

SELMER GROUPS AND QUADRATIC RECIPROCITY

FRANZ LEMMERMEYER

ABSTRACT. In this article we study the 2-Selmer groups of number fields F as well as some related groups, and present connections to the quadratic reciprocity law in F .

Let F be a number field; elements in F^\times that are ideal squares were called singular numbers in the classical literature. They were studied in connection with explicit reciprocity laws, the construction of class fields, or the solution of embedding problems by mathematicians like Kummer, Hilbert, Furtwängler, Hecke, Takagi, Shafarevich and many others. Recently, the groups of singular numbers in F were christened Selmer groups by H. Cohen [4] because of an analogy with the Selmer groups in the theory of elliptic curves (look at the exact sequence (2.2) and recall that, under the analogy between number fields and elliptic curves, units correspond to rational points, and class groups to Tate-Shafarevich groups).

In this article we will present the theory of 2-Selmer groups in modern language, and give direct proofs based on class field theory. Most of the results given here can be found in §§ 61ff of Hecke's book [11]; they had been obtained by Hilbert and Furtwängler in the roundabout way typical for early class field theory, and were used for proving explicit reciprocity laws. Hecke, on the other hand, first proved (a large part of) the quadratic reciprocity law in number fields using his generalized Gauss sums (see [3] and [22]), and then derived the existence of quadratic class fields (which essentially is just the calculation of the order of a certain Selmer group) from the reciprocity law.

In Takagi's class field theory, Selmer groups were moved to the back bench and only resurfaced in his proof of the reciprocity law. Once Artin had found his general reciprocity law, Selmer groups were history, and it seems that there is no coherent account of their theory based on modern class field theory.

Hecke's book [11] is hailed as a classic, and it deserves the praise. Its main claim to fame should actually have been Chapter VIII on the quadratic reciprocity law in number field, where he uses Gauss sums to prove the reciprocity law, then derives the existence of 2-class fields, and finally proves his famous theorem that the ideal class of the discriminant of an extension is always a square. Unfortunately, this chapter is not exactly bedtime reading, so in addition to presenting Hecke's results in a modern language I will also give exact references to the corresponding theorems in Hecke's book [11] in the hope of making this chapter more accessible.

The actual reason for writing this article, however, was that the results on Selmer groups presented here will be needed for computing the separant class group of F , a new invariant that will be discussed thoroughly in [21].

1. NOTATION

Let F be a number field. The following notation will be used throughout this article:

- n is the degree $(F : \mathbb{Q})$ of F . By r and s we denote the number of real and complex places of F ; in particular, we have $n = r + 2s$;
- F_+^\times is the subgroup of all totally positive elements in $F^\times = F \setminus \{0\}$;
- for abelian groups A , $\dim A/A^2$ denotes the dimension of A/A^2 as a vector space over \mathbb{F}_2 ; note that $(A : A^2) = 2^{\dim A/A^2}$;
- E is the unit group of F , and E^+ its subgroup of totally positive units; observe that $\dim E/E^2 = r + s$;
- $\text{Cl}(F)$ and $\text{Cl}^+(F)$ denote the class groups of F in the usual and in the strict sense;
- $\rho = \dim \text{Cl}(F)/\text{Cl}(F)^2$ and $\rho^+ = \dim \text{Cl}^+(F)/\text{Cl}^+(F)^2$ denote the 2-ranks of the class groups in the usual and in the strict sense;
- $\text{Cl}_F\{4\}$ is the ray class group modulo 4 in F , i.e., the quotient of the group of ideals coprime to (2) by the subgroup of principal ideals (α) with $\alpha \equiv 1 \pmod{4}$. Similarly, $\text{Cl}_F^+\{4\}$ is the ray class group modulo 4∞ in F .

2. THE SELMER GROUP

2.1. Definition of the Selmer Groups. The 2-Selmer group $\text{Sel}(F)$ of a number field F is defined as

$$\text{Sel}(F) = \{\alpha \in F^\times : (\alpha) = \mathfrak{a}^2\}/F^{\times 2}.$$

The elements $\omega \in F^\times$ with $\omega F^{\times 2} \in \text{Sel}(F)$ are called singular in the classical literature (see e.g. Hecke [11, § 61, art. 4]); Cohen [4] calls them virtual units. In fact we will see that if F has odd class number, then $\text{Sel}(F) \simeq E/E^2$.

The following lemma will allow us to define homomorphisms from $\text{Sel}(F)$ into groups of residue classes:

Lemma 2.1. *Let \mathfrak{m} be an integral ideal in a number field F . Then every element in $\text{Sel}(F)$ can be represented by an element coprime to \mathfrak{m} .*

Proof. Let $\alpha F^{\times 2} \in \text{Sel}(F)$ and write $(\alpha) = \mathfrak{a}^2$. Now find an ideal \mathfrak{b} coprime to \mathfrak{m} in the ideal class $[\mathfrak{a}]$; then $\gamma\mathfrak{a} = \mathfrak{b}$, hence $\beta = \alpha\gamma^2$ satisfies $(\beta) = \mathfrak{b}^2$. \square

Let us now introduce the following groups:

$$M_4 = (\mathcal{O}_F/4\mathcal{O}_F)^\times, \quad M^+ = F^\times/F_+^\times, \quad M_4^+ = M_4 \oplus M^+.$$

Note that $F^\times/F_+^\times \simeq (\mathbb{Z}/2\mathbb{Z})^r$ via the signature map. Moreover, the isomorphism $M_4/M_4^2 \simeq (\mathbb{Z}/2\mathbb{Z})^n$ is induced by the map sending $\alpha \pmod{2}$ to $1 + 2\alpha \pmod{4}$. This implies that $M_4^+/(M_4^+)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{2r+2s}$.

By Lemma 2.1 we can define a map $\phi : \text{Sel}(F) \rightarrow M_4/M_4^2$ by sending $\alpha F^{\times 2}$, where α is chosen coprime to 2, to the class of $\alpha \pmod{4}$. Now we define certain subgroups of $\text{Sel}(F)$ via the exact sequences

$$\begin{aligned} 1 &\longrightarrow \text{Sel}^+(F) \longrightarrow \text{Sel}(F) \longrightarrow M^+/(M^+)^2 \\ 1 &\longrightarrow \text{Sel}_4(F) \longrightarrow \text{Sel}(F) \longrightarrow M_4/M_4^2 \\ 1 &\longrightarrow \text{Sel}_4^+(F) \longrightarrow \text{Sel}(F) \longrightarrow M_4^+/(M_4^+)^2. \end{aligned}$$

2.2. Computation of the Selmer Ranks. Now let \mathfrak{m} be an arbitrary modulus, i.e. a formal product of an integral ideal and some real infinite primes. There is a natural projection $\text{Cl}_F\{\mathfrak{m}\} \rightarrow \text{Cl}(F)$, and this induces an epimorphism $\nu : \text{Cl}_F\{\mathfrak{m}\}/\text{Cl}_F\{\mathfrak{m}\}^2 \rightarrow \text{Cl}(F)/\text{Cl}(F)^2$. The kernel of ν consists of classes $[(\alpha)]_{\mathfrak{m}}$ with $\alpha \in F^\times$ coprime to \mathfrak{m} . In fact, if we denote the of coprime residue classes modulo \mathfrak{m} by $M_{\mathfrak{m}}$, and define a homomorphism $\mu : M_{\mathfrak{m}}/M_{\mathfrak{m}}^2 \rightarrow \text{Cl}_F\{\mathfrak{m}\}/\text{Cl}_F\{\mathfrak{m}\}^2$ by sending the coset of the residue class $\alpha + \mathfrak{m}$ to the coset of the ideal class $[(\alpha)]_{\mathfrak{m}} \in \text{Cl}_F\{\mathfrak{m}\}$, then it is easily checked that μ is well defined, and that we have $\ker \nu = \text{im } \mu$.

The kernel of $\mu_{\mathfrak{m}}$ consists of all residue classes $\alpha M_{\mathfrak{m}}^2$ for which (α) is equivalent to the principal class modulo squares. If $(\alpha) = \gamma \mathfrak{b}^2$, then $\mathfrak{b}^2 = (\beta)$ is principal (hence $\beta F^{\times 2} \in \text{Sel}(F)$) and can be chosen in such a way that $\alpha \equiv \beta \pmod{4}$; conversely, if α is congruent modulo 4 to some element in the Selmer group, then $\alpha M_{\mathfrak{m}}^2 \in \ker \mu$. This shows that $\ker \mu$ equals the image of the map $\text{Sel}(F) \rightarrow M_{\mathfrak{m}}/M_{\mathfrak{m}}^2$.

By taking $\mathfrak{m} = \infty, 4$, and 4∞ we thus get the exact sequences

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & \text{Sel}^+ & \longrightarrow & \text{Sel} & \longrightarrow & M_+/2 & \longrightarrow & \text{Cl}^+/2 & \longrightarrow & \text{Cl}/2 & \longrightarrow & 1, \\ 1 & \longrightarrow & \text{Sel}_4 & \longrightarrow & \text{Sel} & \longrightarrow & M_4/2 & \longrightarrow & \text{Cl}\{4\}/2 & \longrightarrow & \text{Cl}/2 & \longrightarrow & 1, \\ 1 & \longrightarrow & \text{Sel}_4^+ & \longrightarrow & \text{Sel} & \longrightarrow & M_4^+/2 & \longrightarrow & \text{Cl}^+\{4\}/2 & \longrightarrow & \text{Cl}/2 & \longrightarrow & 1, \end{array}$$

where $A/2$ denotes the factor group A/A^2 .

Let us now determine the order of the Selmer groups. The map sending $\alpha \in \text{Sel}(F)$ to the ideal class $[\mathfrak{a}] \in \text{Cl}(F)$ is a well defined homomorphism which induces an exact sequence

$$1 \longrightarrow E/E^2 \longrightarrow \text{Sel}(F) \longrightarrow \text{Cl}(F)[2] \longrightarrow 1.$$

Since $E/E^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{r+s}$, this implies $\text{Sel}(F) \simeq (\mathbb{Z}/2\mathbb{Z})^{\rho+r+s}$.

The group $\text{Sel}_4(F)$ consists of all $\alpha \in F^\times$ modulo squares such that $F(\sqrt{\alpha})/F$ is unramified outside infinity; this shows that $\dim \text{Sel}_4(F) = \rho^+$. Similarly, the elements of $\text{Sel}_4^+(F)$ correspond to quadratic extensions of F that are unramified everywhere, hence $\dim \text{Sel}_4^+(F) = \rho$. Finally, the first of the three exact sequences above shows that $\dim \text{Sel}^+(F) = \rho^+ + s$.

We have proved

Theorem 2.2. *Let F be a number field and let ρ and ρ^+ denote the 2-ranks of the class groups in the usual and in the strict sense. The dimensions of the Selmer groups as vector spaces over \mathbb{F}_2 are given by the following table:*

A	$\text{Sel}(F)$	$\text{Sel}^+(F)$	$\text{Sel}_4(F)$	$\text{Sel}_4^+(F)$
$\dim A$	$\rho + r + s$	$\rho^+ + s$	ρ^+	ρ

Similarly, the dimensions of the associated ray class groups are

A	$\text{Cl}(F)$	$\text{Cl}^+(F)$	$\text{Cl}_F\{4\}$	$\text{Cl}_F^+\{4\}$
$\dim A/A^2$	ρ	ρ^+	$\rho^+ + s$	$\rho + r + s$

The numbers in these tables suggest some kind of duality between certain Selmer and ray class groups. We will see below that this is indeed the case: as a matter of fact, this duality is a simple consequence of the quadratic reciprocity law.

Let me also mention that $\dim \text{Sel}_4^+ = \rho$ is the existence theorem for quadratic Hilbert class fields, since it predicts that the maximal elementary abelian unramified

2-extension of F is generated by the square roots of $\rho = \dim \text{Cl}(F)/\text{Cl}(F)^2$ elements of F .

3. ASSOCIATED UNIT GROUPS

In analogy to the subgroups $\text{Sel}^*(F)$ of the Selmer group we can define subgroups of E^*/E^2 of E/E^2 as follows:

$$\begin{aligned} E^+ &= \{\varepsilon \in E : \varepsilon \gg 0\}, \\ E_4 &= \{\varepsilon \in E : \varepsilon \equiv \xi^2 \pmod{4}\}, \\ E_4^+ &= \{\varepsilon \in E : \varepsilon \equiv \xi^2 \pmod{4}, \varepsilon \gg 0\}. \end{aligned}$$

Applying the snake lemma to the diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & E/E^2 & \longrightarrow & \text{Sel}(F) & \longrightarrow & \text{Cl}(F)[2] \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & M_4/M_4^2 & \longrightarrow & M_4/M_4^2 & \longrightarrow & 1 \end{array}$$

provides us with an exact sequence

$$1 \longrightarrow E_4/E^2 \longrightarrow \text{Sel}_4(F) \longrightarrow \text{Cl}(F)[2];$$

This (and a similar argument involving M^+ instead of M_4) implies

Proposition 3.1. *If F is a number field with odd class number, then*

$$E/E^2 \simeq \text{Sel}(F), \quad E_4/E^2 \simeq \text{Sel}_4(F) \quad \text{and} \quad E^+/E^2 \simeq \text{Sel}^+(F).$$

Now consider the natural map $\pi : \text{Cl}^+(F) \longrightarrow \text{Cl}(F)$ sending an ideal class $[\mathfrak{a}]_+$ to the ideal class $[\mathfrak{a}]$; this homomorphism is clearly surjective. This gives the exact sequence

$$1 \longrightarrow \ker \pi \longrightarrow \text{Cl}^+(F) \longrightarrow \text{Cl}(F) \longrightarrow 1,$$

where $\ker \pi$ is the group of all ideal classes $[\mathfrak{a}]_+$ in the strict sense such that $[\mathfrak{a}] = 1$, i.e., $\ker \pi = \{[(\alpha)] : \alpha \in F^\times\}$.

Next consider the map $\eta : M^+ = F^\times/F_+^\times \longrightarrow \ker \pi$ defined by sending αF_+^\times to $[(\alpha)]_+$; this map is well defined and surjective, and its kernel consists of classes αF_+^\times that are represented by units, that is, $\ker \eta = EF_+^\times/F_+^\times \simeq E/E^+$. Thus we have

$$1 \longrightarrow E/E^+ \longrightarrow M^+ \longrightarrow \ker \pi \longrightarrow 1$$

Glueing the last two exact sequences together we get the exact sequence

$$(1) \quad 1 \longrightarrow E/E^+ \longrightarrow M^+ \longrightarrow \text{Cl}^+(F) \longrightarrow \text{Cl}(F) \longrightarrow 1.$$

This shows

Proposition 3.2. *We have $h^+(F) = 2^{r-u}h(F)$, where $u = \dim E/E^+$.*

Thus whereas Selmer groups measure the difference of the ranks of $\text{Cl}^+(F)$ and $\text{Cl}(F)$, the unit group contains information about their cardinalities. Trying to extract information on $\rho^+ - \rho$ from the sequence (1) does not work: note that $\text{Hom}(\mathbb{Z}/2\mathbb{Z}, A) \simeq A[2] = \{a \in A : 2a = 0\}$ for an additively written abelian group A . Since $\text{Hom}(\mathbb{Z}/2\mathbb{Z}, \cdot)$ is a left exact functor, and since E/E^+ and M^+ are elementary abelian 2-groups, (1) provides us with the exact sequence

$$1 \longrightarrow E/E^+ \longrightarrow F^\times/F_+^\times \longrightarrow \text{Cl}^+(F)[2] \xrightarrow{\pi} \text{Cl}(F)[2],$$

where we denoted the restriction of π to $\text{Cl}^+(F)[2]$ also by π , and where exactness at $\text{Cl}^+(F)[2]$ is checked directly. Now

$$\text{im } \pi = \widetilde{\text{Cl}}(F) := \{[\mathfrak{a}] \in \text{Cl}(F) : \mathfrak{a}^2 = (\alpha), \alpha \gg 0\},$$

hence we find

Proposition 3.3. *The sequence*

$$1 \longrightarrow E/E^+ \longrightarrow F^\times/F_+^\times \longrightarrow \text{Cl}^+(F)[2] \xrightarrow{\pi} \widetilde{\text{Cl}}(F) \longrightarrow 1$$

is exact; in particular, we have $\dim \widetilde{\text{Cl}}(F) = \rho^+ - r + u$.

4. APPLICATIONS

4.1. Unit Signatures. Lagarias observed in [16] that the residue class modulo 4 of an element $\alpha \in \mathcal{O}_F$ with $\alpha F^{\times 2} \in \text{Sel}(F)$ determines its signature for quadratic fields $F = \mathbb{Q}(\sqrt{d})$, where $d = x^2 + 16y^2$. This observation was generalized in [17, 18]; the main result of [18] is the equivalence of conditions (1) – (4) of the following theorem:

Theorem 4.1. *Let F be a number field and put $\rho_4 = \dim \text{Cl}_F\{4\}/\text{Cl}_F\{4\}^2$. Then the following assertions are equivalent:*

- (1) $s = 0$, and the image of $\alpha F^{\times 2} \in \text{Sel}(F)$ in M_4/M_4^2 determines its signature;
- (2) $s = 0$ and $\rho^+ = \rho$;
- (3) $s = 0$ and $\text{Sel}_4(F) \subseteq \text{Sel}^+(F)$;
- (4) $s = 0$ and the map $\text{Sel}(F) \rightarrow M^+$ is surjective;
- (5) the image of $\alpha F^{\times 2} \in \text{Sel}(F)$ in M^+ determines its residue class modulo 4 up to squares;
- (6) $\rho_4 = \rho$;
- (7) $\text{Sel}^+(F) \subseteq \text{Sel}_4(F)$;
- (8) the map $\text{Sel}(F) \rightarrow M_4/M_4^2$ is surjective.

Actually all these assertions essentially establish the following exact and commutative diagram (for number fields F with $s = \rho^+ - \rho = 0$):

$$\begin{array}{ccccccc} 1 & \longrightarrow & \text{Sel}^+(F) & \longrightarrow & \text{Sel}(F) & \longrightarrow & M^+ & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \text{Sel}_4(F) & \longrightarrow & \text{Sel}(F) & \longrightarrow & M_4/M_4^2 & \longrightarrow & 1, \end{array}$$

here the two vertical maps between the Selmer groups are the identity maps. Conversely, this diagram immediately implies each of the claims (1) – (8) above.

Proof. Consider the exact sequence

$$1 \longrightarrow \text{Sel}^+ \longrightarrow \text{Sel} \longrightarrow M_+ \longrightarrow \text{Cl}^+(F)/\text{Cl}^+(F)^2 \longrightarrow \text{Cl}(F)/\text{Cl}(F)^2 \longrightarrow 1.$$

Clearly $\rho^+ = \rho$ if and only if the map $M^+ \rightarrow \text{Cl}^+/2$ is trivial, that is, if and only if $\text{Sel}(F) \rightarrow M_+$ is surjective. This proves (2) \iff (4).

Similarly, the exact sequence

$$1 \longrightarrow \text{Sel}_4 \longrightarrow \text{Sel} \longrightarrow M_4/M_4^2 \longrightarrow \text{Cl}_F\{4\}/\text{Cl}_F\{4\}^2 \longrightarrow \text{Cl}(F)/\text{Cl}(F)^2 \longrightarrow 1$$

shows that (6) is equivalent to (8).

Theorem 2.2 immediately shows that (2) \iff (6).

(2) \implies (3) & (7): Since $\text{Sel}_4^+(F) \subseteq \text{Sel}^+(F)$ and both groups have the same dimension $\rho^+ + s = \rho$, we conclude that $\text{Sel}_4^+(F) = \text{Sel}^+(F)$. A similar argument shows that $\text{Sel}_4^+(F) = \text{Sel}_4(F)$.

(3) \implies (5): assume that $\alpha \equiv \beta \pmod{4}$; then $\alpha/\beta \in \text{Sel}_4(F) \subseteq \text{Sel}^+(F)$, hence α and β have the same signature.

(5) \implies (7): assume that $\alpha F^{\times 2} \in \text{Sel}^+(F)$. Then α and 1 have the same signature, hence they are congruent modulo 4 up to squares, and this shows that $\alpha F^{\times 2} \in \text{Sel}_4(F)$.

(7) \implies (2): $\text{Sel}^+(F) \subseteq \text{Sel}_4(F)$ implies $\text{Sel}^+(F) \subseteq \text{Sel}_4(F) \cap \text{Sel}^+(F) = \text{Sel}_4^+(F)$, and now Theorem 2.2 shows that $s = 0$ and $\rho^+ = \rho$.

It remains to show that (1) \iff (3). We do this in two steps.

(1) \implies (3): Assume that $\alpha F^{\times 2} \in \text{Sel}_4(F)$. By Lemma 2.1 we may assume that α is coprime to 2, and hence that $\alpha \equiv \xi^2 \pmod{4}$. Since the residue class determines the signature, α has the same signature as ξ^2 , i.e., α is totally positive.

(3) \implies (1): Assume that $\alpha F^{\times 2}, \beta F^{\times 2} \in \text{Sel}(F)$, and that $\alpha \equiv \beta \pmod{4}$. Then $\alpha/\beta \in \text{Sel}_4(F) \subseteq \text{Sel}^+(F)$, hence α and β have the same signature. \square

4.2. The Theorem of Armitage-Fröhlich. As a simple application of Hecke's results on Selmer groups we present a proof of the theorem of Armitage and Fröhlich on the difference between the class groups in the usual and in the strict sense.

We make use of a group theoretical lemma:

Lemma 4.2. *Assume that A is a finite abelian group with subgroups B , C and $D = B \cap C$. Then the inclusions $C \hookrightarrow A$ and $D \hookrightarrow B$ induce a monomorphism $C/D \hookrightarrow A/B$; in particular, we have $(C : D) \mid (A : B)$.*

The proof of this lemma is easy. Applying it to $A = \text{Sel}(F)$, $B = \text{Sel}_4(F)$, $C = \text{Sel}^+(F)$ and $D = \text{Sel}_4^+(F) = \text{Sel}_4(F) \cap \text{Sel}^+(F)$ we get $\rho^+ - \rho \leq \rho - \rho^+ + r$, which gives

Theorem 4.3 (Theorem of Armitage-Fröhlich). *Let F be a number field with r real embeddings. Then the difference of the 2-ranks of the class groups in the strict and in the usual sense is bounded by $\frac{r}{2}$; since this difference is an integer, we even have*

$$\rho^+ - \rho \leq \left\lfloor \frac{r}{2} \right\rfloor.$$

This proof of the theorem of Armitage & Fröhlich [1] is essentially due to Oriat [23]. Proofs dual to Oriat's were given by Hayes [10], who argued using the Galois groups of the Kummer extensions corresponding to elements in $\text{Sel}(F)$.

Applying the lemma to $A = \text{Sel}^+(F)$, $B = \text{Sel}_4^+(F)$, $C = E^+$ and $D = E_4^+$ and using the theorem of Armitage-Fröhlich we find

Theorem 4.4. *Let F be a number field with r real embeddings. Then*

$$\dim E_4^+/E^2 \geq \left\lfloor \frac{r}{2} \right\rfloor - \dim E/E^+.$$

According to Hayes [10], this generalizes results of Greither (unpublished) as well as Hagenmüller [9].

Let us now give a simple application of these results. Consider a cyclic extension F/\mathbb{Q} of prime degree p , and assume that 2 is a primitive root modulo p . Since the cyclic group $G = \text{Gal}(F/\mathbb{Q})$ acts on class groups and units groups, we find (see e.g. [20]) that the dimensions of the 2-class groups $\text{Cl}_2(F)$ and $\text{Cl}_2^+(F)$, as well

as of E^+/E^2 and E_4^+/E^2 (note that G acts fixed point free on E^+/E^2 , but not on E/E^2) as \mathbb{F}_2 -vector spaces are all divisible by $p-1$. Since $\rho^+ - \rho \leq \frac{p-1}{2}$ by Armitage-Fröhlich, we conclude that $\rho^+ = \rho$. This shows

Proposition 4.5. *Let F be a cyclic extension of prime degree p over \mathbb{Q} , and assume that 2 is a primitive root modulo p . Then $\rho^+ = \rho$, and in particular F has odd class number if and only if there exist units of arbitrary signature.*

Here are some numerical examples. For primes $p \equiv 1 \pmod{n}$, let $F_n(p)$ denote the subfield of degree n of $\mathbb{Q}(\zeta_p)$. Calculations with `pari` [2] provide us with the following table:

n	p	$\text{Cl}_2(F)$	$\text{Cl}_2^+(F)$
3	163	(2, 2)	(2, 2)
	1009	(2, 2)	(4, 4)
	7687	(2, 2, 2, 2)	(2, 2, 2, 2)
5	941	(2, 2, 2, 2)	(2, 2, 2, 2)
	3931	(4, 4, 4, 4)	(4, 4, 4, 4)
7	29	1	(2, 2, 2)
	491	(2, 2, 2)	(2, 2, 2, 2, 2, 2)

Now assume that $h^+ > h$, where h and h^+ denote the class numbers of F in the usual and the strict sense. In this case, $\dim E^+/E^2 > 0$, hence $\dim E^+/E^2 = p-1$ and therefore $\dim E/E^+ = \dim E/E^2 - \dim E^+/E^2 = p - (p-1) = 1$; in particular, -1 generates E/E^+ . Using Theorem 4.4 we find that $\dim E_4^+/E^2 \geq \lceil p/2 \rceil - 1 = \frac{p+1}{2}$, and now the Galois action implies that $\dim E_4^+/E^2 = p-1$. Thus $E^+ = E_4^+$, hence $F(\sqrt{E^+})/F$ is a subfield of degree 2^{p-1} of the Hilbert 2-class field of F .

Proposition 4.6. *Let F be a cyclic extension of prime degree p over \mathbb{Q} , and assume that 2 is a primitive root modulo p . If $h^+ > h$, then every totally positive unit is primary, and $F(\sqrt{E^+})/F$ is a subfield of degree 2^{p-1} of the Hilbert class field of F .*

5. HECKE'S PRESENTATION

We will now explain how Hecke's results in [11, § 61] are related to those derived above. The numbers below refer to the 13 articles in § 61 of Hecke's book:

1. $\dim E/E^2 = m := r + s$; (Hecke uses r_1 and r_2 instead of r and s);
2. $\dim F^\times/F_+^\times = r$;
3. $\rho = \dim \text{Cl}(F)/\text{Cl}(F)^2$; (Hecke uses e instead of ρ);
4. $\dim \text{Sel}(F) = \rho + r + s$;
5. $p := \dim \text{Sel}^+(F)$; the image of $\text{Sel}(F)$ in M^+ has dimension $m + e - p$;
6. $\rho^+ = \dim \text{Cl}^+(F)/\text{Cl}^+(F)^2$; $p = \rho^+ - r + m = \rho^+ + s$;
7. $\dim M_4/M_4^2 = n$;
8. $\dim M_4^+/(M_4^+)^2 = n + r = 2r + 2s$;
9. Hecke introduces the group $M_{4\mathfrak{l}}$ of residue classes modulo $4\mathfrak{l}$ for prime ideals $\mathfrak{l} \mid 2$ and proves that $\dim M_{4\mathfrak{l}}/M_{4\mathfrak{l}}^2 = n + r + 1$;
10. $q := \dim \text{Sel}_4(F)$; $q \leq \rho + r + s$;
11. $q_0 := \dim \text{Sel}_4^+(F)$;
12. $\dim \text{Cl}_F\{4\}/\text{Cl}_F\{4\}^2 = 2^{q+s}$;
13. $\dim \text{Cl}_F^+\{4\}/\text{Cl}_F^+\{4\}^2 = 2^{q_0+r+s}$.

In § 62 Hecke then uses analytic methods (and the quadratic reciprocity law) to prove that $q = \rho^+$ and $q_0 = \rho$.

6. CLASS FIELDS

In this section we will realize the Kummer extensions $F(\sqrt{\text{Sel}^*(F)})/F$ as class fields. As a first step, we determine upper bounds for the conductor of these extensions. To this end, we recall the conductor-discriminant formula. For quadratic extensions K/F with $K = F(\sqrt{\omega})$, it states that the discriminant of K/F coincides with its conductor, which in turn is defined as the conductor of the quadratic character $\chi_\omega = \left(\frac{\omega}{\cdot}\right)$.

Proposition 6.1. *Consider the Kronecker character $\chi = \left(\frac{\omega}{\cdot}\right)$, where $\omega \in \mathcal{O}_F$. Then χ is defined modulo \mathfrak{m} if and only if ω satisfies the conditions (*), and the elements $\omega F^{\times 2}$ with ω satisfying (*) form a group denoted by (\dagger) :*

\mathfrak{m}	(*)	(\dagger)
$(4)\infty$	$(\omega) = \mathfrak{a}^2$	$\text{Sel}(F)$
(4)	$(\omega) = \mathfrak{a}^2, \omega \gg 0$	$\text{Sel}^+(F)$
∞	$(\omega) = \mathfrak{a}^2, \omega \in M_4^2$	$\text{Sel}_4(F)$
1	$(\omega) = \mathfrak{a}^2, \omega \gg 0, \omega \in M_4^2$	$\text{Sel}_4^+(F)$

Proof. Every prime ideal with odd norm dividing (ω) to an odd power divides the relative discriminant of $K = F(\sqrt{\omega})$ to an odd power (cf. [11, Satz 119]); if $\mathfrak{l} \mid 2$ is a prime ideal dividing (ω) to an odd power, then $\mathfrak{l}^{2e+1} \parallel \text{disc } K/F$, where $\mathfrak{l}^e \parallel (2)$. Thus if the conductor of (ω/\cdot) divides 4∞ , then (ω) must be an ideal square.

The extension $F(\sqrt{\omega})/F$ is unramified at infinity if and only if $\omega \gg 0$. It is unramified at 2 if and only if ω is a square modulo 4, i.e., if and only if $\omega \in M_4^2$. \square

This shows that $F(\sqrt{\text{Sel}(F)})$ is contained in the ray class field modulo 4∞ . Now let $H(F)$, $H^+(F)$, $H_4(F)$, and $H_4^+(F)$ denote the maximal elementary abelian 2-extension of F with conductor dividing 1, ∞ , 4, and 4∞ , respectively.

If we put

$$\begin{aligned} P^+ &= \{(\alpha) \in P : \alpha \gg 0\}, \\ P_4 &= \{(\alpha) \in P : (\alpha, 2) = (1), \alpha \equiv \xi^2 \pmod{4}\}, \\ P_4^+ &= P^+ \cap P_4, \end{aligned}$$

then P , P^+ , P_4 and P_4^+ are the groups of principal ideals generated by elements $\alpha \equiv 1 \pmod{\mathfrak{m}}$ with $\mathfrak{m} = 1, \infty, (4)$, and $(4)\infty$, respectively. Now we claim

Theorem 6.2. *The class fields $H^*(F)$ can be realized as Kummer extensions $H^*(F) = F(\sqrt{\text{Sel}^*(F)})$ generated by elements of the Selmer group $\text{Sel}^*(F)$. The ideal groups $\mathcal{H}^*(F)$ associated to the extensions $H^*(F)/F$ are also given in the table below:*

$H^*(F)$	$\text{Sel}^*(F)$	$\mathcal{H}^*(F)$	\mathfrak{m}
$H(F)$	$\text{Sel}_4^+(F)$	$I^2 P$	$(4)\infty$
$H^+(F)$	$\text{Sel}_4(F)$	$I^2 P^+$	(4)
$H_4(F)$	$\text{Sel}^+(F)$	$I^2 P_4$	∞
$H_4^+(F)$	$\text{Sel}(F)$	$I^2 P_4^+$	1

The diagram in Fig. 1 helps explain the situation.

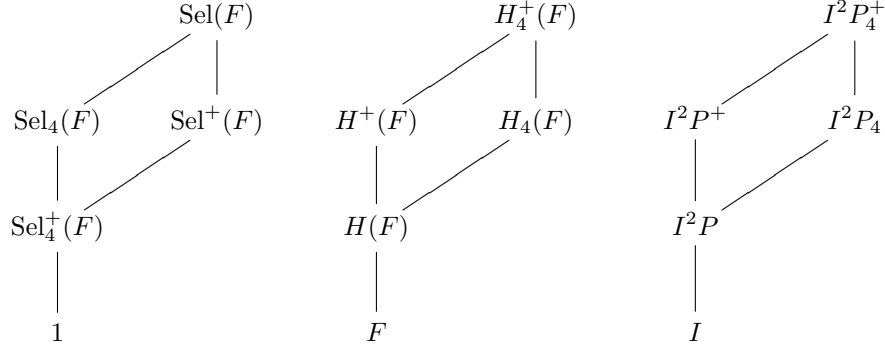


FIGURE 1. Class Fields

Proof. The entries in the second (and the last) column follow immediately from Prop. 6.1. It remains to compute the ideal groups associated to the extensions $F(\sqrt{\text{Sel}^*(F)})/F$.

The ideal group associated to the Hilbert class field $H^1(F)$ is the group $P = P_F$ of principal ideals in F . Let \mathcal{H} denote the ideal group associated to the maximal elementary abelian 2-extension $H(F)/F$; then $P \subseteq \mathcal{H} \subseteq I$, where $I = I_F$ is the group of fractional ideals in F , and \mathcal{H} is the minimal such group for which I/\mathcal{H} is an elementary abelian 2-group. Clearly \mathcal{H} contains $I^2 P$; on the other hand, $I^2 P/P \simeq \text{Cl}(F)^2$, hence $I/I^2 P \simeq \text{Cl}(F)/\text{Cl}(F)^2$ has the right index, and we conclude that $\mathcal{H} = I^2 P$ (see Lagarias [17, p. 3]).

Analogous arguments show that the ideal groups associated to the maximal elementary abelian 2-extensions with conductor dividing ∞ , 4 and 4∞ are $I^2 P^+$, $I^2 P_4$ and $I^2 P_4^+$, respectively. \square

If $\{\omega_1, \dots, \omega_\rho\}$ is a basis of $\text{Sel}_4^+(F)$ as an \mathbb{F}_2 -vector space, and if σ_j denotes the Legendre symbol (ω_j/\cdot) , then the Artin symbol of $H(F)/F$ can be written as $(H(F)/F, \cdot) = (\sigma_1, \dots, \sigma_\rho)$. Since the Artin symbol is defined for all unramified prime ideals we have to explain what (ω/\mathfrak{a}) should mean if \mathfrak{a} and ω are not coprime. Using Lemma 2.1, for evaluating (ω/\mathfrak{a}) we choose $\omega F^{\times 2} = \omega' F^{\times 2}$ with $(\omega') + \mathfrak{a} = (1)$ and put $(\omega/\mathfrak{a}) := (\omega'/\mathfrak{a})$.

As is well known, the Artin symbol defines an isomorphism between the ray class group associated to $H(F)/F$ and the Galois group $\text{Gal}(H(F)/F) \simeq (\mathbb{Z}/2\mathbb{Z})^\rho$. This shows that the kernel of the Artin symbol $(H(F)/F, \cdot) : I = I_F \rightarrow \text{Gal}(H/F)$ is just $I^2 P_F$, that is, the group of all ideals \mathfrak{a} that can be written in the form $\mathfrak{a} = (\alpha)\mathfrak{b}^2$. The ray class group associated to $H(F)$ is $I/I^2 P_F \simeq \text{Cl}(F)/\text{Cl}(F)^2$, and the Artin symbol induces a perfect pairing

$$\text{Cl}(F)/\text{Cl}(F)^2 \times \text{Sel}_4^+(F) \longrightarrow \mu_2,$$

where μ_2 denotes the group of square roots of 1. This pairing is an explicit form of the decomposition law in $H(F)/F$: a prime ideal \mathfrak{p} in F splits completely in $H(F)$ if and only if $(H(F)/F, \mathfrak{p}) = 1$, i.e., if and only if there is some ideal \mathfrak{b} such that $\mathfrak{p}\mathfrak{b}^{-2}$ is principal.

Of course we get similar results for the other Selmer groups:

Theorem 6.3. *Let F be a number field. Then the pairings*

$$(2) \quad \mathrm{Cl}_F^+\{4\} / \mathrm{Cl}_F^+\{4\}^2 \times \mathrm{Sel}(F) \longrightarrow \mu_2$$

$$(3) \quad \mathrm{Cl}_F\{4\} / \mathrm{Cl}_F\{4\}^2 \times \mathrm{Sel}^+(F) \longrightarrow \mu_2$$

$$(4) \quad \mathrm{Cl}^+(F) / \mathrm{Cl}^+(F)^2 \times \mathrm{Sel}_4(F) \longrightarrow \mu_2$$

$$(5) \quad \mathrm{Cl}(F) / \mathrm{Cl}(F)^2 \times \mathrm{Sel}_4^+(F) \longrightarrow \mu_2$$

are perfect.

The claims in this theorem are equivalent to Hecke's theorem 171, 173, 172, and 170, respectively. For totally complex fields with odd class number they were first proved by Hilbert [12, Satz 32, 33], and the general proofs are due to Furtwängler [6].

6.1. Quadratic Reciprocity. Decomposition laws in abelian extensions are reciprocity laws; Hecke proved the quadratic reciprocity law in number fields using quadratic Gauss sums, and then derived the existence of 2-class fields from his results. Furtwängler, on the other hand, used the existence of class fields to derive the reciprocity law:

Theorem 6.4 (Quadratic Reciprocity Law). *Let F be a number field, and let $\alpha, \beta \in \mathcal{O}_F$ be coprime integers with odd norm. Assume moreover that α and β have coprime conductors. Then $(\frac{\alpha}{\beta}) = (\frac{\beta}{\alpha})$.*

The conductor of $\alpha \in F^\times$ is by definition the conductor of the quadratic extension $F(\sqrt{\alpha})/F$. Sufficient conditions for coprime integers $\alpha, \beta \in \mathcal{O}_F$ to have coprime conductors are

- α is primary and totally positive;
- α is primary and β is totally positive.

By the last pairing in Theorem 6.3, we see that $(\frac{\omega}{\alpha}) = 1$ for all $\alpha \in F^\times$ and $\omega \in \mathrm{Sel}_4^+(F)$; in particular, we have $(\frac{\omega}{\mathfrak{a}}) = (\frac{\omega}{\mathfrak{b}})$ for all ideals $\mathfrak{a} \sim \mathfrak{b}$ in the same ideal class, or, more generally, for all ideals in the same coset of $\mathrm{Cl}(F) / \mathrm{Cl}(F)^2$. By applying this observation to certain quadratic extensions of F , Furtwängler was able to prove the quadratic reciprocity law in F :

Proof of Theorem 6.3. Put $K = F(\sqrt{\alpha\beta})$; then $L = K(\sqrt{\alpha}) = K(\sqrt{\beta})$, and since $\alpha F^{\times 2} \in \mathrm{Sel}_4^+(F)$ and $(\alpha, \beta) = 1$, we conclude that L/K is unramified everywhere. Now $\alpha\mathcal{O}_L = \mathfrak{a}^\ell$ and $\beta\mathcal{O}_L = \mathfrak{b}^\ell$; moreover $\mathfrak{a} \sim \mathfrak{b}$ since these ideals differ by the principal ideal generated by $\sqrt{\alpha\beta}$. Let \mathfrak{c} be an ideal in $[\mathfrak{a}] \in \mathrm{Cl}(K)$ that is coprime to $2\mathfrak{a}\mathfrak{b}$. Let (\div) and $(\div)_K$ denote the quadratic residue symbols in F and K , respectively. Then $(\frac{\alpha}{\beta}) = (\frac{\alpha}{\mathfrak{b}})_K$ and $(\frac{\beta}{\alpha}) = (\frac{\alpha}{\mathfrak{a}})_K$ by [19, Prop. 4.2.], $(\frac{\alpha}{\mathfrak{b}})_K = (\frac{\alpha}{\mathfrak{c}})_K$ since $\mathfrak{b} \sim \mathfrak{c}$, $(\frac{\alpha}{\mathfrak{c}})_K = (\frac{\beta}{\mathfrak{c}})_K$ since $K(\sqrt{\alpha}) = K(\sqrt{\beta})$, and by going backwards we find $(\frac{\alpha}{\beta}) = (\frac{\beta}{\alpha})$ as claimed. \square

6.2. The First Supplementary Law of Quadratic Reciprocity. The fact that the pairing

$$\mathrm{Cl}_F^+\{4\} / \mathrm{Cl}_F^+\{4\}^2 \times \mathrm{Sel}(F) \longrightarrow \mu_2 : \langle [\mathfrak{a}], \omega \rangle \longmapsto \left(\frac{\omega}{\mathfrak{a}}\right)$$

is perfect can be made explicit as follows:

Theorem 6.5. *Let \mathfrak{a} be an integral ideal with odd norm in some number field F . Then the following assertions are equivalent:*

- (1) *there is an integral ideal \mathfrak{b} and some $\alpha \equiv 1 \pmod{4\infty}$ such that $\mathfrak{a}\mathfrak{b}^2 = (\alpha)$;*
- (2) *we have $(\frac{\omega}{\mathfrak{a}}) = 1$ for all $\omega \in \text{Sel}(F)$.*

This result is Hilbert's version of the first supplementary law of quadratic reciprocity in number fields F (see Hecke [11, Satz 171]). In fact, for $F = \mathbb{Q}$ this is the first supplementary law of quadratic reciprocity: since \mathbb{Q} has class number 1, condition (1) demands that an ideal (a) is generated by some positive $a \equiv 1 \pmod{4}$; moreover, $\text{Sel}(\mathbb{Q})$ is generated by $\omega = -1$, hence Theorem 6.5 states that $(\frac{-1}{a}) = 1$ if and only if $a > 0$ and $a \equiv 1 \pmod{4}$ (possibly after replacing the generator a of (a) by $-a$).

Similarly, the fact that the pairing $\text{Cl}_F\{4\}/\text{Cl}_F\{4\}^2 \times \text{Sel}^+(F) \longrightarrow \mu_2$ is perfect is equivalent to Hecke [11, Satz 173]).

7. MISCELLANEA

Apart from the applications of Selmer groups discussed in Section 4, the results presented so far go back to Hecke. In this section we will describe a few developments that took place afterwards. Unfortunately, reviewing e.g. Oriat's beautiful article [23] and the techniques of Leopoldt's Spiegelungssatz (reflection theorem) would take us too far afield.

7.1. Reciprocity Laws. In [14], Knebusch & Scharlau presented a simple proof of Weil's reciprocity law based on the theory of quadratic forms and studied the structure of Witt groups. In their investigations, they came across a group they denoted by $P/F^{\times 2}$, which coincides with our $\text{Sel}(F)$, and they showed that $\dim \text{Sel}(F) = \rho + r + s$ in [14, Lemma 6.3.]. In the appendix of [14], they studied $\Delta^+ = \text{Sel}_4^+(F)$ and proved that the pairings (4) and (5) are nondegenerate in the second argument.

Kolster took up these investigations in [15] and generalized the perfect pairings above to certain general class groups and Selmer groups whose definitions depend on a finite set of primes S . In fact, let F be a number field, and let $v_{\mathfrak{p}}(\alpha)$ denote the exponent of \mathfrak{p} in the prime ideal factorization of (α) . For finite sets S of primes in F containing the set S_{∞} of infinite primes, let I_S denote the set of all ideals coprime to the finite ideals in S and to all dyadic primes, and define

$$D(S) = \{\alpha \in F^{\times} : v_{\mathfrak{p}}(\alpha) \equiv 0 \pmod{2} \text{ for all } \mathfrak{p} \notin S\}/F^{\times 2},$$

$$R(S) = I_S^2/I_S^2 \cdot \{(\alpha) \in P_4 : \alpha \in F_{\mathfrak{p}}^{\times 2} \text{ for } \mathfrak{p} \in S\}.$$

Then $D(S_{\infty}) = \text{Sel}(F)$ and $R(S_{\infty}) = I^2/I^2 P_4^+$. One of Kolster's tools is the perfect pairing (see [15, p. 86])

$$D(S) \times R(S) \longrightarrow \mu_2,$$

which specializes to the perfect pairing (2) in Thm. 6.3 for $S = S_{\infty}$.

7.2. Capitulation. Let L/K be an extension of number fields. Then the maps

$$j_{K \rightarrow L} : \text{Sel}(K) \longrightarrow \text{Sel}(L); j(\alpha K^{\times 2}) = \alpha L^{\times 2}$$

and

$$N_{L/K} : \text{Sel}(L) \longrightarrow \text{Sel}(K); N(\alpha L^{\times 2}) = N(\alpha)K^{\times 2}$$

are well defined homomorphism. Since $N_{L/K} \circ j_{K \rightarrow L}$ is raising to the $(L : K)$ -th power, $j_{K \rightarrow L}$ is injective and $N_{L/K}$ is surjective for all extensions L/K of odd degree.

For extensions of even degree, on the other hand, these maps have, in general, nontrivial kernels and cokernels. In fact, for $K = \mathbb{Q}(\sqrt{10})$ we have

$$\text{Sel}_4(K) = \text{Sel}^+(K) = \text{Sel}_4^+(K) = \langle 5 \rangle,$$

and in the quadratic extension $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ we have

$$\text{Sel}_4(L) = \text{Sel}^+(L) = \text{Sel}_4^+(L) = 1$$

because L has class number 1 in the strict sense. More generally, it is obvious that e.g. $\text{Sel}_4^+(K)$ capitulates in the extension $L = K(\sqrt{\text{Sel}_4^+(K)})$.

Note that $E^+/E^2 \hookrightarrow \text{Sel}^+(F)$. Garbanati [8, Thm. 2] observed that, for extensions L/K of totally real number fields, $E_L^+ = E_L^2$ implies that $E_K^+ = E_K^2$. This was generalized by Edgar, Mollin & Peterson [5]:

Proposition 7.1. *Let L/K be an extension of totally real number fields. Then $\dim E_K^+/E_K^2 \leq \dim E_L^+/E_L^2$.*

Proof. Let F^1 and F_+^1 denote the Hilbert class fields of F in the usual and in the strict sense. Then it is easily checked that $K^1 = K_+^1 \cap L^1$. This implies that $(K_+^1 L^1 : L^1) = (K_+^1 : K^1)$, hence $(K_+^1 : K^1) \mid (L_+^1 : L^1)$. \square

Thus although the image of E_K^+/E_K^2 in E_L^+/E_L^2 can become trivial (and will be trivial if and only if L contains $K(\sqrt{E^+})$), the dimension of E_L^+/E_L^2 cannot decrease. Something similar does not hold for E_4^+ : in $K = \mathbb{Q}(\sqrt{34})$, we have $E_4^+/E^2 = \langle \varepsilon E^2 \rangle$ for $\varepsilon = 35 + 6\sqrt{34}$. The field $L = K(\sqrt{\varepsilon}) = \mathbb{Q}(\sqrt{2}, \sqrt{17})$ has class number 1, hence $(E_L)_4^+ = E_L^2$.

7.3. Galois Action. Oriat [23] (see also Taylor [24]) derived, by applying Leopoldt's Spiegelungssatz, a lot of nontrivial inequalities between the ranks of pieces of the class groups in the usual and the strict sense. As a special case of his general result he obtained the following theorem:

Theorem 7.2. *Let K/\mathbb{Q} be a finite abelian extension of number fields. Assume that the exponent of $G = \text{Gal}(K/\mathbb{Q})$ is odd, and that $-1 \equiv 2^t \pmod{n}$ for some t . Then*

$$\rho^+ = \rho, \quad \dim E^+/E^2 \leq \rho, \quad \dim E_4/E^2 \leq \rho.$$

Observe that this contains Prop. 4.5 as a very special case.

In [5] it is erroneously claimed that Oriat proved this theorem for general (not necessarily abelian) extensions; the authors also give a proof of Theorem 7.2 "in the abelian case" which is based on the techniques of Taylor [24].

REFERENCES

- [1] J.V. Armitage, A. Fröhlich, *Classnumbers and unit signatures*, *Mathematika* **14** (1967), 94–98
- [2] C. Batut, K. Belabas, D. Benardi, H. Cohen, M. Olivier, *PARI-GP*, Bordeaux 1998; see <http://pari.home.ml.org>
- [3] M.C. Berg, *The Fourier-Analytic Proof of Quadratic Reciprocity Law*, Wiley 2000
- [4] H. Cohen, *Advanced topics in computational number theory*, GTM 193, Springer-Verlag 2000
- [5] H.M. Edgar, R. Mollin, B.L. Peterson, *Class groups, totally positive units, and squares*, *Proc. Amer. Math. Soc.* **98** (1986), 33–37

- [6] Ph. Furtwängler, *Die Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern (Dritter und letzter Teil)*, Math. Ann. **74** (1913), 413–429
- [7] D. Garbanati, *Unit signatures, and even class numbers, and relative class numbers*, J. Reine Angew. Math. **274/275** (1975), 376–384
- [8] D. Garbanati, *Units of norm -1 and signatures of units*, J. Reine Angew. Math. **283/284** (1976), 164–175
- [9] R. Haggemüller, *Signaturen von Einheiten und unverzweigte quadratische Erweiterungen total-reeller Zahlkörper*, Arch. Math. **39** (1982), 312–321
- [10] D. Hayes, *On the 2-ranks of Hilbert Class Fields*, preprint
- [11] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923
- [12] D. Hilbert, *Über die Theorie der relativquadratischen Zahlkörper*, Math. Ann. **51** (1899), 1–127; Gesammelte Abhandl. I, 370–482
- [13] I. Hughes, R. Mollin, *Totally positive units and squares*, Proc. Amer. Math. Soc. **87** (1983), 613–616
- [14] M. Knebusch, W. Scharlau, *Quadratische Formen und quadratische Reziprozitätsgesetze*, Math. Z. **121** (1971), 346–368
- [15] M. Kolster, *Quadratic Forms and Artin's Reciprocity Law*, Math. Z. **180** (1982), 81–90
- [16] J. Lagarias, *Signatures of units and congruences (mod 4) in certain real quadratic fields*, J. Reine Angew. Math. **301** (1978), 142–146
- [17] J. Lagarias, *Signatures of units and congruences (mod 4) in certain totally real fields*, J. Reine Angew. Math. **320** (1980), 1–5
- [18] J. Lagarias, *Signatures of units and congruences (mod 4) in certain real quadratic fields. II*, J. Reine Angew. Math. **320** (1980), 115–126
- [19] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer-Verlag 2000
- [20] F. Lemmermeyer, *Galois action on class groups*, J. Algebra **264** (2003), 553–564
- [21] F. Lemmermeyer, *Separants*, preprint 2005
- [22] F. Lemmermeyer, *Reciprocity Laws. From Kummer to Hilbert*, Springer-Verlag, in preparation
- [23] B. Orlat, *Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps de nombres*, Bull. Soc. Math. France **104** (1976), 301–307
- [24] M. Taylor, *Galois module structure of class groups and units*, Mathematika **22** (1975), 156–160

BILKENT UNIVERSITY, DEPT. MATHEMATICS, 06800 BILKENT, ANKARA
E-mail address: franz@fen.bilkent.edu.tr