(\mathbb{O})$ is defined by the exact sequence

$$1 \rightarrow K_2(\mathbb{O}) \rightarrow K_2(F) \rightarrow \prod_{p} (\mathbb{O}/p)^* \rightarrow 1,$$

where the product is taken over the finite primes of $F$, and $\tau = (r_p)$ is given by the $p$-adic tame symbols.

In particular, $K_2(\mathbb{O})$ is a subgroup of $K_2(F)$. This permits to do computations with elements of $K_2(\mathbb{O})$ in $K_2(F)$ instead, which can be convenient since the latter is known to be generated by Steinberg symbols.

By a theorem of H. Garland [11], $K_2(\mathbb{O}_F)$ is a finite group for any number field $F$, and it is natural to ask for its order. In 1970, J. Birch [1] and J. Tate [29] conjectured that

$$\#K_2(\mathbb{O}) = \left| w_2(F) \cdot \zeta_p(-1) \right|,$$

for all totally real number fields $F$; here

$$w_2(F) := \max \{ m : \mathrm{Gal}(F(\zeta_m)/F)^2 = 1 \}.$$

Equivalently, $w_2(F) = 2 \prod \ell^{n_\ell(F)}$; the product is taken over all prime numbers $\ell$, and $n_\ell(F) := \max \{ n \geq 0 : \mathbb{Q}(\zeta_{\ell^n})^+ \subseteq F \}$. It is known that $w_2(F)\zeta_p(-1)$ is a rational integer [26]. The proof of the "Main Conjecture" by Mazur and Wiles [23] implies the Birch-Tate conjecture for all totally real abelian number fields up to the 2-primary part. In particular, if $p$ is an odd prime number, then

$$p \mid \#K_2(\mathbb{O}) \iff p \mid w_2(F) \cdot \zeta_p(-1).$$
Thus, odd prime divisors of \#K_2(o) can be found by computing \(w_2(F)\) and \(\zeta_F(-1)\). We state some obvious facts about \(w_2(F)\):

(i) \(w_2(\mathbb{Q}) = 24\).

(ii) If \(F \subseteq \mathbb{E}\), then \(w_2(F)\) divides \(w_2(\mathbb{E})\).

(iii) If \(F = \mathbb{Q}(\sqrt{m})^+\), \(m \in \mathbb{N}\), then

\[
w_2(F) = \begin{cases} 
2m & \text{if } 4 \mid m, \ 3 \mid m, \\
6m & \text{if } 4 \mid m, \ 3 \nmid m, \\
8m & \text{if } 2 \nmid m, \ 3 \mid m, \\
24m & \text{if } 2 \mid m, \ 3 \nmid m.
\end{cases} \tag{3}
\]

(iv) If \(F\) is a subfield of \(\mathbb{Q}(\sqrt{p})^+\), \(p\) prime, then

\[
w_2(F) = \begin{cases} 
24p & \text{if } F = \mathbb{Q}(\sqrt{p})^+, \\
24 & \text{otherwise}.
\end{cases} \tag{4}
\]

The 2-part of the Birch-Tate conjecture remains yet unproved except for some special families of number fields, see [17], [18], [21], [22], [31]. The only general result on the 2-Sylow-subgroup of \(K_2(o)\) is Tate's 2-rank formula, which holds for any number field ([30], see also [22]).

**Theorem 1.5.** Let \(F\) be an arbitrary number field, \(S\) the set of infinite and dyadic primes, \(C^S(F)\) the class group of the ring of \(S\)-integers and \(g_2(F)\) the number of dyadic places of \(F\). Then

\[
\text{rk}_2(K_2(o_F)) = r_1(F) + g_2(F) - 1 + \text{rk}_2(C^S(F)). \tag{5}
\]

If we combine the 2-rank formula with a result of Serre ([26], Prop. 30) we obtain

**Proposition 1.6.** If \(F\) is totally real, then \(2^{\text{rk}_2(K_2(o))}\) divides \(w_2(F)\zeta_F(-1)\).

We give a list of those families of number fields for which the 2-part of the Birch-Tate conjecture has been established up to now. Note that all these fields are abelian.
Theorem 1.7. The Birch-Tate conjecture holds for the fields

1) \( F = \mathbb{Q}(\sqrt{d}) \), where \( d = 2, p, \) or \( 2p, p \) a prime number congruent to \( \pm 3 \) mod 8. In this case, the 2-part of \( \# K_2(o) \) is equal to \( 2^2 \) [17].

2) \( F = \mathbb{Q}(\sqrt{d}) \), where \( d = p \cdot q \) with different primes \( p, q \equiv 3 \) mod 8 or \( d = p \) with a prime \( p \) of the form \( p = u^2 - 2u \), \( u > 0, u \equiv 3 \) mod 4, \( w \equiv 0 \) mod 4. Here \( (\# K_2(o))_2 = 2^3 \) [31].

3) \( F = \mathbb{Q}(\zeta_{2m})^+, \zeta_{2m} \) a primitive \( 2^m \)-th root of unity. \( (\# K_2(o))_2 = 2^{[F:Q]} \) [22].

4) \( F = \mathbb{Q}(\zeta_p)^+ \), where \( p \) is a prime number such that \( q = \frac{p-1}{2} \) is a prime having 2 as a primitive root. Here again \( (\# K_2(o))_2 = 2^{[F:Q]} \) [18].

We will add two classes of fields to this collection. Except for b), all of these fields have the property that the 2-Sylow-subgroup of \( K_2(o) \) is "small", i.e. elementary abelian and of 2-rank \( r_1(F) = [F : Q] \). Before we proceed into this direction we will consider values of zeta-functions of abelian fields and odd prime divisors of the order of \( K_2(o) \).
Chapter 2

Odd divisors of the order of $K_2(o)$

§2.1. Computation of $\zeta_F(-1)$

Now let $F$ be a—not necessarily totally real—abelian number field, $H$ its character group, and $\zeta_F$ its Dedekind zeta-function. For $\chi \in H$, let $f_\chi$ be its conductor, and let $L(s, \chi)$ be the Dirichlet $L$-series associated to $\chi$. For $n \in \mathbb{N}_0$, $\chi \in H$, the generalized Bernoulli polynomials $B_{n, \chi}(z)$ are defined by

$$
\sum_{t=1}^{f_\chi} \frac{\chi(t) \cdot a \cdot e^{(t+z)a}}{e^{f_\chi a} - 1} = \sum_{n=0}^{\infty} B_{n, \chi}(z)^{a_n}. 
$$

From these we obtain the generalized Bernoulli numbers $B_{n, \chi} := B_{n, \chi}(0)$. The ordinary Bernoulli polynomials $B_n(z)$ and numbers $B_n$ belong to the principal character $\chi \equiv 1$. We state the following well-known facts, see [19], [32]:

$$
\zeta_F(s) = \prod_{\chi \in H} L(s, \chi), 
$$

$$
L(-m, \chi) = -\frac{B_{m+1, \chi}}{m+1} \quad \forall m \in \mathbb{N}_0, 
$$

$$
B_{m+1, \chi} = \frac{f_\chi}{m+1} \sum_{t=1}^{f_\chi} \chi(t) B_{m+1} \left( \frac{t}{f_\chi} - 1 \right). 
$$

Putting $S_m(x) := \frac{1}{m+1} B_{m+1}(x - 1)$, we obtain

**Theorem 2.1.** ([17], Thm. 1) Let $F$ be an abelian number field with character group $H$. Then, for all $m \in \mathbb{N}_0$,

$$
\zeta_F(-m) = \frac{(-1)^{[F:Q]} B_{m+1} |d_F|^m}{m+1} \prod_{\chi \in H} \sum_{\chi \neq 1} \chi(t) S_m \left( \frac{t}{f_\chi} \right). 
$$
This result is essentially due to C. L. Siegel [27]. For the proof, note that $\zeta_q(-m) = \frac{B_{m+1}}{m+1}$ is the factor belonging to the principal character, and use the conductor-discriminant formula $|d_F| = \prod_{\chi \in \mathcal{H}} f_\chi$. Observe that $\zeta_F(-m) = 0$ unless $F$ is totally real.

Now let $F$ be totally real abelian with $[F: Q] = n$ and consider the special case $m = 1$: We have $B_2 = \frac{1}{6}$, $B_2(x) = x^2 + x + \frac{1}{6}$, hence $S_1(x) = \frac{1}{2} x(x - 1) + \frac{1}{12}$. Now $\sum_{t=1}^{f_\chi} \chi(t) = 0$ for every nontrivial character $\chi$, furthermore $d_F > 0$, thus

$$\zeta_F(-1) = \frac{(-1)^n}{12} \frac{d_F}{2^{n-1}} \prod_{\chi \in \mathcal{H}} \frac{f_\chi}{2} \sum_{t=1}^{f_\chi} \chi(t) \frac{1}{f_\chi} \left( \frac{t}{f_\chi} - 1 \right),$$

hence, using the conductor-discriminant-formula once again,

$$\zeta_F(-1) = \frac{(-1)^n}{12 \cdot 2^{n-1} \cdot d_F} \prod_{\chi \in \mathcal{H}} \sum_{t=1}^{f_\chi} \chi(t) t (t - f_\chi). \quad (6)$$

§2.2. Large divisors of the order of $K_2(o)$

We will use this formula in the next few paragraphs to obtain conditions on odd primes dividing $\#K_2(o)$. First we prove

**Theorem 2.2.** Let $F$ be a cyclic subfield of $Q(\zeta_m)^+$, $m \in \mathbb{N}$, with $[F: Q] = n$, $o$ its ring of integers. Let $\ell$ be an odd prime number with

(i) $(\ell, mn) = 1,$

(ii) $\ell \nmid \#K_2(o),$

(iii) $\ell \mid \#K_2(o_E)$ for any proper subfield $E$ of $F$.

Then $\ell \equiv 1 \pmod{n}$.
Proof. We have \( \ell \mid \#K_2(o) \) if and only if \( \ell \mid \omega_2(F)_{\ell}(\omega_1) \). By assumption, \( \ell \mid m \), hence 
\( \ell \mid \omega_2(F)_{\ell} \). Considering (6) and writing 
\( S_\chi := \sum_{t=1}^{f_\chi} \chi(t) t (t - f_\chi) \) we obtain

\[
\ell \mid \#K_2(o) \iff \ell \mid \prod_{\chi \in H} S_\chi.
\]

Denote by \( \tilde{H} \) the set of all \( \chi \in H \) having order \( n \), thus \( \chi \in \tilde{H} \) if and only if \( \chi \) does not belong to any proper subgroup of \( H \). Observe that all \( \chi \in \tilde{H} \) have the same conductor. Splitting up the product

\[
\prod_{\chi \in H} S_\chi = \prod_{\chi \in \tilde{H}} S_\chi \prod_{\chi \not\in \tilde{H}} S_\chi
\]

we see that

\[
\ell \mid \prod_{\chi \in \tilde{H}} S_\chi,
\]

since otherwise \( \ell \) would divide \( \#K_2(o_E) \) for some proper subfield \( E \) of \( F \), contrary to the assumption. Now we claim

\[
\prod_{\chi \in \tilde{H}} S_\chi = N S_\psi
\]

for any fixed \( \psi \in \tilde{H} \), where \( N \) denotes the norm of \( K := Q(\zeta_n) \) over \( Q \). To see this, fix \( \psi \in \tilde{H} \) and consider the map

\[
\eta: G = Gal(K/Q) \rightarrow \tilde{H}
\]

\[\sigma \mapsto \sigma \psi\]

where \( \sigma \psi \) is the character defined by \( (\sigma \psi)(t) := \sigma(\psi(t)), t \in Gal(F/Q) \). It is clear that \( \eta \) is well defined and that the order of \( \sigma \psi \) is again \( n \) for all \( \sigma \in G \). \( \eta \) is also injective: If \( \sigma \psi = r \psi \) 
for \( \sigma, r \in G \), then \( \sigma(\psi(g)) = r(\psi(g)) \) for a generator \( g \) of the cyclic group \( Gal(F/Q) \). Since the order of \( \psi \) is \( n \), \( \psi(g) \) is a primitive \( n \)-th root of unity, hence \( \sigma(z) = r(z) \) for all \( z \in K \), i.e.
\[ \sigma = \tau. \] Since \( \#H = \phi(n) = \#G \), \( \eta \) is even bijective. Therefore

\[
\prod_{\chi \in \tilde{H}} S_{\chi} = \prod_{\chi \in \tilde{H}} \sum_{t=1}^{f_{\chi}} \chi(t) t (t - f_{\chi})
\]

and (9) follows. Hence, by (8), \( \ell \parallel N S_{\chi} \) for any fixed \( \chi \in \tilde{H} \). Now let \( \varphi \) be a prime divisor of \( \ell \) in \( \mathbb{Q}(\tau_n) \). Then \( \varphi \parallel N S_{\chi} \) for some \( \chi \in \tilde{H} \), since otherwise \( \varphi \not\parallel N S_{\chi} \) in contradiction to \( \varphi \parallel \ell \) and \( \ell \parallel N S_{\chi} \). Hence \( N \varphi \parallel N S_{\chi} \). Since \( N \varphi = \ell^f \), where \( f \) is the inertial degree of \( \ell \) over \( K = \mathbb{Q}(\tau_n) \), we arrive at \( f = 1 \). By assumption, \( \ell \) is unramified in \( K \), hence \( \ell \) is totally decomposed in \( K \).

Consequently, \( \ell \equiv 1 \mod n. \)

\[ \square \]

**Remarks.** (i) In the case \( m = p \), a prime number, condition (i) can be weakened to \( (\ell, n) = 1 \):

If \( (\ell, p) \neq 1 \), i.e. \( \ell = p \), the conclusion \( \ell \equiv 1 \mod n \) of the theorem holds trivially. We do not know if the condition \( (\ell, m) = 1 \) is actually necessary if \( m \) is not prime.

(ii) None of the other conditions imposed on \( \ell \) can be omitted: For \( (\ell, n) \neq 1 \), i.e. \( \ell \parallel n \), see the next section. For \( \ell^2 \parallel \#K_2(o) \), observe the divisor \( \ell^2 \) of \( \#K_2(o) \), \( F = \mathbb{Q}(\tau \gamma) \). As for condition (iii) of Theorem 2.2, we give the counterexample \( p = 31, n = 15, \ell = 7. \)

§2.8. Small divisors of the order of \( K_2(o) \)

Condition (i) of Theorem 2.2 implies that \( \ell \) is "large", at least \( \ell > n \). So the natural question arises how the "small" divisors of \( \#K_2(o) \) might look like. A result into this direction can be obtained if we narrow our attention to subfields \( F \) of \( \mathbb{Q}(s_p)^{\dagger} := \mathbb{Q}(s_p + s_p^{-1}) \), \( p \) being
an odd prime number. As before, let $[F : \mathbb{Q}] = n$, $d_F$ the discriminant of $F$, $H$ its character group, and let $\mathfrak{o}$ be the ring of integers in $F$. Then $F$ is a cyclic extension of $\mathbb{Q}$, every character in $H$ has conductor $p$, hence $d_F = p^{n-1}$. With (4) and (6) we obtain

$$|w_2(F) \cdot \varepsilon_F(-1)| = \frac{2p^\delta}{(2p)^{n-1}} \prod_{\chi \in H} \sum_{t=1}^{p-1} \chi(t) t (t - p),$$

where $\delta := 1$ if $n = (p - 1)/2$ and 0 otherwise. Let $S_\chi = \sum_{t=1}^{p-1} \chi(t) t (t - p)$.

**Theorem 2.8.** Let $F$ be a subfield of $\mathbb{Q}(z_p)^+$, $p$ prime, and let $\mathfrak{o}$ be its ring of integers.

(i) If $q \geq 5$ is a prime number dividing $[F : \mathbb{Q}]$, then $q$ divides $\#K_2(\mathfrak{o})$.

(ii) If $3^2$ divides $p - 1$ and 3 divides $[F : \mathbb{Q}]$, then 3 divides $\#K_2(\mathfrak{o})$.

**Proof.** By (2) and (10) we have

$$q \mid \#K_2(\mathfrak{o}) \iff q \mid \prod_{\chi \in H, \chi \neq 1} \sum_{t=1}^{p-1} \chi(t) t (t - p) = \prod_{\chi \in H, \chi \neq 1} S_\chi.$$  

Hence it is enough to show the claim for the subfield $F$ of $\mathbb{Q}(z_p)^+$ with $[F : \mathbb{Q}] = q$. Observe that $q$ divides $p - 1$. Since the order of $H$ is $q$, $S_\chi \in \mathbb{Z}[z_q]$ for all $\chi \in H$. Furthermore observe that

$$\sum_{t=1}^{p-1} t (t - 1) = \sum_{t=1}^{p-1} t^2 - \sum_{t=1}^{p-1} t = \frac{p(p - 1)(2p - 1)}{6} - \frac{p(p - 1)}{2},$$

hence $q \mid \sum_{t=1}^{p-1} t (t - 1)$ if $q \geq 5$ and $3 \mid \sum_{t=1}^{p-1} t (t - 1)$ if $3^2 \mid p - 1$. Now consider congruences in $\mathbb{Z}[z_q]$. Fix $\chi \in H, \chi \neq 1$. With $p = kq + 1$ for some $k \in \mathbb{N}$ we obtain

$$\chi(t) t (t - p) = \chi(t) t (t - 1) - \chi(t) t k q,$$
hence
\[
S_X = \sum_{t=1}^{p-1} \chi(t) t (t - p) = \sum_{t=1}^{p-1} \chi(t) t (t - 1)
\]
\[
= \sum_{t=1}^{p-1} \chi(t) t (t - 1) - \sum_{t=1}^{p-1} t (t - 1)
\]
\[
= \sum_{t=1}^{p-1} (\chi(t) - 1) t (t - 1) \pmod q.
\]

Now \( \sigma_q - 1 \mid \chi(t) - 1, 1 \leq t \leq p - 1 \), and \( \sigma_q - 1 \mid q \), hence \( \sigma_q - 1 \mid S_X \) for all \( \chi \in H \). Therefore
\[
(\sigma_q - 1)^{q-1} \mid \prod_{\chi \in H \atop \chi \neq 1} S_X.
\]

Since \( (\sigma_q - 1)^{q-1} = (q) \) as ideals and since \( \prod_{\chi \in H \atop \chi \neq 1} S_X \in \mathbb{Z} \), we obtain
\[
g \mid \prod_{\chi \in H \atop \chi \neq 1} \sum_{t=1}^{p-1} \chi(t) t (t - p),
\]
and we are done by (11). \( \square \)

§2.4. Irregular primes and \( K_2(o) \)

Let \( E := \mathbb{Q}(\sigma_p) \), \( F := \mathbb{Q}(\sigma_p)^+ \), and \( o, o^+ \) their rings of integers. Let \( Cl, Cl^+ \) be their class groups, respectively, and denote by \( h \) and \( h^+ \) their class numbers, i.e. \( h = \# Cl \), and \( h^+ = \# Cl^+ \). Furthermore, let \( h^- := h/h^+ \), the relative class number.

Definition 2.4. A prime number \( p \) is irregular if \( p \) divides \( h \), the class number of \( \mathbb{Q}(\sigma_p) \).
The first five irregular primes are 37, 59, 67, 101, 103. It is a famous theorem of Kummer that \( p \) is irregular if and only if \( p \) divides the numerator of at least one of the Bernoulli numbers \( B_2, B_4, \ldots, B_{p-3} \), see [32]. Another noteworthy property of irregular primes is

**Theorem 2.4. (Kummer)** \( p \mid h \iff p \mid h^-. \)

Vandiver conjectured that \( p \) never divides \( h^+ \). There is an interesting analogue in terms of \( K \)-groups, but with a different outcome. The following result has been proved independently by S. Chaladus [7] and F. Keune [20].

**Theorem 2.5.** \( p \) is irregular \( \iff p \mid \#K_2(\mathcal{O}). \)

Keune observed that Theorem 2.5 holds even if we replace \( \mathcal{O} \) by \( \mathcal{O}^+ \). He used a \( p \)-rank formula that is analogous to the formula (5) for the 2-rank of \( K_2(\mathcal{O}) \). We choose a different approach and use a special case of a result of K. Brown ([5], Cor. to Prop. 8).

**Theorem 2.6.** Let \( p \) be an odd prime. Then the power of \( p \) dividing the denominator of \( \zeta_F(-1) \) is the same as the power of \( p \) dividing the denominator of \( h^-/p \).

**Corollary 2.7.** \( p \) is irregular \( \iff p \mid \#K_2(\mathcal{O}^+). \)

**Proof.** In view of (2) we have \( p \mid \#K_2(\mathcal{O}^+) \) if and only if \( p \mid w_2(F)\zeta_F(-1) \). Here \( w_2(F) = 24p \), see (4). We may assume \( p \geq 5 \). By Theorem 2.6,

\[
p \mid \#K_2(\mathcal{O}) \iff p \mid 24h^- \iff p \text{ is irregular}.
\]
Let us summarize these few observations in a sequence of equivalences.

\[ p \text{ is irregular } \iff p \mid h \]

\[ \iff p \mid h^- \]

\[ \iff p \mid B_{2i}, \text{ some } 1 \leq i \leq \frac{p^3 - 8}{2} \]

\[ \iff p \mid \#K_2(o) \]

\[ \iff p \mid \#K_2(o^+) \]
§8.1. Prerequisites for the proofs

The main result of this chapter is the proof of the Birch-Tate conjecture for two families of totally real abelian number fields, namely for $\mathbb{Q}(\zeta_{3^k})^+$ and for $\mathbb{Q}(\zeta_{3^p})^+$, where $p$ is a prime number satisfying certain conditions. The proofs are based on the following results.

**Theorem 8.1.** ([18], Thm. B) Let $F$ be a totally real subfield of $\mathbb{Q}(\zeta_m)$, $m$ odd. If $2^{[F:\mathbb{Q}]} \mid w_2(F)\zeta_p(-1)$, the following statements are equivalent:

(i) The 2-part of the Birch-Tate conjecture holds.
(ii) The relative class number of $F(i)$ over $F$ is odd.
(iii) The signatures of a system of fundamental units of $F$ at the real primes are independent.

In the special case $F = \mathbb{Q}(\zeta_p^m)^+$, $p$ an odd prime, these statements are also equivalent to
(iv) The relative class number $h^-$ of $\mathbb{Q}(\zeta_p^m)$ over $\mathbb{Q}(\zeta_p^m)^+$ is odd.

We will use Theorem 3.1 to prove the Birch-Tate conjecture for the totally real subfields of $\mathbb{Q}(\zeta_{3^k}), k \in \mathbb{N}$. If $m$ is even, this theorem cannot be applied, and we need to resort to two lemmas.

**Lemma 8.2.** (Weak Lemma) Let $F$ be totally real, $E := F(i)$, and assume that $E$ has only one dyadic prime and that the class number $h$ of $E$ is odd. Then the 2-Sylow-subgroup of $K_2(\mathbb{Q}_p)$ is elementary abelian.
This is a weak version of [18], Lemma 4. It is well known that in the case $E = \mathbb{Q}(\zeta_n), n \in \mathbb{N}$, $h$ is odd if and only if $\sqrt{-1}$ is odd (Kummer, see [32], Thm. 10.2). The next lemma is an application of the 2-rank formula for $K_2(o)$.

**Lemma 8.8.** Let $F$ be totally real. If the 2-Sylow-subgroup of $F$ is elementary abelian and if $2^{[F:Q]} \mid w_2(F)\zeta_F(-1)$, then the Birch-Tate conjecture holds for $F$.

**Proof.** Recall the 2-rank formula (5), which is valid for any number field. If $F$ is totally real, $r_1(F) = [F : Q]$, hence $\text{rk}_2(K_2(o_F)) \geq [F : Q]$. By Proposition 1.6, $2^{\text{rk}_2(K_2(o_F))}$ divides $w_2(F)\zeta_F(-1)$. Hence, by assumption, $\text{rk}_2(K_2(o_F)) \leq [F : Q]$, hence $\text{rk}_2(K_2(o_F)) = [F : Q]$. Since the 2-Sylow-subgroup of $K_2(o_F)$ is elementary abelian,

$$\#(K_2(o_F))_2 = 2^{[F:Q]} = (w_2(F)\zeta_F(-1))_2.$$  

\[\square\]

§8.2. The Birch-Tate conjecture for two families of abelian number fields

First we show that $2^{[F:Q]} \mid w_2(F)\zeta_F(-1)$ for the totally real subfields $F$ of the cyclotomic fields $\mathbb{Q}(\zeta_k), k \in \mathbb{N}$. Then we prove condition (iv) of Theorem 3.1 for these fields.

**Theorem 8.4.** If $F = \mathbb{Q}(\zeta_k)^+, k \geq 1$, then $2^{[F:Q]} \mid w_2(F)\zeta_F(-1)$.

**Proof.** Taking into consideration that the characters of $F$ are even, (6) yields

$$|w_2(F)\zeta_F(-1)| = \frac{3^{k-1}}{d_F} \prod_{\chi \in H} \sum_{t=1}^{2} \chi(t) \tau(t - f_X),$$

where $d_F$ is the discriminant of $F$. For $F = \mathbb{Q}(\zeta_k)^+$, $d_F = 1$, and the result follows.

\[\square\]
where \( d_F \) is some power of 3 and \( |H| = [F : Q] = 3^k-1 \). So it is enough to show that every

\[
S_\chi = \sum_{t=1}^{f_\chi-1} \chi(t) (t - f_\chi), \quad \chi \in H - \{1\},
\]

is divisible by 2 but not by \( 2^2 \). Since the fields \( Q(\zeta_{3^k}), k \geq 1 \), form a tower of fields of relative degrees 3 we can use induction on \( k \). The induction starts for \( k = 1, 2 \) (see Table 2).

The characters \( \chi \) that do not belong to any proper subfield of \( F \) are exactly the ones having conductor \( f_\chi = 3^k \) and order \([F : Q]\) in \( H \). Since the \( S_\chi \) for these \( \chi \) are conjugate in \( Q(\zeta_{3^k-1}) \), it is sufficient to show \( 2 \| S_\chi \) for one \( \chi \) that generates \( H \).

For any prime power \( p^k, p \neq 2 \), a generator \( \psi \) for the character group of \( Q(\zeta_{p^k}) \) can be obtained as follows: Let \( g \) be a primitive root mod \( p^k \) and consider

\[
\psi : \text{Gal}(Q(\zeta_{p^k})/Q) \rightarrow (\mathbb{Z}/p^k)^* \rightarrow (\mathbb{Z}/\phi(p^k))^*, \quad \phi(S_{p^k}) \rightarrow \mathbb{C}
\]

Here \( \psi \) is the automorphism of \( Q(\zeta_{p^k}) \) that sends \( \zeta_{p^k} = e^{2\pi i/p^k} \) to \( \zeta_{p^k}^m \). Call the map in the middle \( \psi \) again. \( \psi^2 \) will be a generator for the character group of \( Q(\zeta_{p^k})^* \).

Let \( \chi := \psi^2 \) and pick \( g = 2 \). Then \( \psi(2^m \mod 3^k) = m \mod \phi(3^k) \)

\[
S_{\chi} = \sum_{t=1}^{3^k-1} \chi(t) (t - 3^k) \in Q(\zeta_{3^k-1}).
\]

As written down, the sum \( S_{\chi} \) has exactly \( 3^k-1 \) nonzero terms since \( \chi(t) = 0 \) if and only if \( t \) is divisible by 3. Let \( \zeta := \zeta_{3^k-1} \). Choose the basis \( 1, \zeta, \zeta^2, \ldots, \zeta^{3^k-2} \) for \( Q(\zeta_{3^k-1}) \) and apply the relations

\[
\zeta^i + \zeta^i + 3^k - 2 + \zeta^i + 2 \cdot 3^k - 2 = 0, \quad 0 \leq i \leq 3^k - 2 - 1.
\]
in order to make the coefficients of $s^{2 \cdot 3^k - 2}, \ldots, s^{3^{k-1} - 1}$ in $S_X$ vanish. Since 2 is a primitive root of $3^{k-1}$, 2 is inert in $\mathbb{Q}(\zeta_{3^k-1})$. Hence it is sufficient to show that after this procedure there is at least one coefficient congruent to 2 modulo 4. Consider the partial sum of $S_X$

$$a_1 + a_2 s^{3^k-2} + a_3 s^{2 \cdot 3^k - 2} = (a_1 - a_3) + (a_2 - a_3) s^{3^k-2},$$

where $a_i = t_i (t_i - 3^k)$ for some $t_i$, $i = 1, 2, 3$. The $a_i$ are even, and it is enough to show that any two of them are incongruent mod 4. In view of (13) we have to find $t_1, t_2, t_3$, $1 \leq t_i \leq \frac{3^k - 1}{2}$, such that

$$\begin{align*}
\chi(t_1) &\equiv 0 \\
\chi(t_2) &\equiv 3^{k-2} \\
\chi(t_3) &\equiv 2 \cdot 3^{k-2}
\end{align*} \mod 3^{k-1},$$

i.e. such that

$$\begin{align*}
t_1 &\equiv 2^0 \\
t_2 &\equiv 2 \cdot 3^{k-2} \\
t_3 &\equiv 2^2 \cdot 3^{k-2}
\end{align*} \mod 3^k.\]$$

Obviously $t_1 = 1$. Since 2 is a primitive root mod $3^{k-1}$ and $3^k$, $2^{3^k-2} \equiv -1 \mod 3^{k-1}$, but $2^{3^k-2} \not\equiv -1 \mod 3^k$, hence

$$\begin{align*}
either a) &\quad 2^{3^k-2} \equiv 3^{k-1} - 1 \\
or b) &\quad 2^{3^k-2} \equiv 2 \cdot 3^{k-1} - 1
\end{align*} \mod 3^k.\]$$

(15)

First we discuss case a), i.e. $t_2 = 3^{k-1} - 1$. If $k$ is even, then $3^k \equiv 1(4)$ and $3^{k-1} \equiv 3(4)$, hence $a_1 = 1 - 3^k \equiv 0(4)$ and $a_2 = (3^{k-1} - 1)(3^{k-1} - 1 - 3^k) \equiv 2(4)$. If $k$ is odd, then $3^k \equiv 3(4)$ and $3^{k-1} \equiv 1(4)$, hence $a_1 \equiv 2(4)$ and $a_2 \equiv 0(4)$. For case b) observe that $2^{2 \cdot 3^{k-2}} \equiv (2 \cdot 3^{k-1} - 1)^2 \equiv 1 - 3^{k-1} \mod 3^k$. Since $\chi(1 - 3^{k-1}) = \chi(3^{k-1} - 1)$, it follows that $t_3 = 3^{k-1} - 1$. Now do the same proof as in case a) to show that $a_1, a_3$ are incongruent mod 4.

□

Our next theorem provides the second step for the proof of the Birch-Tate conjecture for the totally real subfields of $\mathbb{Q}(\zeta_{3^k})$. Moreover, it is of independent interest and is an analogue to a classical result of Weber ([14], [33]) on the class numbers of the fields $\mathbb{Q}(\zeta_{3^k})$. 
Theorem 8.5. The relative class numbers $h^- = h/h^+$ of the cyclotomic fields $\mathbb{Q}(\zeta_{3^k})$ are odd.

Proof. Recall that for any cyclotomic field $E = \mathbb{Q}(\zeta_m)$

$$h^-(E) = Q w \prod_{\chi \text{ odd}} \left( -\frac{1}{2} B_{1,\chi} \right),$$

(16)

see [32], Thm. 4.17. Here $Q = 1$ if $m$ is a prime power, 2 otherwise, and $w$ is the number of roots of unity in $E$, hence in our case $w = 2 \cdot 3^k$. For every $\chi \neq 1$, $B_{1,\chi} = \frac{1}{f_{\chi}} \sum_{t=1}^{f_{\chi}} \chi(t) t$, so

$$h^-(\mathbb{Q}(\zeta_{3^k})) = 2 \cdot 3^k \prod_{\chi \text{ odd}} \frac{f_{\chi}}{2f_{\chi}} \sum_{t=1}^{f_{\chi}} \chi(t) t.$$ 

Hence it is enough to show that the $f_{\chi} B_{1,\chi}$ are exactly divisible by 2—with one exception. Proceed by induction on $k$. The exception is easy to spot: It is the quadratic character $\chi_0 = (\frac{\cdot}{3})$ belonging to $\mathbb{Q}(\zeta_3)$, and $B_{1,\chi_0} = \sum_{t=1}^{3} (\frac{t}{3}) t = -1$. Now consider the characters of $E$ that do not belong to any proper subfield. These are exactly the generators of the character group of $E$. For these characters $\chi$, the $B_{1,\chi}$ are conjugate in $E$. So it is enough to show the claim for one particular generator $\chi$. Let $\chi = \psi$, the character defined in (12), i.e.

$$\chi(2^m \mod 3^k) = m \quad (\text{mod } 2 \cdot 3^{k-1}).$$

We want to show that $B_{1,\chi}$, rewritten in the basis $1, \zeta_{3^k-1}, \ldots, \zeta_{3^k-1}^{2 \cdot 3^{k-2}-1}$, has at least one coefficient congruent to 2 mod 4. We proceed in the spirit of the proof of Theorem 3.4. To obtain a unique basis representation of $B_{1,\chi}$ in $\mathbb{Q}(\zeta_{3^k-1})$, first use the relations

$$\zeta_{2 \cdot 3^{k-1}}^i = -\zeta_{2 \cdot 3^{k-1}}^{i+3^{k-1}}, 0 \leq i \leq 3^{k-1} - 1,$$

then the equations

$$\zeta_{2 \cdot 3^{k-1}}^{2i} + \zeta_{2 \cdot 3^{k-1}}^{2(i+3^{k-2})} + \zeta_{2 \cdot 3^{k-1}}^{2(i+2 \cdot 3^{k-2})} = 0, 0 \leq i \leq 3^{k-2} - 1.$$

In order to produce the desired coefficient congruent to 2 mod 4, consider the above relation
for \( i = 0 \). So we need to find \( t_1, t_2, t_3 \) with
\[
\begin{align*}
\chi(t_1) &\equiv 0 \\
\chi(t_2) &\equiv 2 \cdot 3^k - 2 \\
\chi(t_3) &\equiv 4 \cdot 3^k - 2 \\
\end{align*}
\mod 2 \cdot 3^k - 1,
\]
\[
\equiv 3^k - 1 + 3^k - 2
\]
and in view of the first relation \( \zeta_{2,3}^i \equiv -3^{k-1+i} \), find \( s_1, s_2, s_3 \) with
\[
\begin{align*}
\chi(s_1) &\equiv 3^k - 1 \\
\chi(s_2) &\equiv 3^k - 1 + 2 \cdot 3^k - 2 \\
\chi(s_3) &\equiv 3^k - 1 + 4 \cdot 3^k - 2 \\
\end{align*}
\mod 2 \cdot 3^k - 1,
\]
\[
\equiv 3^k - 2
\]
Since \( \chi \) is odd, we have \( t_i = 3^k - s_i, i = 1, 2, 3 \), and the coefficients \( a_i \) in the partial sum
\[
a_1 + a_2 \zeta_{2,3}^k - 2 + a_3 \zeta_{2,3}^k - 1
\]
of \( B_1, \chi \) are \( a_i = t_i - s_i = 3^k - 2s_i, i = 1, 2, 3 \). Now discuss the cases a) and b) given by (15).

In case a) we have \( s_3 = 3^k - 1 \), and since \( 2^{3^k - 1} \equiv -1 \mod 3^k \), we obtain
\[
2^{3^k - 1 + 2 \cdot 3^k - 2} \equiv -(2^{3^k - 2})^2 \equiv -(3^k - 1)^2 \equiv 2 \cdot 3^k - 1 \mod 3^k,
\]
I.e. \( s_2 = 2 \cdot 3^k - 1 - 1 \). If \( k \) is even, then \( a_2 = 3^k - 2(2 \cdot 3^k - 1 - 1) \equiv 3(4) \) and \( a_3 = 3^k - 2(3^k - 1 - 1) \equiv 1(4) \), hence \( a_2 - a_3 \equiv 2(4) \). If \( k \) is odd, then \( a_2 \equiv 1(4) \) and \( a_3 \equiv 3(4) \), hence again \( a_2 - a_3 \equiv 2(4) \). In case b) \( s_3 = 2 \cdot 3^k - 1 \), hence \( s_2 = 3^k - 1 - 1 \), and we can proceed as in case a), just interchanging \( a_2 \) and \( a_3 \).

Now we can put things together and apply Theorem 3.1 with \( m = 3^k \). We obtain the first main result of this chapter.
Theorem 8.6. The Birch-Tate conjecture holds for the fields $\mathbb{Q}(\zeta_{3^k})^+$, $k \in \mathbb{N}$.

As a corollary we can note that the fields $\mathbb{Q}(\zeta_{3^k})^+$ admit systems of fundamental units having independent signatures at the real places. This again is analogous to Weber's result on the cyclotomic fields $\mathbb{Q}(\zeta_{3^k})$.

The next family of number fields for which we want to verify the Birch-Tate conjecture is closely related to the fields of Theorem 1.7, case 4). Since our proof relies on this result, we state it again for easier reference.

Theorem 8.7. Let $p$ and $q = \frac{p-1}{2}$ be odd primes and assume that 2 is a primitive root mod $q$. Then the 2-primary part of the Birch-Tate conjecture holds for the field $\mathbb{Q}(\zeta_p)^+$.

The proof makes use of Theorem 3.1. We want to extend this result to the fields $\mathbb{Q}(\zeta_{4p})^+$, where $p$ is a prime number as above. As it turns out, we need to impose one more condition on $p$, namely that $p$ be congruent to 3 mod 8. As a preparation for the proof, we state two lemmas.

Lemma 8.8. Let $\chi$ be a character with conductor $f\chi = 4m$, $m$ odd.

(i) If $\chi$ is odd, then $\chi(t) = \chi(2m-t)$, $1 \leq t < m$.

(ii) If $\chi$ is even, then $\chi(t) = -\chi(2m-t)$, $1 \leq t < m$.

(iii) In either case, $\chi(t) = -\chi(2m + t)$, $1 \leq t < 2m$.

Proof. (i) $\chi = \chi_m \cdot \chi_4$, where $\chi_m$ is an even character with conductor $m$ and $\chi_4$ is the (odd) nontrivial character mod 4, i.e. $\chi_4(1) = 1$, $\chi_4(3) = -1$. Observe that $\chi(t) = 0$ for even $t$. If $t \equiv 1(4)$ then so is $2m-t$, and $\chi(t) = \chi_m(t) = \chi_m(2m-t) = \chi(2m-t)$. If $t \equiv 3(4)$, then so is $2m-t$, and $\chi(t) = -\chi_m(t) = -\chi_m(2m-t) = \chi(2m-t)$.
(ii) \( \chi = \chi_m \cdot \chi_{4m} \), where \( \chi_m \) is an odd character with conductor \( m \). If \( t \equiv 1(4) \), then \( \chi(t) = \chi_m(t) = -\chi_m(2m-t) = -\chi(2m-t) \). If \( t \equiv 3(4) \), then \( \chi(t) = -\chi_m(t) = \chi_m(2m-t) = -\chi(2m-t) \).

(iii) follows from (i), (ii), since

\[
\chi(2m+t) = \begin{cases} 
\chi(2m-t) & \text{if } \chi \text{ is even} \\
-\chi(2m-t) & \text{if } \chi \text{ is odd.}
\end{cases}
\]

We will apply this lemma in order to prove the following result on generalized Bernoulli numbers.

**Lemma 8.9.** Let \( \chi \) be a character of conductor \( 4m, m \) odd.

(i) If \( \chi \) is odd, then \( B_{1,\chi} = - \sum_{t=1 \atop t \text{ odd}}^{m-1} \chi(t) \).

(ii) If \( \chi \) is even, then \( B_{2,\chi} = 2 \sum_{t=1 \atop t \text{ odd}}^{m-1} \chi(t) (m-t) \).

**Proof.** (i) Recall that \( B_{1,\chi} = \frac{1}{f_\chi} \sum_{t=1} f_\chi \chi(t) t \) for any character \( \chi \neq 1 \). Hence, in our case,

\[
4mB_{1,\chi} = \sum_{t=1}^{4m} \chi(t) t = \sum_{t=1}^{2m} \chi(t) t + \sum_{t=1}^{2m} \chi(2m-t) (2m+t) = \sum_{t=1}^{2m} \chi(t) t - \sum_{t=1}^{2m} \chi(t) (2m+t) = -2m \sum_{t=1}^{2m} \chi(t) \cdot
\]
Therefore
\[-2B_{1,\chi} = \sum_{t=1}^{m} \chi(t) + \sum_{t=1}^{m} \chi(2m-t)\]
\[= 2 \sum_{t=1}^{m} \chi(t).\]

Now observe that \(\chi(t) = 0\) if \(t\) is even or if \(t = m\). The claim follows.

(ii) For any even character \(\chi \neq 1\), \(B_{2,\chi} = \frac{1}{f_{\chi}} \sum_{t=1}^{f_{\chi}} \chi(t) t^2\), hence in this case,

\[4mB_{2,\chi} = \sum_{t=1}^{4m} \chi(t) t^2\]
\[= \sum_{t=1}^{2m} \chi(t) t^2 + \sum_{t=1}^{2m} \chi(2m+t)(2m+t)^2\]
\[= \sum_{t=1}^{2m} \chi(t)(t^2 - (2m+t)^2)\]
\[= -4m \sum_{t=1}^{2m} \chi(t)(m+t).\]

Therefore
\[-B_{2,\chi} = \sum_{t=1}^{m} \chi(t) (m+t) + \sum_{t=1}^{m} \chi(2m-t)(3m-t)\]
\[= -2 \sum_{t=1}^{m} \chi(t) (m-t),\]

and (ii) follows. \(\square\)

Now we proceed in a similar fashion as we did with the fields \(Q(\zeta_{3k})\), i.e. we will deal with \(\zeta_p(-1)\) and relative class numbers again. Lemma 3.9 will provide us with the necessary summation techniques.

**Theorem 8.10.** Let \(p\) be a prime number congruent to 3 modulo 8 such that \(q = \frac{p-1}{2}\) is a prime number having 2 as a primitive root. Let \(F = Q(\zeta_{3p})^+.\) Then \(2^{[F:Q]} \mid w_2(F)\zeta_p(-1).\)
Proof. Recall that \( L(-1, \chi) = \prod_{\chi \in H} L(-1, \chi) \), where \( H \) is the character group of \( \mathbb{F} \). Furthermore, \( L(-1, \chi) = -\frac{1}{2} B_{2, \chi} \). Observe that \( w_2(\mathbb{F}) = 24p \) and \( B_{2, 1} = B_2 = \frac{1}{6} \). Hence

\[
|w_2(\mathbb{F}) L(-1)| = 2p \prod_{\chi \in H, \chi \neq 1} \frac{1}{2} B_{2, \chi}.
\]

Since \( \#H = [\mathbb{F} : \mathbb{Q}] \), it is enough to show that \( 2^2 \mid B_{2, \chi} \) for all \( \chi \in H, \chi \neq 1 \). \( \mathbb{F} \) has exactly 2 nontrivial subfields, namely \( \mathbb{Q}(\sqrt{ap}) = \mathbb{Q}(\sqrt{p}) \) and \( \mathbb{Q}(wp)^\perp \). Let \( \chi \in H \). We have 3 cases.

(1) \( \chi \) is the quadratic character belonging to \( \mathbb{Q}(\sqrt{p}) \). It has been shown in [15], Thm. 5, that

\[ B_{2, \chi} \equiv 4(8). \]

(2) \( \chi \) is a character of \( \mathbb{Q}(wp)^\perp \). This case has been handled in the proof of Theorem 3.7, see [18]. Again, \( B_{2, \chi} \equiv 4(8) \).

(3) \( \chi \) does not belong to any proper subfield of \( \mathbb{F} \), i.e. \( \chi \) is an even character with conductor \( f_\chi = 4p \). It remains to be proved that \( 2^2 \mid B_{2, \chi} \) for these \( \chi \).

Applying Lemma 3.9 we obtain

\[ B_{2, \chi} = 2 \sum_{t=1}^{p-1} \chi(t)(p-t) \in \mathbb{Q}(s_q). \]

Let \( S_\chi = \frac{1}{2} B_{2, \chi} \). Since 2 is inert in \( \mathbb{Q}(s_q) \), it is enough to show that \( S_\chi \), in unique basis representation, has at least one coefficient congruent to 2 mod 4. Since \( \chi = \chi_p \cdot \chi_4 \), where \( \chi_p \) is a generator of the character group of \( \mathbb{Q}(s_p) \). It is clear that the \( \chi(t) \), \( 1 \leq t < p \), \( t \) odd, are different powers of \( s_q = e^{2\pi i/q} \), with minus signs attached to those \( \chi(t) \) with \( t \equiv 3(4) \). Take the basis \( \pm s_q, \ldots, \pm s_q^{q-1} \) of \( \mathbb{Q}(s_q) \), where the signs are chosen appropriately. Then

\[ S_\chi = \sum_{t=3}^{p-1} \chi(t)((p-t) \pm (p-1)), \]

i.e. the coefficient of \( \chi(3) \) is either \( 2(p-2) \) or \( -2 \). Hence \( 2 \mid S_\chi \), and consequently \( 2^2 \mid B_{2, \chi} \).

This completes the proof. \( \Box \)

Remarks. (i) The condition \( p \equiv 3 \mod 8 \) is actually necessary, as the examples \( p = 7, 23 \) show.

Note, though, that we need this condition only for case (1).
(ii) Under the assumptions of the theorem, the statement $p \equiv 3(8)$ is equivalent to: 2 is a primitive root of $p$. Furthermore it follows that $p \equiv 11(16)$: If 2 is a primitive root mod $p$, then $2^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{2}{p}\right) \mod p$, by Euler's criterion, hence $p \equiv \pm 3(8)$. It is impossible that $p \equiv -3(8)$ since $q = \frac{p-1}{2}$ is odd. Conversely, if $p \equiv 3(8)$, then $2^q \equiv -1(p)$, again by Euler's criterion. Since $q$ is prime, the order of 2 mod $p$ is $p - 1$. Since 2 is a primitive root mod $q$, $q \equiv \pm 3(8)$, hence $p \equiv 7, 11(16)$. $p \equiv 7(16)$ is excluded since $p \equiv 3(8)$.

(iii) The conditions on $p$ look so restrictive that there might be some doubt if primes of that type actually exist. But they do, and not quite as few as one may think at first sight, see Table 3. The first five examples are 11, 59, 107, 347, 587.

The second part of the proof of the Birch-Tate conjecture is furnished by a theorem on class numbers.

**Theorem 8.11.** Let $p$ be a prime number with $q = \frac{p-1}{2}$ prime and assume that 2 is a primitive root mod $q$. Let $E = Q(\zeta_p)$, Then the relative class number $h^{-}(E)$ is odd.

**Proof.** The relative class number formula (16) gives us

$$h^{-}(E) = 8p \prod_{\chi \text{ odd}} -\frac{1}{2} B_{1,\chi}.$$ 

The odd characters of $E$ belong to either $Q(i)$, $Q(\zeta_p)$, or to no proper imaginary subfield of $E$. For $\chi = \chi_4$ we have $B_{1,\chi} = \frac{1}{4} \sum_{t=1}^{4} \chi(t) = -\frac{1}{2}$. In the proof of Theorem 3.7 it has been shown that

$$h^{-}(Q(\zeta_p)) = 2p \prod_{\chi \text{ odd}} -\frac{1}{2} B_{1,\chi}$$ 

is odd. Putting things together it remains to prove that

$$\frac{h^{-}(E)}{4 \cdot h^{-}(Q(\zeta_p))} = \prod_{\chi \text{ odd}} -\frac{1}{2} B_{1,\chi}$$
is odd. It is enough to show that $2 \mid B_{1,\chi}$ for those $\chi$. By Lemma 3.9,

$$B_{1,\chi} = - \sum_{t \text{ odd}}^{p-1} \chi(t) \in \mathbb{Q}(\zeta_q).$$

Since $\chi = \chi_4 \cdot \chi_p$, where $\chi_p$ is a generator of the character group of $\mathbb{Q}(\zeta_p)^+$, the $\chi(t)$, $1 \leq t < p$, $t$ odd, are a set of $q = \frac{p-1}{2}$ different powers of $\zeta_q = e^{2\pi i/q}$, possibly with minus signs attached. Now proceed as in the proof of Theorem 3.10 to produce a coefficient of $B_{1,\chi}$ equal to 2 or $-2$.

As in the case of the fields $\mathbb{Q}(\zeta_q \zeta_k)$, we can now combine these results in the proof of the second major theorem of this chapter.

**Theorem 3.12.** The Birch-Tate conjecture holds for the fields $\mathbb{Q}(\zeta_p)^+$, where $p$ is a prime number congruent to 3 modulo 8 such that $q = \frac{p-1}{2}$ is a prime having 2 as a primitive root.

**Proof.** First we apply Lemma 3.2. Observe that $E := F(i) = \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p)(i)$. By Theorem 3.11, the relative class number $h^-$ of $E$ is odd, hence $h = h(E)$ is odd. By the remark following Theorem 3.10, 2 is a primitive root mod $p$, hence 2 is inert in $\mathbb{Q}(\zeta_p)$. Since $\mathbb{Q}(i)$ has only one dyadic prime, the same is true for $E = \mathbb{Q}(\zeta_p)(i)$. Lemma 3.2 tells us that the 2-Sylow-subgroup of $K_2(\mathcal{O}_E)$ is elementary abelian. By Theorem 3.10, $2^{[F:\mathbb{Q}]} \mid w_2(F)\zeta_F(-1)$. With Lemma 3.3 the Birch-Tate conjecture follows. □

In order to confirm the Birch-Tate conjecture for several special cases using numerical results, we state a variation of Theorem 3.12. The proof is nearly identical.

**Theorem 3.18.** Let $E = \mathbb{Q}(\zeta_k \zeta_p^{1/p})$, where $k \geq 2$, $p$ an odd prime, and $l \geq 1$. Let $F = E^+$. Assume that 2 is a primitive root mod $p^l$, $h(E)$ is odd, and that $2^{[F:\mathbb{Q}]} \mid w_2(F)\zeta_F(-1)$. Then the Birch-Tate conjecture holds for $F$. □
Remark. This theorem settles the Birch-Tate conjecture for the fields $F = \mathbb{Q}(\sqrt{m})^+$, $m = 20, 24, 36, 40, 44, 48, 52, 72, 76, 80, 88, 96, 100$. For a table of class numbers see [32]. Together with results of [18], [22], the Birch-Tate conjecture follows for all $F = \mathbb{Q}(\sqrt{m})^+$, $m \leq 100$, having the property that $2^{[F:\mathbb{Q}]} \mid \omega_2(F)\zeta_F(-1)$. In the next chapter we show that the 2-part of the Birch-Tate conjecture actually holds for all totally real number fields with this property.
Chapter 4

The 2-part of the Birch-Tate conjecture for not necessarily abelian fields

§4.1. The proof

So far we have dealt exclusively with abelian number fields. Recent work on this subject enables us to combine results of [5] and [8] in order to prove the 2-part of the Birch-Tate conjecture for all totally real—not necessarily abelian—number fields having the property that $2^{[F:Q]}$ is the exact 2-power dividing $w_2(F)\xi_P(-1)$ or the order of $K_2(o_F)$, respectively. Before we start we give a list of notations which is derived from these two papers. In case of ambiguity the notation of [8] was preferred.

For an arbitrary number field $F$ let us denote by

- $O_F$ the ring of integers of $F$,
- $r_1(F)$ the number of real places of $F$,
- $r_2(F)$ the number of pairs of conjugate complex places of $F$,
- $g_2(F)$ the number of dyadic places of $F$,
- $S = S(F)$ the set of infinite and dyadic places of $F$,
- $G^S(F)$ the $S$-ideal class group of $F$,
- $h^S(F)$ the $S$-class number of $F$, i.e. the order of $G^S(F)$,
- $U = U_F^S$ the group of $S$-units of $F$.

For $F$ totally real, $E = F(\sqrt{-1})$, we fix the following notation.

- $C_2$ the Galois group of $E$ over $F$,
- $d_1, d_2, d_3$ the number of dyadic primes of $F$ that ramify, are inert, split in $E/F$, respectively,
- $m$ the number of real places of $F$ that ramify in $E/F$,
- $t$ the number of places of $F$ outside $S$ that ramify in $E/F$. 

28
2^a \quad \text{the order of the cokernel of the norm map } N: U_{E}^{S} \to U_{F}^{S},
2^b \quad \text{the order of the kernel of the map } g: C^{S}(F) \to C^{S}(E),
2^c \quad \text{the } 2\text{-part of } h_{S}^{E}(F),
2^e \quad \text{the index of } (U_{E}^{S})^{2} \text{ in } U_{F}^{S},
h_{S}^{E} \quad \text{the order of the kernel of the norm map } N: C^{S}(E) \to C^{S}(F),
w \quad \text{the number of roots of unity in } E,
w_0 \quad \frac{w}{2}.

We proceed by proving the main result of this dissertation. It confirms the 2-primary part of the Birch-Tate conjecture for all totally real number fields with the property that
2^{r_1}(F) \parallel \#K_{2}(o_{F}) \text{ or that } 2^{r_1}(F) \parallel \#K_{2}(o).
In fact, these two conditions are equivalent.

We point out once more that the following theorem holds even in the non-abelian case.

**Main Theorem 4.1.** For any totally real number field $F$,
\[
2^{r_1}(F) \parallel \#K_{2}(o_{F}) \quad \text{if and only if} \quad 2^{r_1}(F) \parallel \#K_{2}(o) \text{ or that } 2^{r_1}(F) \parallel \#K_{2}(o).
\]

Before we give the proof, we state the key results that we need from [5] and [8].

**Proposition 4.2.** ([5], Prop. 9)

(i) If some prime of $F$ lying over 2 splits in $E = F(\sqrt{-1})$, then
\[
\frac{\zeta_{p}(\sqrt{-1})}{2^{e+c-3}} \text{ is } 2\text{-integral.}
\]

(ii) Suppose no prime of $F$ lying over 2 splits in $E$ and let
\[
q = \frac{h_{S}^{E}}{2^{e+c-1}}. \text{ Then } q \text{ is an integer}
\]
and the 2-fractional part of
\[
\frac{\zeta_{p}(\sqrt{-1})}{2^{e+c-3}} \text{ is the same as that of } \frac{q}{w_0}, \text{ in other words,}
\]
is 2-integral and is congruent to $q$ modulo the highest power of 2 dividing $w_0$.

**Proposition 4.8.** ([8], Thm. 4.1, Cor. 4.6) Let $F$ be an arbitrary number field. The following conditions are equivalent.

(i) $F$ admits an extension $E/F$ with $\#K_{2}(o_{E})$ odd,
(ii) \( g_2(F) = 1 \), \( h_S(F) \) is odd, and \( F \) contains \( S \)-units with independent signs,

(iii) \( \# K_2(o_F(\sqrt{-1})) \) is odd,

(iv) \( \text{rk}_2(K_2(o_F)) = r_1(F) \) and the 2-Sylow-subgroup of \( K_2(o_F) \) is elementary abelian,

(v) \( \# \text{2-Sylow} K_2(o_F) = 2^r_1(F) \).

We will also make repeated use of Tate's 2-rank formula (5). Now we are ready to give the proof of our Main Theorem.

**Proof of Theorem 4.1.** "\( \Rightarrow \)" Assume \( 2^r_1(F) \mid \# K_2(o_F) \). Let \( E = F(\sqrt{-1}) \). The 2-rank formula for \( F \) yields \( g_2(F) = 1 \) and \( h_S(F) \) odd. By Proposition 4.3 (iii) we have \( \# K_2(o_E) \) odd, hence, using the 2-rank formula for \( E \), \( g_2(E) = 1 \), and \( h_S(E) \) is odd. We conclude that also \( h_S^-(E) \) is odd. Next we compute the constants \( a, c, \) and \( e. \) Since the group \( H^0(C_2, U_E^S) = U_F^S/N(U_E^S) \) is an elementary abelian 2-group, \( a = \text{rk}_2(H^0(C_2, U_E^S)) \). Now consider the exact sequence

\[
H^0(C_2, C^S(E)) \to H^0(C_2, U_E^S) \xrightarrow{i} R(E/F) \to H^1(C_2, C^S(E)),
\]

see [8], Prop. 2.1 and the remark after the proof of Prop. 2.2. Since \( h_S(E) \) is odd, \( i \) is an isomorphism. By [8], Prop. 2.2, \( \text{rk}_2(R(E/F)) = m + t + d_1 + d_2 - 1 \). In our setting, \( m = r_1(F), t = 0, d_1 + d_2 = 1 \), hence \( a = \text{rk}_2(R(E/F)) = r_1(F) \). Since \( h_S(F) \) is odd, \( c = 0. \) \( e \) is the 2-rank of \( U_F^S/(U_F^S)^2 \), which is given by Dirichlet's S-unit theorem, namely \( e = r_1(F) + r_2(F) + g_2(F) = r_1(F) + 1 \) since \( F \) is totally real and we have already seen that \( g_2(F) = 1 \). Since \( g_2(F) = g_2(E) = 1 \), \( 2 \) does not split in \( E/F \) and we can apply Proposition 4.2 (ii). We find that \( q = \frac{h_S^-}{2e-a+c-1} = h_S^- \) is odd, hence \( \frac{w_0 s_F s(-1)}{2e+c-3} = \frac{w_0 s_F s(-1)}{2^r_1(F) - 2} \) is 2-integral and congruent to 1 modulo 2.

Recall the definition of \( w_2(F) \), i.p. the definition of the exponents \( n_F(F) \):

\[
n_F(F) = \max \{ n \geq 0 : Q(c_n) \subseteq F \};
\]

hence, in view of \( E = F(\sqrt{-1}) \),

\[
n_2(F) = \max \{ n \geq 0 : Q(c_n) \subseteq E \}.
\]
Therefore \((w_2(F))^2 = 2(w_2) = 4(w_0)^2\). Furthermore, \(s_{F, S}(-1) = s_F(-1) \prod_{\mathfrak{p} \mid 2} (1 - N_F)\), where the product is taken over the dyadic primes of \(F\), and \(N_F = \#(o_F/\mathfrak{p})\), hence \(s_{F, S}(-1) = s_F(-1) \cdot (1 - 2^j)\), where \(j\) is the inertial degree of the only dyadic prime of \(F\). So we obtain that \(w_2(F) s_F(-1) \equiv 2r_1(F) \pmod{2}\), i.e. \(2r_1(F) || w_2(F) s_F(-1)\).

**Assume** \(2r_1(F) || w_2(F) s_F(-1)\). Using Proposition 4.3 we have to show that \(K_2(o_F)\) has odd order. In view of the 2-rank formula for \(E\) this is equivalent to showing that

a) \(g_2(E) = 1\),

b) \(h_S(E)\) is odd.

For a) use Serre's result

\[2^{r_2} K_2(o_F) \mid w_2(F) s_F(-1)\]

and the 2-rank formula for \(F\) to obtain \(r_2(K_2(o_F)) = r_1(F)\), i.e. \(g_2(F) = 1\) and \(h_S(F)\) is odd. Now we assume that the dyadic prime of \(F\) splits in \(E\) and obtain a contradiction using Proposition 4.2. As in the first part of the proof we have \(c = 0\), \(e = r_1(F) + 1\), and we conclude that

\[\frac{s_F(-1)}{2e+c-3} = \frac{2r_1(F) - a}{2r_1(F) - 2}\]

is 2-integral. Since 8 divides \(w_2(F)\) it follows that \(\frac{w_2(F) s_F(-1)}{2r_1(F) + 1}\) is 2-integral, contrary to the assumption. Hence \(g_2(E) = g_2(F) = 1\). For b) observe that \(h_S(E)\) is odd if and only if \(h_S^{-}\) is odd, since \(h_S(E) = h_S(F) \cdot h_S^{-}\). This can be obtained as follows.

By definition, \(h_S^{-} = \#\ker N\), where \(N\) is the norm map from \(C^E(F)\) to \(C^F(F)\). Since \(h_S(F)\) is odd, it follows that the map \(g : C^S(F) \to C^S(E)\), induced by inclusion, is injective, see [8], proof of Prop. 2.2 b). Now \(N \circ g\) sends every \(I \in C^S(F)\) to \(I^2\); since \(h_S(F)\) is odd, \(N \circ g\) is surjective, hence so is \(N\). Thus \(h_S(E) = h_S(F) \cdot h_S^{-}\).

Now apply Proposition 4.2 (ii). By considerations that we have made in the first part of the proof we obtain that \(q = \frac{h_S^{-}}{2e+a+c-1} = \frac{h_S^{-}}{2r_1(F) - a}\) and

\[\frac{w_0 s_{F, S}(-1)}{2e+c-3} \equiv \frac{w_2(F) s_F(-1)}{2r_1(F)} \equiv \frac{h_S^{-}}{2r_1(F) - a} \pmod{2}\]

By assumption, \(\frac{w_2(F) s_F(-1)}{2r_1(F)}\) is 2-integral and congruent to 1 modulo 2, hence \(r_1(F) \geq a\). By [5], remark after Prop. 9, we have the inequality \(e - a + b \leq d_3 + 1\); here \(b = 0\) since \(h_S(F)\) is odd, and \(d_3 = 0\) since \(g_2(F) = g_2(E)\), hence \(e - 1 = r_1(F) \leq a\). Altogether we
obtain that \( a = r_1(F) \), hence \( h^S \) is odd, and this implies that \( h^S(E) \) is odd. Having shown a) and b) we conclude that \( \#K_2(\mathcal{O}_F(\sqrt{-1})) \) is odd, and Proposition 4.3 yields the desired result \( 2^{r_1(F)} \parallel \#K_2(\mathcal{O}_F) \).

We state the obvious

**Main Corollary 4.4.** The 2-part of the Birch-Tate conjecture holds for every totally real—not necessarily abelian—number field \( F \) satisfying \( 2^{r_1(F)} \parallel w_2(F)g_F(-1) \).

For the special case of abelian fields, this result has recently been obtained by G. Gras [13]. Since the odd part of the Birch-Tate conjecture has been proved for abelian fields, we immediately obtain

**Corollary 4.5.** The Birch-Tate conjecture holds for every totally real abelian number field \( F \) with \( 2^{r_1(F)} \parallel w_2(F)g_F(-1) \).

We close with a few comments on our computational work.

### §4.2. Numerical results

Theorem 4.1 enables us to confirm the 2-primary part of the Birch-Tate conjecture for a totally real number field whenever we can show that \( 2^{[F:\mathbb{Q}]} \parallel w_2(F)g_F(-1) \). This criterion is accessible to treatment with a computer, as it was done for subfields of cyclotomic fields \( \mathbb{Q}(\zeta_m) \), \( m \leq 100 \), see tables 1 and 2. A program for the computation of values of the zeta functions using formula (6) is presented in the appendix. Our tables confirm the Birch-Tate conjecture.
for all—not only the maximal—totally real subfields of \( \mathbb{Q}(\zeta_m) \), \( m = 2, 3, 5, 7, 8, 9, 11, 12, 13, 16, 19, 20, 23, 24, 25, 27, 32, 36, 37, 40, 44, 47, 48, 49, 52, 53, 59, 61, 64, 67, 71, 72, 76, 79, 80, 81, 83, 88, 96, 100.

All these values are of the form \( m = 2^k \cdot p^l \cdot k, l \geq 0, p \) a prime incongruent to 1 mod 8, which is not surprising since in all the other cases the condition \( 2^{[F:Q]} \parallel \nu_2(F)\zeta_F(-1) \) cannot hold for \( F = \mathbb{Q}(\zeta_m)^+ \). This follows from (6), the 2-rank formula (5), and the fact that \( F \) contains more than one dyadic prime if \( m \) is not of the above form, see [18].
Bibliography


Tables
We give the values of $|w_2(F)\zeta_p(-1)|$ for the subfields of $\mathbb{Q}(\zeta_p)\uparrow$, $p < 100$, having degree $n$ over $\mathbb{Q}$. The computations have been handled by an IBM 3081 and a VAX 11/750 using MACSYMA on top of EUNICE. Most of the large number decompositions are due to 'Buell's Factoring Express'. An entry followed by "PRP" is a probable prime base 2, 3, 5.

| $p$ | $n$ | $|w_2(F)\zeta_p(-1)|$ |
|-----|-----|------------------|
| 2   | 1   | 2                |
| 3   | 1   | 2                |
| 5   | 2   | $2^2$            |
| 7   | 3   | $2^3$            |
| 11  | 5   | $2^5 \cdot 5$   |
| 13  | 2   | $2^2$            |
| 17  | 2   | $2^3$            |
| 19  | 3   | $2^3 \cdot 3$   |
| 23  | 11  | $2^{11} \cdot 11 \cdot 37 \cdot 181$ |
| 29  | 2   | $2^3 \cdot 3$   |
| 31  | 3   | $2^5 \cdot 7$   |
| 37  | 2   | $2^2 \cdot 5$   |
| 5   | 5   | $2^5 \cdot 11$  |
| 15  | 5   | $2^{17} \cdot 5^2 \cdot 7 \cdot 11 \cdot 23 \cdot 2383$ |
| 37  | 2   | $2^2 \cdot 5$   |
| 3   | 3   | $2^3 \cdot 7$   |
| 6   | 6   | $2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 37$ |
| 9   | 9   | $2^9 \cdot 5^2 \cdot 7 \cdot 19 \cdot 577$ |
| 18  | 18  | $2^{18} \cdot 3^2 \cdot 5 \cdot 7 \cdot 19 \cdot 37 \cdot 73 \cdot 577 \cdot 17209$ |
| \( p \) | \( n \) | \( |w_2(F)x_p(-1)| \) |
|-------|-----|------------------|
| 41    | 2   | \( 2^5 \)         |
|       | 4   | \( 2^8 \cdot 13 \) |
|       | 5   | \( 2^5 \cdot 5 \cdot 431 \) |
|       | 10  | \( 2^{13} \cdot 5 \cdot 31^2 \cdot 431 \) |
|       | 20  | \( 2^{24} \cdot 5 \cdot 13 \cdot 31^2 \cdot 431 \cdot 2501 \cdot 83721 \) |
| 43    | 3   | \( 2^5 \cdot 19 \) |
|       | 7   | \( 2^7 \cdot 7 \cdot 29 \cdot 463 \) |
|       | 21  | \( 2^{23} \cdot 7 \cdot 19 \cdot 29 \cdot 463 \cdot 1051 \cdot 4165 \cdot 32733 \) |
| 47    | 23  | \( 2^{23} \cdot 23 \cdot 139 \cdot 823 \cdot 97087 \cdot 12451 \cdot 98633 \) |
| 53    | 2   | \( 2^3 \cdot 7 \) |
|       | 13  | \( 2^{13} \cdot 13 \cdot 96331 \cdot 3 \cdot 79549 \) |
|       | 26  | \( 2^{26} \cdot 7 \cdot 13 \cdot 85411 \cdot 96331 \cdot 3 \cdot 79549 \cdot 6419 \cdot 49283 \) |
| 59    | 29  | \( 2^{39} \cdot 29 \cdot 89 \cdot 998 \cdot 85536 \cdot 13691 \cdot 39381 \cdot 13587 \cdot 94271 \cdot \text{PRP} \) |
| 61    | 3   | \( 2^2 \cdot 11 \) |
|       | 3   | \( 2^3 \cdot 7 \cdot 19 \) |
|       | 5   | \( 2^5 \cdot 5 \cdot 2801 \) |
|       | 6   | \( 2^6 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31 \) |
|       | 10  | \( 2^{10} \cdot 5 \cdot 11^2 \cdot 2081 \cdot 2801 \) |
|       | 15  | \( 2^{15} \cdot 5 \cdot 7 \cdot 19 \cdot 2801 \cdot 5142 \cdot 16621 \) |
|       | 30  | \( 2^{30} \cdot 5 \cdot 7^2 \cdot 11^2 \cdot 19 \cdot 31 \cdot 2081 \cdot 2801 \cdot 40231 \cdot 4 \cdot 11241 \cdot 5142 \cdot 16621 \) |
|       | 67  | \( 2^3 \cdot 193 \) |
|       | 11  | \( 2^{11} \cdot 11 \cdot 661 \cdot 2861 \cdot 8009 \) |
|       | 33  | \( 2^{33} \cdot 11 \cdot 67 \cdot 193 \cdot 661^2 \cdot 2861 \cdot 8009 \cdot 11287 \cdot 9 \cdot 38320 \cdot 04556 \cdot 91459 \cdot \text{PRP} \) |
| 71    | 5   | \( 2^5 \cdot 5 \cdot 31 \cdot 211 \) |
|       | 7   | \( 2^7 \cdot 7 \cdot 113 \cdot 12713 \) |
|       | 35  | \( 2^{35} \cdot 5 \cdot 7 \cdot 31 \cdot 113 \cdot 211 \cdot 281 \cdot 701^2 \cdot 12713 \) |
|       |     | \( \cdot 130 \cdot 70849 \cdot 91922 \cdot 56557 \cdot 29061 \cdot \text{PRP} \) |
| 73    | 2   | \( 2^3 \cdot 11 \) |
|       | 3   | \( 2^3 \cdot 3 \cdot 79 \) |
|       | 4   | \( 2^7 \cdot 11 \cdot 89 \) |
|       | 6   | \( 2^7 \cdot 3 \cdot 11 \cdot 79 \cdot 241 \) |
|       | 9   | \( 2^9 \cdot 3^2 \cdot 79 \cdot 33 \cdot 41773 \) |
|       | 12  | \( 2^{15} \cdot 3 \cdot 11 \cdot 79 \cdot 89 \cdot 241 \cdot 23917 \) |
|       | 18  | \( 2^{19} \cdot 3^2 \cdot 11 \cdot 79 \cdot 241 \cdot 33 \cdot 41773 \cdot 115 \cdot 96933 \) |
|       | 36  | \( 2^{39} \cdot 3^2 \cdot 11 \cdot 79 \cdot 89 \cdot 241 \cdot 23917 \cdot 33 \cdot 41773 \cdot 115 \cdot 96933 \) |
|       |     | \( \cdot 31 \cdot 96495 \cdot 98933 \cdot 17833 \cdot \text{PRP} \) |
| $p$ | $n$ | $|w_2(F)\sigma_p(-1)|$ |
|-----|-----|-----------------|
| 79  | 3   | $2^3 \cdot 199$ |
|     | 13  | $2^{13} \cdot 13 \cdot 157 \cdot 521^2 \cdot 1130429$ |
|     | 39  | $2^{39} \cdot 13 \cdot 157 \cdot 199 \cdot 521^2 \cdot 1249 \cdot 4447 \cdot 323623 \cdot 1130429$ |
|     |     | $\cdot 68438 \cdot 64861 \cdot 45081 \cdot 49381$ PRP |
| 83  | 41  | $2^{41} \cdot 41 \cdot 172 \cdot 10653 \cdot 1512 \cdot 51379 \cdot 1893 \cdot 47613 \cdot 32741$ |
|     |     | $\cdot 488 \cdot 33370 \cdot 47633 \cdot 13247 \cdot 49419$ |
| 89  | 2   | $2^3 \cdot 13$ |
|     | 4   | $2^7 \cdot 5 \cdot 13 \cdot 37$ |
|     | 11  | $2^{11} \cdot 11 \cdot 4027 \cdot 2625 \cdot 04573$ |
|     | 22  | $2^{23} \cdot 11 \cdot 13 \cdot 4027 \cdot 2625 \cdot 04573 \cdot 1535 \cdot 46997 \cdot 28897$ |
|     | 44  | $2^{47} \cdot 5 \cdot 11 \cdot 13 \cdot 37 \cdot 397 \cdot 4027 \cdot 2625 \cdot 04573 \cdot 1535 \cdot 46997 \cdot 28897$ |
|     |     | $\cdot 491350 \cdot 60828 \cdot 9955\cdot 16703 \cdot 74357$ PRP |
| 97  | 2   | $2^3 \cdot 17$ |
|     | 3   | $2^3 \cdot 367$ |
|     | 4   | $2^6 \cdot 17 \cdot 149$ |
|     | 6   | $2^7 \cdot 17 \cdot 367 \cdot 421$ |
|     | 8   | $2^{11} \cdot 17 \cdot 149 \cdot 147689$ |
| 12  |     | $2^{14} \cdot 17 \cdot 149 \cdot 367 \cdot 421 \cdot 651997$ |
| 16  |     | $2^{20} \cdot 17 \cdot 149 \cdot 2753 \cdot 147689 \cdot 21205889$ |
| 24  |     | $2^{27} \cdot 5^2 \cdot 17 \cdot 149 \cdot 367 \cdot 421 \cdot 147689 \cdot 651997 \cdot 54297 \cdot 04177$ |
| 48  |     | $2^{52} \cdot 5^2 \cdot 7^2 \cdot 17 \cdot 149 \cdot 241 \cdot 367 \cdot 421 \cdot 2753 \cdot 147689 \cdot 651997 \cdot 21205889$ |
|     |     | $\cdot 414 \cdot 81169 \cdot 54297 \cdot 04177 \cdot 275 \cdot 80539 \cdot 52369$ |
Here are the values of $|w_2(F)\xi_F(-1)|$ for the maximal totally real subfields $F$ of $Q(\zeta_m)$, $m \leq 100$, composite, and $m \not\equiv 2 \mod 4$. The degree of $F$ over $Q$ is $n = \frac{1}{2} \phi(m)$, and $d_F$ denotes the discriminant of $F$.

| $m$ | $n$ | $d_F$ | $w_2(F)$ | $|w_2(F)\xi_F(-1)|$ |
|-----|-----|-------|-----------|-----------------|
| 8   | 2   | $2^3$ | $2^4 \cdot 3$ | $2^2$ |
| 9   | 3   | $3^4$ | $2^3 \cdot 3^2$ | $2^3$ |
| 12  | 2   | $2^2 \cdot 3$ | $2^3 \cdot 3$ | $2^2$ |
| 15  | 4   | $3^2 \cdot 3$ | $2^3 \cdot 3^5$ | $2^5$ |
| 16  | 4   | $2^{11}$ | $2^5 \cdot 3$ | $2^4 \cdot 5$ |
| 20  | 4   | $2^4 \cdot 5^3$ | $2^3 \cdot 3^5$ | $2^4 \cdot 5$ |
| 21  | 6   | $3^5 \cdot 7^5$ | $2^3 \cdot 3^7$ | $2^7 \cdot 7$ |
| 24  | 4   | $2^8 \cdot 3^2$ | $2^4 \cdot 3$ | $2^4 \cdot 3$ |
| 25  | 10  | $5^{17}$ | $2^3 \cdot 3^5 \cdot 2^2$ | $2^{10} \cdot 71 \cdot 641$ |
| 27  | 9   | $3^{22}$ | $2^3 \cdot 3^3$ | $2^9 \cdot 19 \cdot 307$ |
| 28  | 6   | $2^6 \cdot 7^5$ | $2^3 \cdot 3^7$ | $2^8 \cdot 13$ |
| 32  | 8   | $2^{31}$ | $2^6 \cdot 3$ | $2^8 \cdot 3^2 \cdot 5 \cdot 97$ |
| 33  | 10  | $3^5 \cdot 11^9$ | $2^3 \cdot 3^11$ | $2^{11} \cdot 3 \cdot 5 \cdot 421$ |
| 35  | 12  | $5^9 \cdot 7^{10}$ | $2^3 \cdot 3^5 \cdot 7$ | $2^{13} \cdot 13^2 \cdot 37 \cdot 61$ |
| 36  | 6   | $2^6 \cdot 3^9$ | $2^3 \cdot 3^2$ | $2^6 \cdot 31$ |
| 39  | 12  | $3^6 \cdot 13^{11}$ | $2^3 \cdot 3^13$ | $2^{14} \cdot 3^4 \cdot 13^2 \cdot 19$ |
| 40  | 8   | $2^{16} \cdot 5^6$ | $2^4 \cdot 3^5$ | $2^8 \cdot 5 \cdot 7 \cdot 41$ |
| 44  | 10  | $2^{10} \cdot 11^{9}$ | $2^3 \cdot 3^11$ | $2^{10} \cdot 5 \cdot 7 \cdot 31 \cdot 101$ |
| 45  | 12  | $3^8 \cdot 5^9$ | $2^3 \cdot 3^2 \cdot 5$ | $2^{13} \cdot 73 \cdot 3637$ |
| 48  | 8   | $2^{24} \cdot 3^4$ | $2^5 \cdot 3$ | $2^8 \cdot 3 \cdot 5 \cdot 73$ |
| 49  | 21  | $73^8$ | $2^3 \cdot 3^7^2$ | $2^{21} \cdot 113 \cdot 2437 \cdot 1940454849859$ |
| 51  | 16  | $3^8 \cdot 17^{15}$ | $2^3 \cdot 3^17$ | $2^{21} \cdot 73 \cdot 130 04081$ |
| 52  | 12  | $2^{12} \cdot 13^{11}$ | $2^3 \cdot 3^13$ | $2^{12} \cdot 13 \cdot 19 \cdot 73 \cdot 769$ |
| 55  | 20  | $5^{15} \cdot 11^{18}$ | $2^3 \cdot 3^5 \cdot 11$ | $2^{22} \cdot 3^4 \cdot 11^2 \cdot 41 \cdot 5581 \cdot 16061$ |
| $m$ | $n$ | $d_F$ | $w_2(F)$ | $|w_2(F)w_F(-1)|$ |
|-----|-----|-------|----------|----------------|
| 56  | 12  | $2^{24} \cdot 7^2$ | $2^6 \cdot 3 \cdot 7$ | $2^{15} \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 43$ |
| 57  | 18  | $3^9 \cdot 13^{17}$ | $2^3 \cdot 3 \cdot 19$ | $2^{19} \cdot 3^2 \cdot 7 \cdot 19 \cdot 97 \cdot 487 \cdot 83701$ |
| 60  | 8   | $2^8 \cdot 3^4 \cdot 5^6$ | $2^3 \cdot 3 \cdot 5$ | $2^{11} \cdot 3 \cdot 5$ |
| 63  | 18  | $3^{27} \cdot 7^{15}$ | $2^3 \cdot 3^2 \cdot 7$ | $2^{23} \cdot 5^2 \cdot 7^2 \cdot 19 \cdot 67 \cdot 193 \cdot 211$ |
| 64  | 16  | $7^9$ | $2^7 \cdot 3$ | $2^{16} \cdot 3^2 \cdot 5 \cdot 17 \cdot 97 \cdot 93347873$ |
| 65  | 24  | $5^{18} \cdot 13^{22}$ | $2^3 \cdot 3 \cdot 5 \cdot 13$ | $2^{41} \cdot 7^2 \cdot 19 \cdot 29 \cdot 37^2 \cdot 61 \cdot 97 \cdot 107^2$ |
| 68  | 16  | $216 \cdot 17^{15}$ | $2^3 \cdot 3 \cdot 17$ | $2^{20} \cdot 17 \cdot 73 \cdot 48741313$ |
| 69  | 22  | $3^{11} \cdot 23^{21}$ | $2^3 \cdot 3 \cdot 23$ | $2^{24} \cdot 3 \cdot 11 \cdot 23 \cdot 37181 \cdot 21796416731$ |
| 72  | 12  | $2^{24} \cdot 3^{18}$ | $2^4 \cdot 3^2$ | $2^{13} \cdot 3^2 \cdot 13 \cdot 19 \cdot 31 \cdot 79$ |
| 75  | 20  | $3^{10} \cdot 5^{35}$ | $2^3 \cdot 3 \cdot 5^2$ | $2^{21} \cdot 71 \cdot 641 \cdot 5797259381$ |
| 76  | 18  | $2^{18} \cdot 19^{17}$ | $2^3 \cdot 3 \cdot 19$ | $2^{18} \cdot 3^2 \cdot 19 \cdot 109 \cdot 229 \cdot 487 \cdot 221203$ |
| 77  | 30  | $7^{25} \cdot 11^{27}$ | $2^3 \cdot 3 \cdot 7 \cdot 11$ | $2^{44} \cdot 3^2 \cdot 5 \cdot 11 \cdot 19^2 \cdot 31 \cdot 139 \cdot 181 \cdot 3855211 \cdot 19916791$ |
| 80  | 16  | $2^{48} \cdot 5^{12}$ | $2^5 \cdot 3 \cdot 5$ | $2^{16} \cdot 5^2 \cdot 7 \cdot 41 \cdot 269 \cdot 337 \cdot 409$ |
| 81  | 27  | $3^{54}$ | $2^3 \cdot 3^4$ | $2^{27} \cdot 19 \cdot 307 \cdot 571 \cdot 10149 \cdot 32599 \cdot 25797 \cdot 70423$ |
| 84  | 12  | $2^{12} \cdot 3^6 \cdot 10^1$ | $2^3 \cdot 3 \cdot 5$ | $2^{15} \cdot 7 \cdot 13 \cdot 397$ |
| 85  | 32  | $5^{24} \cdot 17^{30}$ | $2^3 \cdot 3 \cdot 5 \cdot 17$ | $2^{45} \cdot 3^2 \cdot 5 \cdot 17 \cdot 73 \cdot 137 \cdot 257 \cdot 1201 \cdot 1697 \cdot 3678977$ |
| 87  | 28  | $3^{14} \cdot 29^{27}$ | $2^3 \cdot 3 \cdot 29$ | $2^{33} \cdot 3 \cdot 7 \cdot 13 \cdot 17 \cdot 43 \cdot 17837 \cdot 67726 \cdot 67760 \cdot 95561$ |
| 88  | 20  | $2^{40} \cdot 11^{18}$ | $2^4 \cdot 3 \cdot 11$ | $2^{20} \cdot 5 \cdot 7 \cdot 11^2 \cdot 23 \cdot 31 \cdot 101 \cdot 641 \cdot 15641$ |
| 91  | 36  | $7^{30} \cdot 13^{33}$ | $2^3 \cdot 3 \cdot 7 \cdot 13$ | $2^{47} \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 61 \cdot 73 \cdot 109 \cdot 139 \cdot 151$ |
| 92  | 22  | $2^{22} \cdot 23^{21}$ | $2^3 \cdot 3 \cdot 23$ | $2^{24} \cdot 5 \cdot 7 \cdot 11 \cdot 463 \cdot 9857 \cdot 37181 \cdot 21796416731$ |
| 93  | 30  | $3^{15} \cdot 21^{29}$ | $2^3 \cdot 3 \cdot 31$ | $2^{37} \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 19^2 \cdot 31 \cdot 274831 \cdot 2302381$ |
| 95  | 36  | $5^{27} \cdot 19^{34}$ | $2^3 \cdot 3 \cdot 5 \cdot 19$ | $2^{39} \cdot 3^4 \cdot 5 \cdot 13^3 \cdot 19 \cdot 37 \cdot 61 \cdot 421 \cdot 487 \cdot 7507 \cdot 7741$ |
| 96  | 16  | $2^{64} \cdot 3^8$ | $2^6 \cdot 3$ | $2^{16} \cdot 3^3 \cdot 5 \cdot 73 \cdot 97 \cdot 324889$ |
| 99  | 30  | $3^{45} \cdot 11^{27}$ | $2^3 \cdot 3^2 \cdot 11$ | $2^{31} \cdot 3^2 \cdot 5 \cdot 13^2 \cdot 31^2 \cdot 421^2 \cdot 51001 \cdot 510481 \cdot 3646681$ |
| 100 | 20  | $2^{20} \cdot 3^5$ | $2^3 \cdot 3 \cdot 5^2$ | $2^{20} \cdot 5^2 \cdot 71 \cdot 641 \cdot 347325 \cdot 50521$ |
This table gives all prime numbers $p < 10000$ such that $q = \frac{p-1}{2}$ is prime and 2 is a primitive root of $q$. The smallest primitive root $g$ of $p$ is given in the second column.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$g$</th>
<th>$q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>23</td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td>59</td>
<td>2</td>
<td>29</td>
</tr>
<tr>
<td>107</td>
<td>2</td>
<td>53</td>
</tr>
<tr>
<td>167</td>
<td>5</td>
<td>33</td>
</tr>
<tr>
<td>263</td>
<td>5</td>
<td>131</td>
</tr>
<tr>
<td>347</td>
<td>2</td>
<td>173</td>
</tr>
<tr>
<td>359</td>
<td>7</td>
<td>179</td>
</tr>
<tr>
<td>587</td>
<td>2</td>
<td>293</td>
</tr>
<tr>
<td>839</td>
<td>11</td>
<td>419</td>
</tr>
<tr>
<td>887</td>
<td>5</td>
<td>443</td>
</tr>
<tr>
<td>983</td>
<td>5</td>
<td>491</td>
</tr>
<tr>
<td>1019</td>
<td>2</td>
<td>509</td>
</tr>
<tr>
<td>1307</td>
<td>2</td>
<td>653</td>
</tr>
<tr>
<td>1319</td>
<td>13</td>
<td>659</td>
</tr>
<tr>
<td>2039</td>
<td>7</td>
<td>1019</td>
</tr>
<tr>
<td>2459</td>
<td>2</td>
<td>1229</td>
</tr>
<tr>
<td>2903</td>
<td>5</td>
<td>1451</td>
</tr>
<tr>
<td>2999</td>
<td>17</td>
<td>1499</td>
</tr>
<tr>
<td>3467</td>
<td>2</td>
<td>1733</td>
</tr>
<tr>
<td>3803</td>
<td>2</td>
<td>1901</td>
</tr>
<tr>
<td>3863</td>
<td>5</td>
<td>1931</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p$</th>
<th>$g$</th>
<th>$q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3947</td>
<td>2</td>
<td>1973</td>
</tr>
<tr>
<td>4139</td>
<td>2</td>
<td>2069</td>
</tr>
<tr>
<td>4283</td>
<td>2</td>
<td>2141</td>
</tr>
<tr>
<td>4679</td>
<td>11</td>
<td>2339</td>
</tr>
<tr>
<td>4919</td>
<td>13</td>
<td>2459</td>
</tr>
<tr>
<td>5099</td>
<td>2</td>
<td>2549</td>
</tr>
<tr>
<td>5387</td>
<td>2</td>
<td>2693</td>
</tr>
<tr>
<td>5999</td>
<td>7</td>
<td>2699</td>
</tr>
<tr>
<td>5483</td>
<td>2</td>
<td>2741</td>
</tr>
<tr>
<td>5639</td>
<td>7</td>
<td>2819</td>
</tr>
<tr>
<td>5879</td>
<td>11</td>
<td>2939</td>
</tr>
<tr>
<td>5927</td>
<td>5</td>
<td>2963</td>
</tr>
<tr>
<td>6599</td>
<td>13</td>
<td>3299</td>
</tr>
<tr>
<td>6827</td>
<td>2</td>
<td>3413</td>
</tr>
<tr>
<td>6983</td>
<td>5</td>
<td>3491</td>
</tr>
<tr>
<td>7079</td>
<td>7</td>
<td>3539</td>
</tr>
<tr>
<td>7559</td>
<td>13</td>
<td>3779</td>
</tr>
<tr>
<td>7607</td>
<td>5</td>
<td>3803</td>
</tr>
<tr>
<td>7703</td>
<td>5</td>
<td>3851</td>
</tr>
<tr>
<td>8039</td>
<td>11</td>
<td>4019</td>
</tr>
<tr>
<td>8699</td>
<td>2</td>
<td>4349</td>
</tr>
<tr>
<td>8747</td>
<td>2</td>
<td>4373</td>
</tr>
</tbody>
</table>
A program for the computation of $\varepsilon_p(-1)$

We briefly discuss a program written in Macsyma that was used for the computation of table 1. It is straightforward and could easily be optimized. A Pascal-version of the same program that contained some technical niceties in order to keep the numbers small was used to handle several smaller values of $p$ and $n$. The program that produced the entries for table 2 is similar but considerably longer since it is more difficult to generate character groups for composite values. Moreover conductors have to be taken care of.

We use formula (10) to compute the values of $|\omega_2(F)\varepsilon_p(-1)|$ for the totally real subfields of $E = \mathbb{Q}(\sqrt{p})$. Since the character group of $E$ is cyclic, these fields are in one-to-one correspondence to the divisors of $\frac{p-1}{2}$. The program requires three input values: A prime number $p$, a primitive root $w$ of $p$, and the field degree $\deg = [F : \mathbb{Q}]$.

I. A character $\chi_i$ having order $p - 1$ is generated using (12).

II. $\chi[1] = \chi^2$ is a generator for the character group of $\mathbb{Q}(\sqrt{p})^\dagger$. The other nontrivial even characters are $\chi[j] = \chi[1]^j$, $2 \leq j \leq \frac{p-3}{2}$. It is enough to compute their values at $a$, where $a$ ranges between 1 and $\frac{p-1}{2}$.

III. $S_i = \sum_{t=1}^{\frac{p-1}{2}} \chi(t) * (t - p) = \frac{1}{2} \sum_{t=1}^{\frac{p-1}{2}} \chi(t) * (t - p)$, where $\chi = \chi[i]$. Only the sums belonging to characters of $F$ are computed. The $S_i$ are elements of $\mathbb{Q}(\sqrt{p})^\dagger$, represented as polynomials in $\frac{p-1}{2}$.

IV. We do arithmetic in $\mathbb{Q}(\sqrt{\frac{p-1}{2}})$: Multiplication is polynomial multiplication, where the exponents are reduced modulo $\frac{p-1}{2}$.

V. Circle chasing is a heuristic procedure that is devised to make the result $r$ more readable by (hopefully) producing as many zero entries in the array $r$ as possible. It exploits the various relations $\sum t^i = 0$, where $t$ runs through different $\frac{p-1}{2}$-th roots of unity. Since the result is a rational integer, the ideal effect of this procedure would be $r[i] = 0$, $1 \leq i \leq \frac{p-3}{2}$, which is
unfortunately not always obtained.

VI., VII. The result is known to be highly divisible by 2 and p. These canceling routines save some later work in factoring.

VIII. The array r is printed and may have to be simplified somewhat by hand, twexp and prexp are the exponents of 2 and p that have been obtained in steps VI and VII.

The final result is to be multiplied by \( \frac{w_2(F)}{12} = 2p^\delta \), where \( \delta = 1 \) if \( \deg = \frac{p-1}{2} \) and 0 otherwise. It has to be divided by the discriminant \( d_F = p^{\deg-1} \). Of course, these steps could be easily included in the program. CPU-running time averaged between 1 and 2 hours, the longest run (\( p = 83 \)) took 3 hours and 38 minutes.
A MACSYMA-program that computes \( w_2(F)^{\frac{p-1}{2}} \) for subfields \( F \) of \( \mathbb{Q}(\sqrt{p}) \), \( p \) prime.

Inputs:

1. a prime number \( p \)
2. a primitive root \( w \) of \( p \)
3. the field degree \( \text{deg} = [F : \mathbb{Q}] \)

\[
\text{mod} \ (a, b) := a - \text{entier}(a/b) \times b;
\]

\[
\text{array} \ (g, p); \quad /* \text{powers of } w \quad */
\]

\[
\text{array} \ (X_1, p); \quad /* \text{generating char. mod } p \quad */
\]

\[
\text{array} \ (r, p); \quad /* \text{intermediate product} \quad */
\]

\[
\text{array} \ (res, p); \quad /* \text{auxiliary product} \quad */
\]

\[
\text{array} \ (s, p, p); \quad /* \text{even characters mod } p \quad */
\]

\[
\text{array} \ (a, p, p); \quad /* \text{sums } S_i \quad */
\]

\[
\text{reldeg} : (p - 1)/(2 \times \text{deg}); \quad /* \text{rel. field deg. } [\mathbb{Q}(\sqrt{p})^+ : F] \quad */
\]

\[
q : (p - 3)/2; \quad /* \text{upper bound for summation} \quad */
\]

\[
twexp : 0; \quad /* \text{exponent of } 2 \quad */
\]

\[
pexp : 0; \quad /* \text{exponent of } p \quad */
\]

/* I. Generate a character mod \( p \) having order \( p - 1 \) */

\[
g[0] : 1;
\]

\[
g[1] : w;
\]

\[
v : w;
\]

for \( n : 2 \) thru \( p - 2 \) do

\[
(v : \text{mod}(v \times w, p),
\]

/* */
\[ g[n] : v \]

);   
for \( n : 0 \) thru \( p - 2 \) do \( X_i[g[n]] : n; \)

/\* II. Generate the even characters mod \( p \) */
for \( a : 1 \) thru \( q + 1 \) do
  \( (x[1, a] : \text{mod}(2 \times X_i[a], p - 1), \)
  for \( j : 2 \) thru \( q \) do
    \( z[j, a] : \text{mod}(x[j - 1, a] + x[1, a], p - 1) \)
);   

/\* III. Generate the sums \( S_i \) */
for \( j : 1 \) thru \( q \) do for \( k : 0 \) thru \( q \) do \( s[j, k] : 0; \)
for \( d : 1 \) thru \( (p - 1)/(2 \times \text{reldeg}) - 1 \) do
  \( (i : \text{reldeg} \times d, \)
  for \( t : 1 \) thru \( q + 1 \) do
    \( s[i, x[i, t]/2] : s[i, x[i, t]/2] + t \times (t - p) \)
);   

/\* IV. Multiplication of the sums \( S_i \) */
for \( k : 0 \) thru \( q \) do \( r[k] : s[\text{reldeg}, k]; \)
for \( k : 0 \) thru \( q \) do \( r[k] : r[k]/2; \)
\( \text{tweexp} : \text{tweexp} + 1; \)
for \( d : 2 \) thru \( (p - 1)/(2 \times \text{reldeg}) - 1 \) do
  \( (i : \text{reldeg} \times d, \)
  for \( k : 0 \) thru \( q \) do \( \text{res}[k] : 0; \)
  for \( n : 0 \) thru \( q \) do
    for \( m : 0 \) thru \( q \) do
      \( (\text{prod} : r[n] \times s[i, m], \)
      \( \text{exp} : \text{mod}(n + m, q + 1), \)
res[exp] : res[exp] + prod

),
for k : 0 thru q do r[k] : res[k]
);

/* V. Circle chasing: Keep coefficients small */
for k : 1 thru (p - 1)/4 do
  ( if mod(q + 1, k) = 0 then
    ( for j : 0 thru k - 1 do
      ( hb : r[j],
        for l : 0 thru (q + 1)/k - 1 do
          if hb > r[k * l + j] then hb : r[k * l + j],
          for l : 0 thru (q + 1)/k - 1 do
            r[k * l + j] : r[k * l + j] - hb
      )
    )
  );

/* VI. Cancel powers of 2 */
divcheck : true;
for i : 1 thru p do
  if divcheck then
    ( for k : 0 thru q do
      ( h : mod(r[k], 2),
        if h # 0 then divcheck : false
      ),
    ),
  if divcheck then
    ( for k : 0 thru q do r[k] : r[k]/2, twexp : twexp + 1)
);
/* VII. Cancel powers of $p$ */

divcheck : true;

for $i : 1$ thru $p$ do
    if divcheck then
        ( for $k : 0$ thru $q$ do
            ( $h : \text{mod}(r[k], p)$,
                if $h \not= 0$ then divcheck : false
            ),
        
        if divcheck then
            ( for $k : 0$ thru $q$ do $r[k] : r[k] / p$, prexp : prexp + 1)
        );

/* VIII. Output */

for $k : 0$ thru $q$ do display($r[k]$);
display($p$);
display(deg);
display(twezp);
display(prezp);

/* * * * * * * * * * * * * * * * * * * * * * */
/* */
/* End of the program */
/* */
Vita

I, Karl Friedrich Hettling, was born on February 17, 1956, in Hamburg, Federal Republic of Germany, where I attended elementary and high school. I studied Mathematics with minor in Computer Science from 1974 to 1982 at the University of Hamburg, where I received a Bachelor's degree in 1978 and a Master's degree in 1982. I entered Louisiana State University in 1983 and am currently working on a Ph.D. degree in Mathematics.
DOCTORAL EXAMINATION AND DISSERTATION REPORT

Candidate: Karl Friedrich Hettling

Major Field: Mathematics: Number Theory

Title of Dissertation: On $K_2$ of Rings of Integers of Totally Real Number Fields

Approved:

[Signatures]

EXAMINING COMMITTEE:

[Signatures]

Date of Examination: 4-15-1985