Class Field Towers

Franz Lemmermeyer

September 7, 2010

Contents

Chapter 1

Some History

At present we know three different methods for constructing Hilbert class fields: an analytic method based on the theory of complex multiplication (which only works well over imaginary quadratic number fields), another one using the Stark conjectures on values of L-functions and their derivatives at $s = 0$, and an arithmetic method based on Kummer theory. In this chapter, we will survey our knowledge on class field towers, with special attention given to Scholz's and Taussky's work on the capitulation of ideal classes. In Chap. 3 we will give more details on constructing Hilbert class fields and present connections with Herbrand's theorem on the structure of the p-class group of $\mathbb{Q}(\zeta_p)$ and Leopoldt's Spiegelungssatz. We will also try to give a reasonably complete list of references.

1.1 The Prehistory

1.1.1 Fermat, Euler, and Gauß: Binary Quadratic Forms

The prehistory of Hilbert class fields starts with the work of Fermat and Euler on non-unique factorization in quadratic number fields, or rather on the representability of primes by binary quadratic forms. Fermat used his method of descente infinie to show that, for example, an odd prime p is the sum of two squares if and only if $p \equiv 1 \bmod 4$. As every student of algebraic number theory knows, this is a corollary of the fact that in $\mathbb{Z}[\sqrt{-1}\,]$ the theorem of unique factorization into prime elements holds (up to factors of units, of course). In a similar vein, the results

$$\left.\begin{array}{lcll} p = x^2 + 2y^2 & \Longleftrightarrow & p = 2 & \text{or } p \equiv 1, 3 \bmod 8 \\ p = x^2 + 3y^2 & \Longleftrightarrow & p = 3 & \text{or } p \equiv 1 \bmod 3, \end{array}\right\} (*)$$

also proved by Fermat, can be viewed as encoding the unique factorization theorem for the integral domains $\mathbb{Z}[\sqrt{-2}\,]$ and $\mathbb{Z}[\rho]$, where $\rho^2+\rho+1 = 0$. On the other hand, Fermat noticed that the corresponding result for $\mathbb{Z}[\sqrt{-5}\,]$ does not hold; in fact he conjectured that

$$\left.\begin{array}{lcl} p \equiv 1, 9 \bmod 20 & \Longrightarrow & p = x^2 + 5y^2 \\ p, q \equiv 3, 7 \bmod 20 & \Longrightarrow & pq = x^2 + 5y^2 \end{array}\right\} (**)$$

but could not find a proof. Neither could Euler, who conjectured more precisely that

$$\begin{array}{lcll} p = x^2 + 5y^2 & \Longleftrightarrow & p = 5 & \text{or } p \equiv 1, 9 \bmod 20 \\ 2p = x^2 + 5y^2 & \Longleftrightarrow & p = 2 & \text{or } p \equiv 3, 7 \bmod 20. \end{array}$$

(Studying the divisors of other quadratic forms, Euler was led to conjecture the quadratic reciprocity law.) It was Lagrange who finally found a proof for $(*)$ and $(**)$; he showed that

$$\begin{array}{lcll} p = x^2 + 5y^2 & \Longleftrightarrow & p = 5 & \text{or } p \equiv 1, 9 \bmod 20 \\ p = 2x^2 + 2xy + 3y^2 & \Longleftrightarrow & p = 2 & \text{or } p \equiv 3, 7 \bmod 20, \end{array}$$

which contains Euler's and Fermat's conjectures because of the identity

$$(2x^2+2xy+3y^2)(2u^2+2uv+3v^2)=(2xu+xv+yu+3yv)^2+5(xv-yu)^2.$$

The point is now that $(*)$ and $(**)$ imply the failure of unique factorization in $\mathbb{Z}[\sqrt{-5}\,]$: in fact,

$$3\cdot 7=1^2+5\cdot 2^2=(1+2\sqrt{-5})(1-2\sqrt{-5})$$

are two essentially different factorizations of 21 in $\mathbb{Z}[\sqrt{-5}\,]$. For quadratic number fields, Lagrange and Gauß were able to overcome the difficulties caused by non-unique factorization through the introduction of the *class group* of binary quadratic forms. The notion of a class field is not yet visible in their work, although Gauß' results on the genus class group can be interpreted as a theory of the genus class field; in fact, his theorem on genus characters is really Artin's reciprocity law for the genus class field of k.

1.1.2 Kummer and Dedekind: Ideals

The success of Gauß' theory of binary quadratic forms led Eisenstein and Dirichlet to believe that the language of forms was the correct one when it comes to describing the arithmetic of number fields. It turned out, however, that it is much more convenient to use the language of ideals, which Dedekind introduced to generalize Kummer's concept of ideal numbers; these had been invented by Kummer to compensate for the failure of unique factorization in cyclotomic number fields. In fact, using ideals, the factorizations

$$21=3\cdot 7=(1+2\sqrt{-5})(1-2\sqrt{-5})=(4+\sqrt{-5})(4-\sqrt{-5})$$

of elements in $\mathcal{O}_k=\mathbb{Z}[\sqrt{-5}\,]$ (in general, $\mathcal{O}_k$ denotes the ring of algebraic integers in k) turns into a single factorization of ideals

$$3\cdot 7\mathcal{O}_k=(3,1+2\sqrt{-5})(3,1-2\sqrt{-5})(7,1+2\sqrt{-5})(7,1-2\sqrt{-5}),$$

and the different factorizations of the elements come from different combinations of the ideal factors:

$$\begin{array}{rcl} 3\mathcal{O}_k & = & (3,1+2\sqrt{-5})(3,1-2\sqrt{-5}), \\ (1+2\sqrt{-5})\mathcal{O}_k & = & (3,1+2\sqrt{-5})(7,1+2\sqrt{-5}) \quad \text{etc.} \end{array}$$

Both Kummer and Dedekind tried to win over their contemporaries to the new language by showing that the ideal numbers (and ideals) of some number field k become actual numbers (or principal ideals) in certain finite extensions K/k. To see what they were doing let us look at the example $k=\mathbb{Q}(\sqrt{-5}\,)$ above. This field has class number 2, and the non-trivial ideal class is generated by the prime ideal $\mathfrak{2}=(2,1+\sqrt{-5})$. Euler's conjecture $(**)$ has the following ideal theoretical explanation: an odd prime $p\nmid \operatorname{disc} k=-20$ splits in $k/\mathbb{Q}$ if and only if $(-20/p)=+1$, i.e. iff $p\equiv 1,3,7,9 \bmod 20$. Suppose that $p\equiv 3,7 \bmod 20$; then $p\mathcal{O}_k=\mathfrak{p}\mathfrak{p}'$ splits, and $\mathfrak{p}$ cannot be principal, because $\mathfrak{p}=(x+y\sqrt{-5}\,)$ implies that $p=x^2+5y^2\equiv x^2+y^2\equiv 1 \bmod 4$. Similarly, the prime ideals above primes $p\equiv 1,9 \bmod 20$ necessarily generate principal ideals: otherwise these ideals would be in the same class as $\mathfrak{2}$, hence $\mathfrak{2}\mathfrak{p}=(x+y\sqrt{-5}\,)$ is principal, and then $2p=x^2+5y^2\equiv 6 \bmod 8$ yields the contradiction $p\equiv 3 \bmod 4$.

We have seen: if p is a prime, then $p\mathcal{O}_k=\mathfrak{p}\mathfrak{p}'$ if and only if $p\equiv 1,3,7,9 \bmod 20$; moreover,

$$\begin{array}{rcccl} \mathfrak{p} \text{ is principal} & \iff & p\equiv 1 \bmod 4 & \iff & \left(\frac{-1}{p}\right)=+1 \\ \mathfrak{2}\mathfrak{p} \text{ is principal} & \iff & p\equiv 3 \bmod 4 & \iff & \left(\frac{-1}{p}\right)=-1 \end{array}$$

Now suppose that K is a finite extension of k with the property that all ideals of k become principal when lifted to K; then there is an $\alpha\in\mathcal{O}_K$ auch that $\mathfrak{2}\mathcal{O}_K=\alpha\mathcal{O}_K$, and taking the relative norm to k we find $\mathfrak{2}^{(K:k)}=(N_{K/k}\alpha)$. But the $(K:k)$-th power of $\mathfrak{2}$ is principal if and only if $(K:k)$ is even (k has class number 2), therefore all such fields K must have even degree over k. There are a lot of quadratic extensions K/k in which $\mathfrak{2}$ becomes principal (actually, there are infinitely many): just take any quadratic number field F with even discriminants such that $2\mathcal{O}_F=\mathfrak{p}^2$ for some *principal* ideal $\mathfrak{p}=\alpha\mathcal{O}_F$ (for example, $F=\mathbb{Q}(\sqrt{m}\,)$ with $m=-2,-1,2,3,7,11,14,\ldots$). Then $K=kF$ is a number field such that $2\mathcal{O}_K=\alpha^2\mathcal{O}_K=\mathfrak{2}^2\mathcal{O}_K$, and the theorem of unique factorization into prime ideals implies

that $\mathfrak{2}\mathcal{O}_K = \alpha\mathcal{O}_K$ is indeed a principal ideal. This implies, by the way, that *every* ideal $\mathfrak{a}$ of $\mathcal{O}_k$ becomes principal in $\mathcal{O}_K$: if $\mathfrak{a}$ is principal in $\mathcal{O}_k$ then there is nothing to show, otherwise $\mathfrak{a}$ generates the same ideal class as $\mathfrak{2}$, i.e. there is a $\xi \in k$ such that $\mathfrak{a} = \mathfrak{2}\xi$, hence $\mathfrak{a}\mathcal{O}_K = \alpha\xi\mathcal{O}_K$ is also principal.

The fact that all ideals of k are becoming principal in K does of course not imply that K has class number 1, because the ideals coming from k might split. In fact, if a quadratic extension K of k has class number 1, then all the prime ideals $\mathfrak{p}$ in the ideal class of $\mathfrak{2}$ must stay inert: otherwise $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}\mathfrak{P}'$, and if $\mathfrak{P}$ were principal in K, taking the norm would yield that $\mathfrak{p}$ is principal in k. There is such an extension: we have seen above that the prime ideals in the ideal class $[\mathfrak{2}]$ are exactly those which stay inert in $k(\sqrt{-1}\,)/k$; in other words: the splitting of a prime ideal in the extension $k(\sqrt{-1}\,)/k$ depends only on the ideal class to which it belongs. For this reason, it was called a *class field* by Hilbert.

1.1.3 Kummer and Weber: Kummer Theory

In his quest for higher reciprocity laws, Kummer studied cyclic ℓ-extensions of the cyclotomic number field $\mathbb{Q}(\zeta_\ell)$ and developed what we now know as Kummer theory; some refinements are due to Weber who used these methods to prove that every abelian number field is subfield of some $\mathbb{Q}(\zeta_m)$. For a more modern presentation of Kummer theory we refer the reader to Chap. 3.

Throughout this section, we will make the following assumptions:

a) k/F is abelian with $G = \mathrm{Gal}\,(k/F)$, and $\zeta_n \in k$;

b) $K = k(\sqrt[n]{\mu})$, and $(K : k) = n$; in particular, $A = \mathrm{Gal}\,(K/k)$ is cyclic of order n.

It is well known that $k(\sqrt[n]{\mu}\,) = k(\sqrt[n]{\nu})$ if and only if $\mu = \nu^a\xi^n$, where $a \in \mathbb{N}$ is prime to n, and $\xi \in k^\times$. We begin by asking when K/F will be Galois:

Proposition 1.1.1. *Let $K/k/F$ be as above; then K/F is normal if and only if for every $\sigma \in G$ there exist $\alpha_\sigma \in k$ and $a(\sigma) \in \mathbb{N}$ such that $\mu^{\sigma - a(\sigma)} = \alpha_\sigma^m$; here $a(\sigma)$ is unique mod n, and α_σ is determined up to an n-th root of unity.*

Proof. If K/F is normal, then $\sqrt[n]{\mu}^\sigma \in K$. This implies that $k(\sqrt[n]{\mu}^\sigma\,) = k(\sqrt[n]{\mu})$, hence there exists an $a = a(\sigma) \in \mathbb{N}$ and a $\xi = \alpha_\sigma \in k^\times$ such that $\mu^\sigma = \mu^{a(\sigma)}\alpha_\sigma^n$. The other direction will be proved below by explicitly writing down the elements of the Galois group. □

Proposition 1.1.2. *Suppose that K/F is normal; then $\mu^{\sigma - a(\sigma)} = \alpha_\sigma^n$ for every $\sigma \in G$. Define $\omega = \sqrt[n]{\mu}$. Then every $\alpha \in K$ has a unique representation of the form $\alpha = \sum_{\nu=0}^{n-1} a_\nu\omega^\nu$, and the maps*

$$\widetilde{\sigma}_j : L \longrightarrow L : \sum_{\nu=0}^{n-1} a_\nu\omega^\nu \longmapsto \sum_{\nu=0}^{n-1} a_\nu^\sigma\zeta^{j\nu}\alpha_\sigma^\nu\omega^{\nu a(\sigma)}, \quad (0 \le j \le n-1)$$

are pairwise different automorphisms of K/F whose restrictions to k coincide with σ.

Proof. The maps $\widetilde{\sigma}_j, 0 \le j \le n-1$, are pairwise different because they act differently on ω; in fact $\widetilde{\sigma}_j(\omega) = \zeta^j\omega^{a(\sigma)}$. Moreover, their restriction to k coincides with σ because $\widetilde{\sigma}_j(a_0) = a_o^\sigma$. In order to prove that the $\widetilde{\sigma}_j$ are homomorphisms, it suffices to observe that $\widetilde{\sigma}_j(\omega^n) = \widetilde{\sigma}_j(\mu) = \mu^{a(\sigma)}\alpha_\sigma^n = (\omega\alpha_\sigma)^n = \widetilde{\sigma}_j(\omega)^n$. □

Proposition 1.1.3. *Suppose that $K = \mathbb{Q}(\sqrt[n]{\mu})$ with $\mu^\sigma = \mu^a\alpha_\sigma^m$ (this implies that K/F is normal) and put $\tau = \widetilde{\mathrm{id}}_1$; assume that $\zeta^\sigma = \zeta^r$, where σ generates G. Fix any extension of $\sigma \in G$ to an automorphism of K/F; this extension will also be denoted by σ). Then $\sigma^{-1}\tau\sigma = \tau^{a^{-1}r}$, where a^{-1} denotes the inverse of a modulo $(K : k)$.*

Proof. Put $\rho = \sigma^{-1}$; then from $\mu^\sigma = \alpha_\sigma\mu^a$ we get, by applying τ and σ,

$$\mu^{a\rho} = \mu\alpha_\sigma^{-\rho}, \quad \mu^{a\rho\tau} = \zeta\mu\alpha_\sigma^{-\rho}, \quad \mu^{a\rho\tau\sigma} = \zeta^\sigma\mu^a = \zeta^{raa^{-1}}\mu^a,$$

and this shows that $\mu^{\rho\tau\sigma} = \zeta^{ra^{-1}}\mu$. □

An exact sequence $E: 1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$ of finite groups is called an *extension* of G by A. E is called a *central extension* if $A \subseteq Z(\Gamma)$ is contained in the center of Γ (where we have identified A and its image in Γ). A normal tower $K/k/F$ of fields is called central if the exact sequence $1 \longrightarrow \mathrm{Gal}\,(K/k) \longrightarrow \mathrm{Gal}\,(K/F) \longrightarrow \mathrm{Gal}\,(k/F) \longrightarrow 1$ corresponding to the tower is central.

Corollary 1.1.4. *Suppose that $K = \sqrt[\nu]{\mu}$ with $\mu^\sigma = \mu^a \alpha_\sigma^m$ (i.e. K/F is normal); then $K/k/F$ is central if and only if $\zeta^\sigma = \zeta^{a(\sigma)}$ for every $\sigma \in G$.*

Proof. $K/k/F$ is central if and only if σ and τ commute, i.e. if and only if $r = a$. □

Since central extensions of cyclic groups are abelian, we get

Corollary 1.1.5. *Suppose that K/F is normal and that k/F is cyclic. Then K/F is abelian if and only if $\zeta^\sigma = \zeta^{a(\sigma)}$ for every $\sigma \in G$.*

Another way to put this is by introducing $\Omega = k^\times / k^{\times \ell}$: if $\omega \in \Omega$ and $\zeta^\sigma = \zeta^r$ for some σ generating $G = \mathrm{Gal}\,(k/F)$, then $k(\sqrt[\ell]{\omega})/k$ is abelian over F if and only if $\omega^\sigma = \omega^r$. It should be remarked that the situation becomes quite complicated if k/F is not cyclic. The case of abelian k/F has been discussed by Wojcik [533].

We will need the following lemma which was stated without proof by Furtwängler [378] for the construction of unramified quaternion extensions:

Lemma 1.1.6. *Let K/F be a quartic extension with $\mathrm{Gal}\,(K/F) \simeq (2,2)$; let σ, τ and $\sigma\tau$ denote its nontrivial automorphisms, and put $M = K(\sqrt{\mu})$. Then M/F is normal if and only if $\mu^{1-\rho} \stackrel{2}{=} 1$ for all $\rho \in \mathrm{Gal}\,(K/F)$. If this is the case, write $\mu^{1-\sigma} = \alpha_\sigma^2$, $\mu^{1-\tau} = \alpha_\tau^2$ and $\mu^{1-\sigma\tau} = \alpha_{\sigma\tau}^2$. It is easy to see that $\alpha_\rho^{1+\rho} = \pm 1$ for all $\rho \in \mathrm{Gal}\,(K/F)$; define $S(\mu, K/F) = (\alpha_\sigma^{1+\sigma}, \alpha_\tau^{1+\tau}, \alpha_{\sigma\tau}^{1+\sigma\tau})$ and identify vectors which coincide upon permutation of their entries. Then*

$$\mathrm{Gal}\,(M/F) \simeq \begin{cases} (2,2,2) & \Longleftrightarrow S(\mu, K/F) = (+1,+1,+1), \\ (2,4) & \Longleftrightarrow S(\mu, K/F) = (-1,-1,+1), \\ D_4 & \Longleftrightarrow S(\mu, K/F) = (-1,+1,+1), \\ H_8 & \Longleftrightarrow S(\mu, K/F) = (-1,-1,-1). \end{cases}$$

Moreover, M is cyclic over the fixed field of $\langle\rho\rangle$ if and only if $\alpha_\rho^{1+\rho} = -1$, and has type $(2,2)$ otherwise.

Proof. Let K/k be a quadratic extension and put $M = K(\sqrt{\mu})$ for some $\mu \in K$. Let σ denote the nontrivial automorphism of K/k. Then M/k is normal if and only if $M^\sigma = M$, and by Kummer Theory this is equivalent to $\mu^\sigma \stackrel{2}{=} \mu$, i.e. to $\mu^{1-\sigma} = \alpha_\sigma^2$ for some $\alpha_\sigma \in K^\times$. Since $(\alpha_\sigma^2)^{1+\sigma} = \mu^{(1-\sigma)(1+\sigma)} = 1$, we see that $\alpha_\sigma = \pm 1$.

Next suppose that M/k is normal; then $\widetilde{\sigma} : a + b\sqrt{\mu} \longmapsto a^\sigma + b^\sigma \alpha_\sigma \sqrt{\mu}$ defines an automorphism of M/k whose restriction to K/k coincides with σ. But now $\widetilde{\sigma}^2 : a + b\sqrt{\mu} \longmapsto a + b\alpha^{1+\sigma}\sqrt{\mu}$, hence $\widetilde{\sigma}$ has order 4 if $\alpha^{1+\sigma} = -1$ and order 2 if $\alpha^{1+\sigma} = +1$.

Now clearly M/F will be normal if and only if $\mu^\rho \stackrel{2}{=} \mu$ for all $\rho \in \mathrm{Gal}\,(K/F)$, i.e. if and only if M/k_i is normal for all three quadratic subextensions k_i of K/k. Moreover, the noncyclic groups of order 8 can be classified by their number of elements of order 4: this number is $0, 1, 2$ or 3 if $G \simeq (2,2,2), D_4, (2,4)$ or H_8, respectively. The claims of Lemma 1.1.6 now follow. □

We also will need to know the behaviour of certain prime ideals in Kummer extensions of prime degree:

Proposition 1.1.7. *Suppose that k contains the ℓth roots of unity, and let $K = k(\sqrt[\ell]{\omega})$ be a Kummer extension of odd prime degree ℓ. Let $\mathfrak{L}$ denote a prime ideal above ℓ and define an integer $a \in \mathbb{N}$ by $\mathfrak{L}^a \parallel (1 - \zeta_\ell)$. If ω is prime to ℓ, then K/k is unramified at $\mathfrak{L}$ if and only if $\omega \equiv \xi^\ell \bmod \mathfrak{L}^{a\ell}$.*

1.2 The Genesis of the Hilbert Class Field

1.2.1 Kronecker and Weber: Complex Multiplication

The first example of a Hilbert class field was given by Kronecker [1]. In fact, in his work on the theory of complex multiplication he discovered that the quadratic number field $k = \mathbb{Q}(\sqrt{-31})$ admitted a cyclic cubic unramified extension K/k, whose defining equation $(X^3 - 10X)^2 + 31(X^2 - 1)^2$ he computed using analytic techniques. He noticed that prime ideals in $\mathcal{O}_k$ split in K/k if and only if they are principal, and derived a reciprocity law from this observation (this is related to the singular numbers studied by Hilbert and Furtwängler):

Proposition 1.2.1. *Let $k = \mathbb{Q}(\sqrt{-31})$, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_k$ above a prime p which splits in $k/\mathbb{Q}$. Then $\mathfrak{p}$ is principal if and only if the fundamental unit ε_{93} of $K = \mathbb{Q}(\sqrt{93})$ is a cubic residue modulo the prime ideal above p in $\mathcal{O}_K$.*

Let $\mathbb{H} = \{z \in \mathbb{C} : \Im z > 0\}$ denote the upper halfplane. For every $\tau \in \mathbb{H}$, define the lattice $\Lambda = \Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$ in $\mathbb{C}$. Next define the invariants

$$\begin{array}{rcccl} g_2(\Lambda_\tau) & = & g_2(\tau) & = & 60 \sum'_{\omega \in \Lambda} \omega^{-4} \\ g_3(\Lambda_\tau) & = & g_3(\tau) & = & 140 \sum'_{\omega \in \Lambda} \omega^{-6} \\ \Delta(\Lambda_\tau) & = & \Delta(\tau) & = & g_2(\tau)^3 - 27 g_3(\tau)^2 \\ j(\Lambda_\tau) & = & j(\tau) & = & 1728 \frac{g_2(\tau)^3}{\Delta(\tau)}. \end{array}$$

Two lattices Λ and Λ' are called *homothetic* if there is a $\lambda \in \mathbb{C}^\times$ such that $\Lambda = \lambda\Lambda'$. Define $\mathrm{SL}_2(\mathbb{Z}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \det A = 1 \right\}$ and let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ act on $\mathbb{H}$ via $\gamma\tau := \frac{a\tau + b}{c\tau + d}$. The simplest properties of the invariants g_2, g_3, Δ and j are collected in

Proposition 1.2.2. *a) $\Delta(\Lambda) \neq 0$ for all lattices Λ in $\mathbb{C}$;*

b) two lattices Λ, Λ' are homothetic if and only if $j(\Lambda) = j(\Lambda')$;

c) $j(\tau') = j(\tau)$ if and only if there exists a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau' = \gamma\tau$;

d) the holomorphic map $j : \mathbb{H} \longrightarrow \mathbb{C}$ is surjective.

We say that a lattice Λ admits multiplication by $\alpha \in \mathbb{C}$ if $\alpha\Lambda \subseteq \Lambda$. Of course, every lattice admits multiplication by $\mathbb{Z}$. If Λ admits multiplication by $\alpha \in \mathbb{C} \backslash \mathbb{Z}$, then Λ is said to have complex multiplication. It is easy to see that such $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ are algebraic integers contained in some imaginary quadratic number field. In particular, the ring of integers $\mathcal{O}_K$ of an imaginary quadratic number field has complex multiplication by $\mathcal{O}_K$. Now the big surprise is

Theorem 1.2.3. *Write $\mathcal{O}_K = \mathbb{Z} + \tau\mathbb{Z}$ for some $\tau \in \mathcal{O}_K \cap \mathbb{H}$; then $j(\tau)$ is an algebraic integer of degree $h(K)$ over K, and $K(j(\tau))$ is the Hilbert class field of K.*

For example, the values

$$\begin{array}{rcrrcr} j(i) & = & 12^3 & j(\sqrt{-2}) & = & 20^3 \\ j\left(\frac{-1+\sqrt{-3}}{2}\right) & = & 0 & j\left(\frac{1+\sqrt{-7}}{2}\right) & = & (-15)^3 \end{array}$$

express the fact that the fields $\mathbb{Q}(\sqrt{-m})$ $(m = -1, -2, -3, -7)$ have class number 1. For more on Complex Multiplication and in particular on *Kronecker's Jugendtraum*, the generalization of the theorem of Kronecker and Weber to abelian extensions of imaginary quadratic fields, see Vladut [102] and Schertz [104], as well as Cox [298] and Kedlaya's thesis [643].

1.2.2 Hilbert: Hilbert Class Fields

Hilbert actually gave two different definitions of a class field. After the proof that unramified cyclic extensions K/k of prime degree ℓ can only exist if the class number $h(k)$ is divisible by ℓ (Satz 94 in Hilbert's Zahlbericht), he simply says that he will call such fields class fields. In his work on the quadratic reciprocity law he came up with a more precise definition:

> A finite extension K of a number field k is called a class field of k if exactly the principal prime ideals of $\mathcal{O}_k$ split completely in K/k.

Hilbert's work on the class fields (from now on called *Hilbert class fields*) of number fields with class number 2 led him to the conjectures 1–4 and 6 below. These were proved by Furtwängler, together with the Completeness theorem 5 which curiously is not mentioned in Hasse's Klassenkörperbericht:

Theorem 1.2.4. Main Theorem of Hilbert Class Field Theory
Let k be a number field.

1. *(Uniqueness) If k has a Hilbert class field then it is uniquely determined.*
2. *(Existence) The Hilbert class field k^1 of k exists.*
3. *(Reciprocity Law) k^1 is a finite normal extension of k, with Galois group $\mathrm{Gal}\,(k^1/k) \simeq \mathrm{Cl}(k)$.*
4. *(Decomposition Law) A prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$ splits into g prime ideals of inertia degree f, where $fg = (k^1 : k) = h(k)$ and f is the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(k)$.*
5. *(Completeness) The Hilbert class field is the maximal abelian unramified extension of k.*
6. *(Principal Ideal Theorem) Every ideal in k becomes principal in k^1.*

1.2.3 Furtwängler: Singular Numbers

Let K be a number field containing the ℓ-th roots of unity, and let e denote the ℓ-rank of $\mathrm{Cl}(K)$. The construction of the maximal elementary-abelian unramified ℓ-extension K_ℓ/K is done as follows: choose ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_e$ such that their ideal classes have order ℓ and generate a subgroup of order ℓ^e. Let $r = r_1 + r_2 - 1$ denote the $\mathbb{Z}$-rank of E_K and find generators $E_K = \langle \varepsilon_0 = \zeta_\ell, \varepsilon_1, \ldots, \varepsilon_r \rangle$ of the unit group. For $j = 1, \ldots, e$ put $\varepsilon_{r+j} = \alpha_j$, where ${\mathfrak{a}_j}^\ell = \alpha_j \mathcal{O}_K$. Now define the group $\mathfrak{E} = \langle \varepsilon_0, \ldots, \varepsilon_{r+e} \rangle$. There exist $\omega_1, \ldots, \omega_e \in \mathfrak{E}$ such that $K_\ell = K(\sqrt[\ell]{\omega_1}, \ldots, \sqrt[\ell]{\omega_e})$. These ω_j are called singular numbers.

Let $K_j = K(\sqrt[\ell]{\omega_j})$, and let $C_j = N_{K_j/K}\mathrm{Cl}(K_j)$ be the ideal class group corresponding to K_j/K. Then $(\mathrm{Cl}(K) : C_j) = \ell$, and for ideals $\mathfrak{a}$ prime to ℓ we have

$$\left(\frac{\omega_j}{\mathfrak{a}}\right)_\ell = 1 \quad \Longleftrightarrow \quad [\mathfrak{a}] \in C_j,$$

where $[\mathfrak{a}]$ denotes the ideal class of $\mathfrak{a}$; the class group C_j is said to *belong* to the singular number ω_j, or rather to the coset $\omega_j {K^\times}^\ell$.

From a theoretical point of view, the arithmetic construction of K_ℓ is quite easy if the ground field contains the ℓ-th roots of unity: all one needs to know are generators of the unit group and the class group of K. In fact it is sufficient to know generators of E_K/E_K^ℓ and ${}_\ell\mathrm{Cl}(K)$, where ${}_\ell\mathrm{Cl}(K)$ denotes the subgroup of $\mathrm{Cl}(K)$ annihilated by ℓ.

Now assume that K does *not* contain the ℓ-th roots of unity. Of course we start by adjoining the ℓ-th roots of unity first, i.e. we put $K' = K(\zeta_\ell)$; let σ be a generator of the cyclic group $\mathrm{Gal}\,(K'/K)$, and define $r \in \mathbb{F}_\ell^\times$ by $\zeta^\sigma = \zeta^r$. Next choose a basis $\eta_0 = \zeta_\ell, \eta_1, \ldots, \eta_\lambda$ of $E_{K'}/E_{K'}^\ell$ (this amounts to a knowledge of an ℓ-maximal unit group). Find generators $\mathfrak{b}_1, \ldots, \mathfrak{b}_f$ of ${}_\ell\mathrm{Cl}(K')$ and set $\mathfrak{b}_j^\ell = \beta_j \mathcal{O}_{K'}$. Now form the group

$$\mathfrak{E} = \langle \eta_0, \ldots, \eta_\lambda, \beta_1, \ldots, \beta_f \rangle {K'}^\ell \subseteq {K'}^\times / {K'}^{\times \ell};$$

then every primary $\omega \in \mathfrak{E}$ gives rise to an unramified cyclic extension $L' = K'(\sqrt[\ell]{\omega})$ of K'. If, in addition, $\omega^\sigma = \omega^r$ and $\omega \neq 1$ (recall that ω is a coset of the form $\omega = \alpha {K'}^{\times \ell}$), then L' is abelian over K, and since

L'/K' is unramified and $((K' : K), \ell) = 1$, the abelian subextension L of L'/K with degree ℓ over K is an unramified cyclic extension of degree ℓ over K.

What we have outlined above is the original naive approach of Furtwängler which was not meant to be used for actually constructing the class field but for proving its existence. In Chapter 3 we will use ideas of Herbrand, Leopoldt and G. Gras to show that there are more efficient methods for computing Hilbert (or ray) class fields.

1.2.4 Takagi: Class Field Theory

The class field theory of Hilbert and Furtwängler was generalized by Takagi by allowing abelian extensions to be ramified. Moreover, he defined the class field differently (we will only give the unramified part of Takagi's theory): Let K/k be a finite extension of number fields. Then $H_{K/k} = N_{K/k}\mathrm{Cl}(K)$ is a subgroup of $\mathrm{Cl}(k)$; call H the class group associated to K/k. Using analytic techniques dating back to Dirichlet, it is not hard to show that $(\mathrm{Cl}(k) : H_{K/k}) \leq (K : k)$ (in fact, the inequality is strict if K/k is not normal). Takagi called K a class field of k if $(\mathrm{Cl}(k) : H_{K/k}) = (K : k)$. Now Takagi proved

Theorem 1.2.5. Takagi's Main Theorem for Hilbert Class Fields
Let k be a number field.

1. *For every subgroup $H \leq \mathrm{Cl}(k)$, there exists a unique class field K such that $H = H_{K/k}$;*
2. *K/k is abelian, and $\mathrm{Gal}\,(K/k) \simeq \mathrm{Cl}(k)/H$;*
3. *K/k is unramified;*
4. *If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_k$, and if f is the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(k)/H$ (i.e. the smallest integer ≥ 1 such that $[\mathfrak{p}]^f \in H$) then $\mathfrak{p}$ splits into $g = (K : k)/f$ prime ideals in K;*
5. *Every unramified abelian extension K/k is a class field for some subgroup $H \leq \mathrm{Cl}(k)$.*
6. *Let K/k be a finite extension, and let k^1 denote the Hilbert class field of k, i.e. the class field for the class group $H = \{1\}$. Then $(\mathrm{Cl}(k) : N_{K/k}\mathrm{Cl}(K)) = (k^1 \cap K : k)$.*

If we put $H = \{1\}$ in Takagi's theory we get back Hilbert's conjectures (minus the principal ideal theorem); in fact, 4 shows that the prime ideals splitting completely in k^1/k are exactly the principal ones.

Takagi proved the isomorphism $\mathrm{Gal}\,(K/k) \simeq \mathrm{Cl}(k)/H$ by reducing the problem to cyclic groups and then counting their orders. It was Artin who found a canonical description: he defined a map $\left(\frac{K/k}{\cdot}\right) : \mathrm{Cl}(k) \longrightarrow \mathrm{Gal}\,(K/k)$ by letting $\left(\frac{K/k}{\mathfrak{p}}\right)$ be the Frobenius automorphism (where $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_k$), extending it multiplicatively to the group of fractional ideals in $\mathcal{O}_k$, and defining $\left(\frac{K/k}{c}\right) := \left(\frac{K/k}{\mathfrak{a}}\right)$, where $c = [\mathfrak{a}]$ (first, of course, he showed that $\left(\frac{K/k}{\mathfrak{a}}\right)$ does only depend on the ideal class of $\mathfrak{a}$).

Theorem 1.2.6. Artin's Reciprocity Law
Let K/k be an unramified abelian extension. Then the Artin map induces a short exact sequence

$$1 \longrightarrow H \longrightarrow \mathrm{Cl}(k) \longrightarrow \mathrm{Gal}\,(K/k) \longrightarrow 1,$$

where the kernel H of the Artin map is

$$H = \{c \in N_{K/k}\mathrm{Cl}(K)\} = \left\{c \in \mathrm{Cl}(k) : \left(\frac{K/k}{c}\right) = 1\right\}.$$

1.2.5 From Hilbert to Hasse

In this section we will sketch the development of the theory of class field towers excluding results related to the work of Golod and Shafarevich which will be discussed later. The need to study class field towers originated with the only conjecture of Hilbert concerning the Hilbert class field which turned out to be incorrect, namely the claim that the Hilbert class field of a number field with class number 4 has odd class number.

In fact, Hilbert's approach to proving the reciprocity law for fields with even class numbers was the following:

1. establishing the quadratic reciprocity law in fields with odd class number;
2. proving it in fields with even class number by applying the reciprocity law in its Hilbert class field which he conjectured implicitly to have odd class number.

It was Furtwängler [378] who realized in 1916 that the Hilbert 2-class field $k^1_{(2)}$ of a number field with 2-class group $\simeq (2,2)$ need not have an odd class number. He observed that Hilbert's method to prove the quadratic reciprocity law in k would still work if the 2-class field $k^2_{(2)}$ of $k^1_{(2)}$ had odd class number. This made Furtwängler ask the following question: does the p-class field tower of a number field k always terminate? Furtwängler proved that the answer is yes if $\mathrm{Cl}_p(k)$ is cyclic. He also thought he had shown that the Hilbert p-class field tower terminates after the first step if k contains a p-th root of unity and if $\mathrm{Cl}_p(k) \simeq (p,p)$. Wingberg [191] has shown, however, that there exist cyclotomic fields $\mathbb{Q}(\zeta_p)$ with $\mathrm{Cl}_p(k) \simeq (p,p)$ and infinite p-class field tower, contradicting Furtwängler's claim.

Scholz [136] proved that there exist p-class field towers of length $\geq n$ for every $n \in \mathbb{N}$. Nevertheless, Furtwängler and Artin conjectured that the p-class field tower always terminates, and Artin suggested that an improvement of the Minkowski bounds might lead to a proof; on the other hand the belief that the "group theoretical method" would not lead to a solution was shared by at least Artin, Furtwängler and Scholz (cf. Frei [437], Artin's letter to Hasse (Aug. 19, 1927), and Taussky [403]). They all conjectured that there is an infinite sequence Γ_n of finite p-groups with the property that $\Gamma_{n+1}/\Gamma^{(n)}_{n+1} \simeq \Gamma_n$ for each $n \geq 1$ (here $\Gamma^{(n)}$ denotes the n-th derived group). Already Magnus [483] gave an example of such a sequence for $\Gamma_1 \simeq (3,3,3)$, and after Hobby [492] had made some progress, J. P. Serre [499] proved

Theorem 1.2.7. *Let G be a finite p-group, and suppose that G is not cyclic and that $G \neq (2,2)$. Then there exists an infinite sequence Γ_n of p-groups such that $\Gamma_1 \simeq G$ and $\Gamma_{n+1}/\Gamma^{(n)}_{n+1} \simeq \Gamma_n$ for all $n \geq 1$.*

Concerning the normality of class field towers, Hasse observed (as before, we only give the part relating to unramified extensions):

Proposition 1.2.8. *Let K/k be a normal extension with $G = \mathrm{Gal}(K/k)$, and let L be an unramified abelian extension of K. Put $C = N_{L/K}\mathrm{Cl}(L)$; then L is*

a) normal over k if and only if $C = C^\tau$ for every $\tau \in G$;

b) central over K/k if and only if $c^{\tau-1} \in C$ for all $c \in \mathrm{Cl}(K)$ and all $\tau \in G$.

Proof. The functoriality of the Artin isomorphism shows that L^τ is the class field of $K^\tau = K$ for C^τ; therefore $L^\tau = L$ if and only if $C^\tau = C$.

For the second claim, let $\sigma = \left(\frac{L/K}{c}\right)$; then $\tau^{-1}\sigma\tau = \left(\frac{L/K}{\tau(c)}\right)$, hence σ is in the center of $\mathrm{Gal}(L/k)$ if and only if $c^{\tau-1}$ lies in the kernel C of the Artin symbol. □

Corollary 1.2.9. (Madden and Vélez [507]) *Let L/K be an unramified abelian extension of degree $n = (L:K)$, and let k be a subfield of k such that $(K:k) = 2$. If the class number h of k and n are relatively prime, then L/k is normal.*

Proof. Put $C = N_{L/K}\mathrm{Cl}(L)$ and let $c \in \mathrm{Cl}(K)$; since $(c^{1+\tau})^h = 1 \in C$ and since h is relatively prime to the order n of the factor group $\mathrm{Cl}(K)/C$, we conclude that already $c^{1+\tau} \in C$. Therefore, $c \in C$ implies $c^\tau \in C$, and Prop. 1.2.8a) proves our claim. □

The elementary properties of class field towers are collected in the following

Proposition 1.2.10. *Let k be a number field.*

1. *k possesses a finite extension K/k with class number 1 if and only if $(k^\infty : k)$ is finite, i.e. iff the class field tower terminates.*
2. *k possesses a finite extension K/k with p-class number 1 if and only if $(k_{(p)}^\infty : k)$ is finite, i.e. iff the p-class field tower terminates.*
3. *If K/k is a finite normal extension, then so is K^1/k.*
4. *k^n/k is a finite normal extension for all $n \in \mathbb{N}$.*
5. *If $\mathrm{Cl}_p(k)$ is cyclic, then the p-class field tower of k terminates at $k_{(p)}^1$.*
6. *If $\mathrm{Cl}_2(k) \simeq (2,2)$, then the 2-class field tower of k terminates after at most two steps, i.e. $k_{(2)}^\infty = k_{(2)}^1$ or $= k_{(2)}^2$.*

Properties (1) and (2) can be found in Holzer [139], (3) and (4) are simple consequences of the maximality of the Hilbert class field, (5) and (6) were first proved by Furtwängler and Taussky.

1.3 Genus Class Fields

1.3.1 Quadratic Number Fields

The genus class field for quadratic number fields was introduced and studied in R. Fueter's dissertation [5] supervised by D. Hilbert. Let $k = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with discriminant d; d is called a *prime discriminant* if d is a prime power up to sign. The prime discriminants are -4, ± 8, and $(-1)^{(p-1)/2}p$, where p is an odd prime.

Proposition 1.3.1. *The discriminant d of a quadratic number field can be written uniquely (up to order) as a product $d = d_1 \cdots d_t$ of prime discriminants d_j.*

The genus field (in the strict sense) k_{gen}^+ of k is defined to be the maximal extension contained in the Hilbert class field (in the strict sense) which is abelian over $\mathbb{Q}$. Fueter proved

Proposition 1.3.2. *Let $k = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with discriminant d; let $d = d_1 \cdots d_t$ be its factorization into prime discriminants. Then*

$$k_{gen}^+ = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_t}),$$

and $\mathrm{Gal}(k_{gen}^+/k) \simeq \mathrm{Cl}^+(k)/\mathrm{Cl}^+(k)^2$; in particular, $\mathrm{Cl}^+(k)$ has 2-rank equal to $t-1$, t being the number of finite primes ramified in $k/\mathbb{Q}$. A prime ideal $\mathfrak{p}$ in k splits completely in k_{gen}^+/k if and only if its ideal class is contained in the principal genus $\mathrm{Cl}^+(k)^2$. Moreover, all ambiguous ideal classes of k become principal in k_{gen}^+.

Similar results hold for the genus class field k_{gen} in the usual sense, which is the maximal extension of k which is unramified everywhere over k and abelian over $\mathbb{Q}$. If $d < 0$ or $d > 0$ and all the factors d_j are positive, then $k_{\mathrm{gen}} = k_{\mathrm{gen}}^+$; if, however, $d > 0$ and some of the d_j are negative, say $d_1, \ldots, d_s < 0$ and $d_{s+1}, \ldots, d_t > 0$, then $k_{\mathrm{gen}} = \mathbb{Q}(\sqrt{d_1 d_2}, \ldots, \sqrt{d_1 d_s}, \sqrt{d_{s+1}}, \ldots, \sqrt{d_t}) = k_{\mathrm{gen}} \cap \mathbb{R}$ is the maximal subextension of k_{gen}^+/k which is unramified everywhere. Again it can be shown that

$$\mathrm{rank}\,\mathrm{Cl}_2(K) = \begin{cases} t-1, & \text{if all } d_j > 0, \\ t-2, & \text{if some } d_j < 0. \end{cases}$$

The part of Prop. 1.3.2 about squares of ideal classes is called the Principal Genus Theorem for quadratic number fields. Its generalizations in class field theory and its connections with Hasse's norm

theorem were studied by Herbrand [230], E. Noether [231], Terada [236, 238], Kuniyoshi and Takahashi [239], Gold [258], and Gold and Madan [259].

Other references for the theory of genus class fields of quadratic number fields are Hasse [233], Kubokawa [261], Gogia and Luthar [57], Zagier [280], Cox [298], and Spearman and Williams [301]; see also the surveys of Antropov [269] and Frei [271] on the historical development of genera.

1.3.2 Abelian Number Fields

Much of the genus theory of quadratic number fields generalizes to cyclic extensions $K/\mathbb{Q}$ of odd prime degree ℓ. In fact, let f be the conductor of $K/\mathbb{Q}$; then $f = \prod_{j=1}^{t} f_j$ is the product of prime power conductors f_j, and the genus class field K_{gen} of K is the compositum of the cyclic extensions $\mathbb{Q}(f_j)$ of degree ℓ over $\mathbb{Q}$ and with conductor f_i. In particular, $\mathrm{Cl}(K)$ has a subgroup of type $(\mathbb{Z}/\ell\mathbb{Z})^{t-1}$. In contrast to the quadratic case, however, the ℓ-rank of $\mathrm{Cl}(K)$ can be strictly larger than $t-1$; in fact, Moriya [308] and Leopoldt [237] have shown:

Proposition 1.3.3. *Let $K/\mathbb{Q}$ be a cyclic extension of prime degree ℓ, and assume that exactly t primes ramify. Then*

$$t-1 \;\le\; r = \operatorname{rank} \mathrm{Cl}_\ell(K) \;\le\; (\ell-1)(t-1).$$

It is easy to see that the maximal unramified elementary abelian ℓ-extension of K has degree ℓ^r over K, and that $(K_{\text{gen}} : K) = \ell^{t-1}$. Moreover it is known that $\operatorname{rank} \mathrm{Cl}_\ell(K) = (\ell-1)(t-1)$ if $\mathrm{Cl}_\ell(K)$ contains an element of order ℓ^2, and this implies that the Hilbert ℓ-class field of K coincides with its genus class field if and only if $\mathrm{Cl}_\ell(K) \simeq (\mathbb{Z}/\ell\mathbb{Z})^{t-1}$ (cf. Li [94]).

For explicit constructions of genus class fields, see Ishida [256, 276, 278, 295], Bhaskaran [270, 288, 293], and Xianke [289]; applications to the structure of ideal class groups were studied by Cornell [247, 263, 281, 285, 290].

1.3.3 General Number Fields

The construction of the genus class field of quadratic number fields k is almost trivial, because it amounts to the factorization of $\operatorname{disc} k$ into prime discriminants. It was noticed by Goldstein [249] that this method can be generalized from quadratic extensions $k/\mathbb{Q}$ to quadratic extensions k/F of number fields F with class number 1 in the strict sense. To this end, let F be a field with class number 1 and observe that $\mathcal{O}_k$ has an $\mathcal{O}_F$-basis $\{1, \alpha\}$; then the *relative discriminant* $\operatorname{disc}(k/F) = \operatorname{disc}(1, \alpha)$ is determined up to squares of units. Such a discriminant is called a *prime discriminant* if $\operatorname{disc}(k/F)$ is a power of a prime ideal. Goldstein asked whether every discriminant $\operatorname{disc}(k/F)$ can be written as a product of prime discriminants. The answer given by him [249], Sunley [251, 275] and Davis [264] was

Theorem 1.3.4. *Let F be a number field with class number $h = 1$; then the following assertions are equivalent:*

1. *every discriminant $d = \operatorname{disc}(k/F)$ is a product of prime discriminants;*
2. *F has class number $h^+ = 1$ in the strict sense.*

In this case, the factorization $d = d_1 \cdots d_t$ is unique up to order, and the genus class field k^+_{gen} of k/F is given by $k^+_{gen} = F(\sqrt{d_1}, \ldots, \sqrt{d_t})$.

Questions concerning the genus field of quadratic extensions of $\mathbb{Q}(i)$ (which are not covered by the above theorem) were studied in Brandt [234] and Louboutin [299], the genus field of cyclic cubic extensions of $\mathbb{Q}(\sqrt{-3})$ was computed in Wada [246].

If k/F is an arbitrary finite extension of number fields, the genus field k_{gen} of k is defined to be the maximal field of type Kk such that K/F is abelian and Kk/k is unramified. The definition for normal fields was first given by Scholz in [567]. Examples for such extensions can be given easily: let $F/\mathbb{Q}$ be an extension of prime degree ℓ such that a prime $p \equiv 1 \bmod \ell$ is completely ramified. Then there exists a subfield $K \subseteq \mathbb{Q}(\zeta_p)$ of degree ℓ over $\mathbb{Q}$, and it is easily checked (for example by using Abhyankar's lemma)

that FK is contained in the genus field of F. This implies at once that the fields $\mathbb{Q}(\sqrt[\ell]{m})$, where m is divisible by a prime $p \equiv 1 \bmod \ell$, have class number divisible by ℓ (see Honda [34]).

If K/k is abelian, there is a formula for the genus class number of K going back to Gauss, Hilbert, and Furtwängler (see also Furuta [242]):

$$g_{K/k} = (K_{\text{gen}} : K) = h(k) \cdot \frac{\prod^{\infty} e(\mathfrak{p})}{(K:k)(E:H)},$$

where $\prod^{\infty} e(\mathfrak{p})$ is the product of the ramification indices of all primes $\mathfrak{p}$ in k (including the primes at ∞), E is the unit group of $\mathcal{O}_k$, and H is the subgroup of all units which are local norms at every completion of K/k.

The formula (1) for the genus class number of an abelian extension K/k was generalized to normal extensions by Furuta [242] and to arbitrary finite extensions of number fields by Taylor [252].

As an example of how to construct genus fields of general number fields, we present a result of Ishida [256]:

Theorem 1.3.5. *Let $K = \mathbb{Q}(\alpha)$ be a cubic number field, and suppose that α is a root of $x^3+ax+b \in \mathbb{Z}[x]$. Assume moreover that there is no prime p such that $p^2 \mid a$ and $p^3 \mid b$. Put*

$$\begin{aligned} P_1 &= \{p \equiv 1 \bmod 3 \text{ prime} : \ p \mid a, \ p \parallel b\}, \\ P_2 &= \{p \equiv 1 \bmod 3 \text{ prime} : \ p^2 \mid a, \ p^2 \parallel b\}, \end{aligned}$$

and define $P = P_1 \cup P_2 \cup \{3\}$ if $a \equiv 18 \bmod 27$ and $3^2 \parallel b$, or if $a \equiv 6 \bmod 9$ and $b \equiv \pm 1 \bmod 9$, and $P = P_1 \cup P_2$ otherwise. For $p \in P$, let $k^*(p)$ denote the unique cubic subfield of $\mathbb{Q}(\zeta_{p^2})$. Then the genus class field of k is given by

$$k_{gen} = \prod_{p \in P} k^*(p).$$

1.3.4 Central Extensions

Recall that a tower $L/K/k$ is called *central* if L/k is normal and if $\mathrm{Gal}\,(L/K)$ is contained in the center of $\mathrm{Gal}\,(L/k)$; in particular, L/K must be abelian. Central extensions have been studied in connection with some rather deep problems in algebraic number theory – here we will concentrate on the validity of Hasse's norm theorem.

Let k/F be a normal extension of number fields. Since k^1/F is normal, we have a group extension

$$E : 1 \longrightarrow \mathrm{Gal}\,(k^1/k) \longrightarrow \mathrm{Gal}\,(k^1/F) \longrightarrow \mathrm{Gal}\,(k/F) \longrightarrow 1.$$

Herz [24] claimed that the extension E always splits if $F = \mathbb{Q}$. Wyman [504] gave a counterexample and proved that E splits if $k/\mathbb{Q}$ is cyclic. In [506], Gold gave simpler proofs, and Cornell and Rosen [520] showed that the equality $k_{\text{gen}} = k_{\text{cen}}$ is necessary for E to split. For explicit examples of splitting and non-splitting extensions see Bond [528].

The main reference for the rest of this section is Jehne [273]. Let k be a number field; embedding $k^\times$ into the idele group J_k gives rise to the exact sequence $1 \longrightarrow k^\times \longrightarrow J_k \longrightarrow C_k \longrightarrow 1$, where C_k is called the idele class group of k. The kernel of the canonical map $J_k \longrightarrow I_k$ of the idele group onto the group of fractional ideals is the unit idele group U_k, giving rise to another exact sequence $1 \longrightarrow U_k \longrightarrow J_k \longrightarrow I_k \longrightarrow 1$. Finally there is the classical sequence

$$1 \longrightarrow H_k \longrightarrow I_k \longrightarrow \mathrm{Cl}_k \longrightarrow 1$$

defining the ideal class group Cl_k as the factor group of the group I_k of fractional ideals modulo the group H_k of principal ideals. All these exact sequences fit into a commutative diagram (the fundamental

square)

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & E_k & \longrightarrow & k^\times & \longrightarrow & H_k & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & U_k & \longrightarrow & J_k & \longrightarrow & I_k & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathcal{E}_k & \longrightarrow & C_k & \longrightarrow & \mathrm{Cl}_k & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

Now Jehne considers exact sequences

$$1 \longrightarrow A_k \longrightarrow B_k \longrightarrow C_k \longrightarrow 1 \tag{1.1}$$

of certain abelian groups attached to number fields k (actually we will only consider the six exact sequences contained in the fundamental square). For normal extensions K/k with Galois group G and relative norm $N = N_{K/k}$ he applies the snake lemma to the diagram (ABC)

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A_K & \longrightarrow & B_K & \longrightarrow & C_K & \longrightarrow & 1 \\
 & & \downarrow N & & \downarrow N & & \downarrow N & & \\
1 & \longrightarrow & A_k & \longrightarrow & B_k & \longrightarrow & C_k & \longrightarrow & 1
\end{array}$$

and gets the exact sequence

$$\begin{aligned}
1 \longrightarrow \quad {}_N A_K \quad \longrightarrow \quad {}_N B_K \quad \longrightarrow \quad {}_N C_K \quad \xrightarrow{\delta} \\
A_k/NA_K \longrightarrow B_k/NB_K \longrightarrow C_k/NC_K \longrightarrow 1.
\end{aligned}$$

The connection homomorphism δ maps an element $a = \alpha A_K \in {}_N C_K$ to $\delta(a) = N_{K/k}(\alpha) N_{K/k} A_K$; since α is an element of B_K whose relative norm lands in A_k, this is well defined. This shows that $\mathrm{im}\delta = A_k \cap N_{K/k} B_K / N_{K/k} A_K =: [A, B]$; Jehne calls $[A, B]$ the knot associated to the sequence (1.1). Now we split up the exact sequence at δ and get two short exact sequences involving the knot:

$$1 \longrightarrow {}_N A_K \longrightarrow {}_N B_K \longrightarrow {}_N C_K \longrightarrow [A, B] \longrightarrow 1 \tag{1.2}$$

$$1 \longrightarrow [A, B] \longrightarrow A_k/NA_K \longrightarrow B_k/NB_K \longrightarrow C_k/NC_K \longrightarrow 1. \tag{1.3}$$

The exact sequences of the fundamental square thus give rise to six knots. But one of them is trivial:

Lemma 1.3.6. $[U, J] = 1$.

Thus we are left with five different knots:

1. the number knot $\nu = \nu_{K/k} = [K^\times, I_K] = k^\times \cap N J_K / N K^\times$;
2. the first unit knot $\omega = \omega_{K/k} = [E_K, K^\times] = E_k \cap N K^\times / N E_K$;
3. the second unit knot $\omega' = \omega'_{K/k} = [E_K, U_K] = E_k \cap N U_K / N E_K$;
4. the ideal knot $\delta = \delta_{K/k} = [H_K, I_K] = H_k \cap N I_K / N H_K$;
5. the idele knot $\gamma = \gamma_{K/k} = [\mathcal{E}_K, C_K] = \mathcal{E}_k \cap N C_K / N \mathcal{E}_K$.

The knots are functorial in the following sense: if we have two diagrams (ABC) and $(A'B'C')$, then we get a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & {}_NA_K & \longrightarrow & {}_NB_K & \longrightarrow & {}_NC_K & \longrightarrow & [A,B] & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & {}_NA'_K & \longrightarrow & {}_NB'_K & \longrightarrow & {}_NC'_K & \longrightarrow & [A',B'] & \longrightarrow & 1 \end{array}$$

Applying (1.2) to the last two rows of the fundamental square (and keeping in mind that $[U,J]=1$) we get an exact and commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & {}_NU_K & \longrightarrow & {}_NJ_K & \longrightarrow & {}_NI_K & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & {}_N\mathcal{E}_K & \longrightarrow & {}_NC_K & \longrightarrow & {}_N\mathrm{Cl}_K & \longrightarrow & \gamma & \longrightarrow & 1 \end{array} \tag{1.4}$$

Now we need the following version of the snake lemma (which can be proved by a simple diagram chase):

Proposition 1.3.7. *Given a commutative diagram*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 1 \\ & & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & & \\ 1 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

with exact rows, there exists an exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \ker f & \longrightarrow & \ker\alpha & \longrightarrow & \ker\beta & \longrightarrow & \ker\gamma \\ & & & & & & & & \delta\downarrow \\ 1 & \longleftarrow & \operatorname{coker} g' & \longleftarrow & \operatorname{coker}\gamma & \longleftarrow & \operatorname{coker}\beta & \longleftarrow & \operatorname{coker}\alpha \end{array}$$

Applying it to diagram (1.4) yields an exact sequence

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & {}_NE_K & \longrightarrow & {}_NK^\times & \longrightarrow & {}_NH_K & \longrightarrow & & & \\ & & \omega' & \longrightarrow & \nu & \longrightarrow & \delta & \longrightarrow & \gamma & \longrightarrow & 1, \end{array}$$

and if we break up this sequence at ω' we get

Theorem 1.3.8. The Fundamental Knot Sequence

$$1 \longrightarrow \omega_{K/k} \longrightarrow \omega'_{K/k} \longrightarrow \nu_{K/k} \longrightarrow \delta_{K/k} \longrightarrow \gamma_{K/k} \longrightarrow 1.$$

Now Scholz's unit knot ω^0 is the quotient $\omega'/\omega \simeq E_k \cap NU_K/E_k \cap NK^\times$; defining yet another knot $\delta^0 := \operatorname{im}(\nu \longrightarrow \delta)$, the fundamental knot sequence gives becomes

Theorem 1.3.9. Scholz's Knot Sequence $1 \longrightarrow \omega^0_{K/k} \longrightarrow \nu_{K/k} \longrightarrow \delta^0_{K/k} \longrightarrow 1.$

For cyclic extensions K/k, Hasse has shown that $\nu_{K/k}=1$, and Scholz introduced knots in order to study the validity of Hasse's norm theorem in non-cyclic extensions. The knots defined above can be interpreted in terms of Galois groups of certain subfields in the Hilbert class field of K:

Theorem 1.3.10. *We have* $\delta^0 \simeq \operatorname{Gal}(K_{cen}/K_{gen})$, $\delta \simeq \operatorname{Gal}(K_{cen}/k^1K)$, *and* $\gamma \simeq \operatorname{Gal}(K_{gen}/k^1K)$.

The middle term of Scholz's exact knot sequence can also be related to the *Schur Multiplier* $\mathfrak{M}(G)$ of the Galois group $G = \operatorname{Gal}(K/k)$. The Schur Multiplier of a finite group G is most easily defined as follows: a group extension $E: 1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$ is called central if $A \subseteq Z(G)$; E is called a *covering* if $A \subseteq \Gamma'$. Schur [563] has shown that the order of the groups A in central coverings is bounded. Moreover, the groups A in any maximal central covering are mutually isomorphic. The isomorphism class of A in a maximal central covering is called the Schur Multiplier of G, the groups Γ are called *covering groups* of G.

Example 1.3.1. *$G = (2,2)$ has Schur Multiplier $\mathfrak{M}(G) = \mathbb{Z}/2\mathbb{Z}$; G has two non-isomorphic covering groups, namely the dihedral group D_4 and the quaternion group H_8, both of order 8.*

The structure of $\mathfrak{M}(G)$ for abelian groups G is known since Schur [563]:

Proposition 1.3.11. *Let G be an abelian p-group, and let $C(p^a)$ denote a cyclic group of order p^a. Write $G = C(p^{n_1}) \times \ldots \times C(p^{n_m})$ in such a way that $n_1 \geq n_2 \geq \ldots \geq n_m$. Then*

$$\mathfrak{M}(G) \simeq C(p^{n_2}) \times C(p^{n_3})^2 \times \ldots \times C(p^{n_m})^{m-1}.$$

In particular, the p-rank of $\mathfrak{M}(G)$ is $\binom{m}{2}$.

Since the Schur multiplier can be defined cohomologically by $\mathfrak{M}(G) \simeq H^2(G, \mathbb{Q}/\mathbb{Z})$, we can now prove the theorem of Scholz [564, 567] and Tate:

Theorem 1.3.12. *Let K/k be a normal extension with Galois group G; then there is an exact sequence $\coprod_{\mathfrak{P}} \mathfrak{M}(G_{\mathfrak{P}})\hat{} \longrightarrow \mathfrak{M}(G)\hat{} \longrightarrow \nu_{K/k} \longrightarrow 1$, where $G_{\mathfrak{P}}$ denotes the Galois group of the extension $K_{\mathfrak{P}}/k_{\mathfrak{p}}$, and where $K_{\mathfrak{P}}$ and $k_{\mathfrak{p}}$ are the completions of K and k at the prime ideal $\mathfrak{P} \mid \mathfrak{p}$, respectively. Moreover, $A\hat{} = \mathrm{Hom}\,(A, \mathbb{Q}/\mathbb{Z})$ denotes the dual of an abelian group A.*

Proof. For a prime $\mathfrak{p}$ in $\mathcal{O}_k$ and a prime $\mathfrak{P}$ in $\mathcal{O}_K$ above $\mathfrak{p}$ let $k_{\mathfrak{p}}$ and $K_{\mathfrak{P}}$ denote the completions of k and K at these primes; moreover, put $G_{\mathfrak{p}} = \mathrm{Gal}\,(K_{\mathfrak{P}}/k_{\mathfrak{p}})$. Consider the exact sequence

$$1 \longrightarrow {}_N K^{\times} \longrightarrow {}_N J_K \longrightarrow {}_N C_K \longrightarrow \nu \longrightarrow 1.$$

Then ${}_N C_K = H^{-1}(G, C_K)$ and, by global class field theory, ${}_N J_K = H^{-1}(G, J_K) \simeq \coprod_{\mathfrak{p}} H^{-1}(G_{\mathfrak{p}}, K_{\mathfrak{P}}^{\times})$. Tate reciprocity shows that $H^{-1}(G_{\mathfrak{p}}, K_{\mathfrak{P}}^{\times}) \simeq H^{-3}(G_{\mathfrak{p}}, \mathbb{Z})$ and $H^{-1}(G, C_K) \simeq H^{-3}(G, \mathbb{Z})$. Moreover, the duality theorem of the cohomology of finite groups $H^{-q}(G, \mathbb{Q}/\mathbb{Z}) \simeq H^q(G, \mathbb{Z})\hat{} \simeq H^{q-1}(G, \mathbb{Q}/\mathbb{Z})\hat{}$ gives $H^{-3}(G, \mathbb{Z}) \simeq H^2(G, \mathbb{Q}/\mathbb{Z})\hat{}$ and $H^{-3}(G_{\mathfrak{p}}, \mathbb{Z}) \simeq H^2(G_{\mathfrak{p}}, \mathbb{Q}/\mathbb{Z})\hat{}$. □

Observe that it contains Hasse's norm theorem as a corollary: the Schur multiplier of cyclic groups is trivial, so we conclude that $\nu_{K/k} = 1$.

Corollary 1.3.13. *Let K/k be a finite unramified normal extension with Galois group $G = \mathrm{Gal}\,(K/k)$; then $\nu_{K/k} \simeq \mathfrak{M}(G)$.*

In fact, if K/k is unramified then so is $K_{\mathfrak{P}}/k_{\mathfrak{p}}$; but unramified extensions of local fields are cyclic, hence $\mathfrak{M}(G_{\mathfrak{P}}) = 1$ for all primes $\mathfrak{P}$.

We continue to assume that K/k is unramified; then every unit in E_k is a local norm, i.e. $E_k \cap N U_K = E_k$, and we find $\omega^0_{K/k} \simeq E_k / E_k \cap N K^{\times}$. Now Scholz's knot sequence implies

Corollary 1.3.14. *Let K/k be a finite unramified normal extension with Galois group $G = \mathrm{Gal}\,(K/k)$; then there is an exact sequence*

$$1 \longrightarrow E_k/E_k \cap N K^{\times} \longrightarrow \mathfrak{M}(G)\hat{} \longrightarrow \mathrm{Gal}\,(K_{cen}/K_{gen}) \longrightarrow 1.$$

Remark 1. *If we regard the exact sequences above not as exact sequences of Galois modules but of abstract abelian groups, then we may replace $\mathfrak{M}(G)\hat{}$ by $\mathfrak{M}(G)$, since the dual of a finite abelian group is (noncanonically) isomorphic to the group itself.*

Cor. 1.3.14 is a very powerful result for showing that certain fields have nontrivial class numbers. Consider e.g. an imaginary quadratic number field k such that $\mathrm{Cl}_2\,(k) = (2,2,2)$. Then the Hilbert 2-class field k^1 coincides with k_{gen}, and $G = \mathrm{Gal}\,(k_{\mathrm{gen}}/k) \simeq (2,2,2)$; but $\mathfrak{M}(G) \simeq (2,2,2)$, and $E_k/E_k \cap N K^{\times}$ is a factor group of $\mathbb{Z}/2\mathbb{Z}$ (since the unit group $E_k = \{-1, 1\}$). Now Corollary 1.3.14 implies that $\mathrm{Gal}\,(K_{\mathrm{cen}}/K_{\mathrm{gen}})$ contains a subgroup of type $(2,2)$ (cf. Benjamin [189]).

Here is a related observation due to Iwasawa [408]:

Proposition 1.3.15. *Let k be a number field whose p-class field tower terminates with K, and put $G = \mathrm{Gal}\,(K/k)$; then $E_k/N E_K \simeq \mathfrak{M}(G)$.*

This has some interesting consequences: take, for example, an imaginary quadratic number field k and assume that its 2-class field tower terminates with K. Then $G = \mathrm{Gal}\,(K/k)$ is a 2-group whose Schur multiplier has order at most 2; this shows that there are many 2-groups which cannot occur as $\mathrm{Gal}\,(k^\infty/k)$ for imaginary quadratic k. The question which groups can be realized as $\mathrm{Gal}\,(k^\infty/k)$ remains open, because there are 2-groups whose Schur multipliers have order at most 2 and which do not occur as $\mathrm{Gal}\,(k^\infty/k)$ for imaginary quadratic k.

As another application we give a result due to Bond [448]:

Corollary 1.3.16. *Let k be a number field, and let r denote the p-rank of E_k/E_k^p. If the p-class field tower of k is abelian, then* $\mathrm{rank}\,\mathrm{Cl}_p\,(k) \leq \frac{1+\sqrt{1+8r}}{2}$.

Proof. Assume that the p-class field tower terminates with $K = k^{(1)}$. Then by Prop. 1.3.15, $\mathfrak{M} = \mathfrak{M}(\mathrm{Gal}\,(K/k)) \simeq E_k/N_{K/k}E_K$. This implies that $\mathfrak{M}$ has p-rank at most r. On the other hand, the p-rank of M is just $\binom{s}{2}$ by Prop. 1.3.11, where s denotes the p-rank of $Cl_p(k)$.

Now $s(s-1)/2 \leq r \iff (2s-1)^2 \leq 1+8r$, and taking the square root yields our claim. □

Proposition 1.3.17. *If the p-class field tower of k terminates with K, then*

$$E_k \cap N_{K/k}K^* = N_{K/k}E_K.$$

Proof. In this case $K_{\mathrm{cen}} = K_{\mathrm{gen}} = K$, hence Cor. 1.3.14 gives $E_k/E_k \cap NK^\times \simeq \mathfrak{M}(G)$. On the other hand, Prop. 1.3.15 shows that $E_k/NE_K \simeq \mathfrak{M}(G)$. Our claim follows. □

Finally, here's a similar result due to D. Folk [465]:

Proposition 1.3.18. *Let K/k be a normal extension and put $L = K^1$; then $N_{L/k}L^\times \cap E_k \subseteq N_{K/k}E_K$.*

We also remark that Jehne has derived the following bound for the rank of p-class groups from his knot sequences:

Proposition 1.3.19. *Let K/k be a cyclic extension of prime degree p. Then*

$$\mathrm{rank}\,\mathrm{Cl}_p\,(K/k) \geq \#\mathrm{Ram}(K/k) - \mathrm{rank}_p E_k/H - 1.$$

For a proof, observe that $\delta \simeq \mathrm{Gal}\,(K_{\mathrm{cen}}/k^1K)$; this implies of course that $\mathrm{rank}\mathrm{Cl}_p\,(K/k) \geq \mathrm{rank}_p\delta$. The exact sequence $\nu \longrightarrow \delta \longrightarrow \gamma \longrightarrow 1$ gives $\mathrm{rank}_p\delta \geq \mathrm{rank}_p\gamma$. The exact sequence

$$1 \longrightarrow \gamma \longrightarrow \mathcal{E}_k/N\mathcal{E}_K \longrightarrow H^0(C_K) \longrightarrow$$

shows that $\mathrm{rank}_p\gamma \geq \mathrm{rank}_p\mathcal{E}_k/N\mathcal{E}_K - \mathrm{rank}_p H^0(C_K)$. But $H^0(C_K) \simeq G^{ab} \simeq \mathbb{Z}/p\mathbb{Z}$, hence $\mathrm{rank}_p H^0(C_K) = 1$. Finally, the exact sequence $1 \longrightarrow E_k/E_k \cap NU_K \longrightarrow H^0(U_K) \longrightarrow \mathcal{E}_k/N\mathcal{E}_K \longrightarrow 1$ implies $\mathrm{rank}_p\mathcal{E}_k/N\mathcal{E}_K \geq t_{K/k} - \mathrm{rank}_p E_k/E_k \cap NU_K$.

1.4 2-Class fields

1.4.1 Quadratic Number Fields

The first example of an unramified extension not contained in the genus class field is due to Hilbert [2] himself: he considered the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{-7}\,)$. This field has class number 2 and Hilbert class field $L = K(\sqrt{\mu}\,)$, $\mu = (\sqrt{2}-1)(\sqrt{2}-\sqrt{-7}\,)$. This follows from μ being an ideal square satisfying the congruence $\mu \equiv \left(1 - \sqrt{2}\frac{1-\sqrt{-7}}{2}\right)^2 \bmod 4$. Since K is the genus class field of $k = \mathbb{Q}(\sqrt{-14}\,)$ and $\mathrm{Cl}(k) \simeq C_4$, L also is the Hilbert class field of k.

The first structured approach to the construction of 2-class fields is due to Fueter [5] and was taken up later in more detail by Rédei, Reichardt and Scholz in their papers [12], [15], [16], and [535]. Let k be a quadratic number field with discriminant d; a factorization $d = d_1 \cdot d_2$ of d into relatively prime discriminants d_1 and d_2 will be called a C_4-factorization if the primes dividing d_1 split in $\mathbb{Q}(\sqrt{d_2}\,)$ and vice versa, i.e. if $(d_1/p_2) = (d_2/p_1) = +1$ for all primes $p_j \mid d_j$. An extension K/k is called a C_4-extension if K/k is normal with $\mathrm{Gal}\,(K/k) \simeq C_4$, the cyclic group of order 4. The following theorem summarizes the work of Fueter, Rédei and Reichardt on the construction of unramified C_4-extensions of quadratic number fields (bear in mind that 'unramified' means 'unramified outside ∞'):

Theorem 1.4.1. *Let k be a quadratic number field with discriminant d. There is a bijection between unramified cyclic C_4-extensions and C_4-factorizations of $d = \operatorname{disc} k$. In fact, if K/k is an unramified C_4-extension, then $K/\mathbb{Q}$ is normal with $\operatorname{Gal}(K/\mathbb{Q}) \simeq D_4$. The quartic normal extension $F/\mathbb{Q}$ contained in K can be written in the form $F = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. A careful examination of the decomposition and inertia groups of the ramifying primes shows that $(d_1, d_2) = 1$ and that $d = d_1 \cdot d_2$ is a C_4-factorization.*

Conversely, if $d = d_1 \cdot d_2$ is a C_4-factorization of d, then the diophantine equation $X^2 - d_1 Y^2 = d_2 Z^2$ has a nontrivial primitive solution (x, y, z), and the extension $K = k(\sqrt{d_1}, \sqrt{\mu})$, where $\mu = x + y\sqrt{d_1}$, is a C_4-extension of k unramified outside 2∞. By choosing the signs of x, y, z suitably one can make K/k unramified outside ∞.

Example 1.4.1. *Let $k = \mathbb{Q}(\sqrt{-3 \cdot 11 \cdot 23})$ (cf. Daberkow [112]); then $d = -11 \cdot 69$ is a C_4-factorization, and in fact $\operatorname{Cl}(k) \simeq (2, 4, 3)$. The genus class field is $k_{gen} = k(\sqrt{-3}, \sqrt{-11})$, and the unramified cyclic quartic extension K/k is constructed by solving $x^2 + 11y^2 = 69z^2$; the solution $x = 5$, $y = 2$, $z = 1$ yields $K = k(\sqrt{-11}, \sqrt{-5 + 2\sqrt{-11}})$.*

The question of whether the cyclic quartic extension K/k constructed in Theorem 13.1. is real or not was answered by Scholz [535]. Clearly this question is only interesting if both d_1 and d_2 are positive. Moreover, if one of them, say d_1, is divisible by a prime $q \equiv 3 \bmod 4$, then there always exists a real cyclic quartic extension K/k: this is so because $\alpha = x + y\sqrt{d_1}$ as constructed above is either totally positive or totally negative (since it has positive norm), hence either $\alpha \gg 0$ or $-q\alpha \gg 0$, so either $k(\sqrt{\alpha})$ or $k(\sqrt{-q\alpha})$ is the desired extension. We may therefore assume that d is not divisible by a prime $q \equiv 3 \bmod 4$, i.e. that d is the sum of two squares. Then Scholz [535] has shown

Proposition 1.4.2. *Let k be a real quadratic number field with discriminant d, and suppose that d is the sum of two squares. Assume moreover that $d = d_1 \cdot d_2$ is a C_4-factorization. Then the cyclic quartic C_4-extensions K/k containing $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ are real if and only if $(d_1/d_2)_4 (d_2/d_1)_4 = +1$. Moreover, if there exists an octic cyclic unramified extension L/k containing K, then $(d_1/d_2)_4 = (d_2/d_1)_4$.*

If d_1 and d_2 are prime, we can say more ([535]):

Theorem 1.4.3. *Let $k = \mathbb{Q}(\sqrt{d})$ be a real quadratic number field, and suppose that $d = \operatorname{disc} k = d_1 d_2$ is the product of two positive prime discriminants d_1, d_2. Let $h(k)$, $h^+(k)$ and ε denote the class number, the class number in the strict sense, and the fundamental unit of $\mathcal{O}_k$, respectively; moreover, let ε_1 and ε_2 denote the fundamental units of $k_1 = \mathbb{Q}(\sqrt{d_1})$ and $k_2 = \mathbb{Q}(\sqrt{d_1})$. There are the following possibilities:*

1. *$(d_1/d_2) = -1$: then $h(k) = h^+(k) \equiv 2 \bmod 4$, and $N\varepsilon = -1$.*
2. *$(d_1/d_2) = +1$: then $(\varepsilon_1/d_2) = (\varepsilon_2/d_1) = (d_1/d_2)_4 (d_2/d_1)_4$, and 1.4.1 shows that there is a cyclic quartic subfield K of k^1 containing $k_1 k_2$;*

   i) $(d_1/d_2)_4 = -(d_2/d_1)_4$: then $h^+(k) = 2 \cdot h(k) \equiv 4 \bmod 8$, $N\varepsilon = +1$, and K is totally complex;

   ii) $(d_1/d_2)_4 = (d_2/d_1)_4 = -1$: then $h^+(k) = h(k) \equiv 4 \bmod 8$, $N\varepsilon = -1$, and K is totally real.

   iii) $(d_1/d_2)_4 = (d_2/d_1)_4 = +1$: then $h^+(k) \equiv 0 \bmod 8$, and K is totally real.

Here $(d_1/d_2)_4$ denotes the rational biquadratic residue symbol (multiplicative in both numerator and denominator). Notice that $(p/8)_4 = +1$ for primes $p \equiv 1 \bmod 16$ and $(p/8)_4 = -1$ for primes $p \equiv 9 \bmod 16$. Moreover, (ε_1/p_2) is the quadratic residue character of $\varepsilon_1 \bmod \mathfrak{p}$ (if $p_2 \equiv 1 \bmod 4$), where $\mathfrak{p}$ is a prime ideal in k_1 above p_2; for $d_2 = 8$ and $d_1 \equiv 1 \bmod 8$, the symbol $(\varepsilon_1/8)$ is defined by $(\varepsilon_1/8) = (-1)^{T/4}$, where $\varepsilon_1 = T + U\sqrt{d_1}$.

Corollary 1.4.4. *Suppose that $q = d_2 \equiv 1 \bmod 4$ is fixed; then*

$$\begin{array}{lcccl} 4 | h^+(k) & \iff & (d_1/d_2) = 1 & \iff & p \in \operatorname{Spl}(\Omega_4^+(d_2)/\mathbb{Q}) \\ 4 | h(k) & \iff & (d_1/d_2)_4 = (d_2/d_1)_4 & \iff & p \in \operatorname{Spl}(\Omega_4(d_2)/\mathbb{Q}) \\ 8 | h^+(k) & \iff & (d_1/d_2)_4 = (d_2/d_1)_4 = 1 & \iff & p \in \operatorname{Spl}(\Omega_4^+(d_2)/\mathbb{Q}) \end{array}$$

Here, the *governing fields* $\Omega_j(d_2)$ are defined by

$$\Omega_4^+(d_2) \;=\; \mathbb{Q}(i,\sqrt{d_2}\,), \quad \Omega_4(d_2) \;=\; \mathbb{Q}(i,\sqrt{d_2},\sqrt{\varepsilon_2}\,), \quad \Omega_8^+(d_2) \;=\; \mathbb{Q}(i,\sqrt[4]{d_2},\sqrt{\varepsilon_2}\,).$$

The reason for studying governing fields comes from the fact that sets of primes splitting in a normal extension have Dirichlet densities. The existence of fields governing the property $8|h^+(k)$ allows us to conclude that there are infinitely many such fields. Governing fields for the property $8|h(k)$ or $16|h^+(k)$ are not known and conjectured not to exist. Nevertheless the primes $d_1 = p$ such that $8 \mid h(k)$ (or $16 \mid h(k)$ etc.) appear to have exactly the Dirichlet density one would expect if the corresponding governing fields existed. Governing fields were introduced by Cohn and Lagarias [536, 539] (see also Cohn's book [83]) and studied by Morton [537, 538, 540, 543] and Stevenhagen [541, 542, 544]. A typical result is

Proposition 1.4.5. *Let $p \equiv 1 \bmod 4$ and $r \equiv 3 \bmod 4$ be primes and consider the quadratic number field $k = \mathbb{Q}(\sqrt{-rp}\,)$. Then $8 \mid h(k) \iff (-r/p)_4 = +1$.*

Other articles on unramified cyclic quartic extensions of quadratic number fields are Herz [24], Vaughan [86], and Williams and Liu [110].

Already Rédei [22] showed how to construct unramified cyclic 2-extensions of quadratic number fields and gave a few examples of cyclic octic class fields; his paper was apparently unknown to Barrucand and Cohn, who remarked in [38] that the explicit construction of the class field of $\mathbb{Q}(\sqrt{-41}\,)$ was probably difficult. Cooke [45] constructed this class field, and his approach was generalized in Cohn and Cooke [48]. Other papers dealing with the construction of cyclic octic class fields are Kaplan [53] and Hettkamp [69]; a few explicit examples can be found in Schoof [179], Lbekouri [93] and Cougnard [106]. The corresponding problem for cyclic extensions of relative degree 16 was dealt with in Cohn [60, 66, 83] and Yamamoto [82]; see also Cougnard [107]. Another discussion of Rédei's construction was given in Zink's dissertation [162].

Quaternion extensions (these are normal extensions with Galois group H_8, the quaternion group of order 8, simply called H_8-extensions in the sequel) have been studied ever since Dedekind [479] gave the first example; embedding problems and construction of H_8-extensions over $\mathbb{Q}$ and number fields of small degree were studied in [481], [486], [487], [502], [516], [522], [524], [527], [530] [640], [642], [644].

Unramified extensions of quadratic number fields were studied by Furtwängler [378] and Hettkamp [69]; Horie [96] has given the first examples of unramified H_8-extensions, but only considered fields whose 2-class groups were of type $(2,2)$ or $(2,2,2)$. The general problem of their existence and construction was solved by Lemmermeyer [122] by proving the following result which is completely analogous to Thm. 1.4.1:

Theorem 1.4.6. *Let k be a quadratic number field with discriminant d. Then the following assertions are equivalent:*

1. *There exists an unramified H_8-extension M/k such that $M/\mathbb{Q}$ is normal;*
2. *There is a factorization $d = d_1d_2d_3$ of d into three discriminants which are relatively prime and which satisfy the conditions $(d_1d_2/p_3) = (d_2d_3/p_1) = (d_3d_1/p_2) = +1$ for all $p_i \mid d_i$.*

Moreover, if these conditions are satisfied, then there exists an odd squarefree $a \in \mathbb{Z}$ such that the system

$$\begin{aligned} d_1X_1^2 - d_2X_2^2 &= -ad_3X_3^2 \quad (I)\\ Y_1^2 - d_1Y_2^2 &= aY_3^2 \quad (II)\\ Z_1^2 - d_2Z_2^2 &= -aZ_3^2 \quad (III) \end{aligned}$$

of diophantine equations has nontrivial solutions in $\mathbb{Z}$. If $x_i, y_i, z_i \in \mathbb{Z}$ form a solution, put

$$\mu \;=\; (x_1\sqrt{d_1} + x_2\sqrt{d_2}\,)(y_1 + y_2\sqrt{d_1}\,)(z_1 + z_2\sqrt{d_2}\,)/r,$$

where $r \in \mathbb{Z}$ is an arbitrary nonzero integer. Then $M = \mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\sqrt{d_3},\sqrt{\mu}\,)$ is an H_8-extension of k which is normal over $\mathbb{Q}$ with $\mathrm{Gal}\,(M/\mathbb{Q}) \simeq D_4 \curlyvee C_4$. If we choose $r \in \mathbb{Z}$ in such a way that μ is integral and not divisible by any rational prime p, then there is a 2-primary element in $\{\pm\mu\}$ if $d_1d_2 \equiv 0, 1 \bmod 8$, and in $\{\mu, 2\mu\}$ if $d_1d_2 \equiv 4 \bmod 8$.

The question whether the quaternion extension constructed above is unramified at ∞ is answered by the next proposition; if some prime $q \equiv 3 \bmod 4$ divides d, the same remarks as in the cyclic quartic case apply.

Proposition 1.4.7. *Let d_1, d_2, d_3 be positive discriminants not divisible by a prime $q \equiv 3 \bmod 4$, and assume that $d = d_1 d_2 d_3$ is an H_8-factorization. If M/k is a quaternion extension of $k = \mathbb{Q}(\sqrt{d}\,)$ containing $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}\,)$ which is unramified outside ∞, then M is totally real if and only if*

$$\Big(\frac{d_1 d_2}{d_3}\Big)_4 \Big(\frac{d_2 d_3}{d_1}\Big)_4 \Big(\frac{d_3 d_1}{d_2}\Big)_4 \;=\; \Big(\frac{d_1}{d_2}\Big)\Big(\frac{d_2}{d_3}\Big)\Big(\frac{d_3}{d_1}\Big).$$

In special cases, this goes back to Hettkamp [69]. See Table 1.1 for some examples.

Table 1.1:

d	d_1	d_2	d_3	μ	$\mathrm{Cl}(k)$
3848	8	13	37	$(12\sqrt{2}+5\sqrt{13}\,)(18-5\sqrt{13}\,)$	$(2,2)$
2120	5	8	53	$(3\sqrt{5}+7\sqrt{2}\,)(1+\sqrt{2}\,)$	$(2,2)$
1480	5	8	37	$(3\sqrt{5}+2\sqrt{2}\,)(2-\sqrt{5}\,)$	$(2,2)$
520	5	8	13	$(3\sqrt{2}+\sqrt{5}\,)(1+\sqrt{2}\,)$	$(2,2)$
-120	-3	5	8	$(2\sqrt{2}+\sqrt{5}\,)(2+\sqrt{5}\,)$	$(2,2)$
-255	-3	5	17	$(\sqrt{5}+2\sqrt{-3}\,)(2+\sqrt{5}\,)$	$(2,2,3)$
-420	-4	5	21	$(4i-\sqrt{5}\,)(2+\sqrt{5}\,)$	$(2,2,2)$
-455	-7	5	13	$(2\sqrt{13}-3\sqrt{5}\,)(2+\sqrt{5}\,)$	$(2,2,5)$
-520	-8	5	13	$(2\sqrt{-2}+\sqrt{5}\,)(2+\sqrt{5}\,)$	$(2,2)$

1.4.2 Cubic Number Fields

In his lectures on algebraic number theory [2], Hilbert also presented an unramified quadratic extension of a cubic number field: Let α be the real root of the equation $x^3 + 4x - 1 = 0$; then $K = \mathbb{Q}(\alpha)$ is a cubic extension with discriminant $d = -283$ and class number 2. Its Hilbert class field is $K^1 = K(\sqrt{\alpha}\,)$: in fact, since $\alpha > 0$ and K has only one real embedding, no infinite prime can ramify. Moreover, α is a unit, hence the only primes possibly ramifying are those dividing 2: but the congruence $\alpha^3 = 1 - 4\alpha \equiv 1 \bmod 4$ shows that $K(\sqrt{\alpha^3}\,) = K(\sqrt{\alpha}\,)$ is unramified at these primes, too.

This example was generalized in Rückle's dissertation [3], where he studied cubic extensions generated by roots of $x^3 - 4^a x - 1 = 0$. His methods also work for polynomials $f(x) = x^3 + 4ax - 1$: for $a \geq 1$, f has discriminant $-27 - 256a^3 < 0$; the real root α of f is positive ($0 < \alpha < 1$), and if d is squarefree then $K = \mathbb{Q}(\alpha)$ is a cubic extension with discriminant d, and $L = K(\sqrt{\alpha}\,)$ is an unramified quadratic extension of K. It should be remarked, however, that neither Hilbert nor Rückle excluded the possibility that α might be a square.

After Rückle there was a long silence, and it was Cohn's introduction of the family of simplest cubic fields which sparked the interest in unramified quadratic extensions of cyclic cubic fields. Cohn's family of cubic fields with even class numbers was explained by Shanks through the construction of the corresponding 2-class fields. The papers of Uchida [42, 43], Watabe [76], Washington [90], Lan [92] and Lemmermeyer and Pethö [116] all deal with 2-class fields of the same family. Washington's article presents connections of the 2-class fields with certain elliptic curves; see also Eisenbeis, Frey and Ommerborn [346], Nakano [78], Kawachi and Nakano [363], U. Schneiders [368, 369, 374] and Schaefer's paper [371], where he constructs a noncyclic cubic field whose 2-class group has rank ≥ 13. General questions about connections between elliptic curves and class groups are discussed in Billing [311], Brumer & Kramer [339], Buell [340], Bölling [351], Satgé [354], Quer [355], Frey [358], Aoki [364], Soleng [366] abd Sato [373].

Ennola [98] constructed 2-class fields for a family of non-normal cubic fields, and Hwang [61] studied 2-class fields of pure cubic number fields. Similar problems were discussed by Bachoc and Kwon [527], Jehanne [531], and Cassou-Nogues and Jehanne [534].

1.4.3 General Number Fields

2-class fields of general number fields have been constructed in order to show that there are infinitely many number fields of a given degree whose 2-class groups have 'large' rank. We simply note the following references: Ishida [35, 46], and Ichimura [70].

Another motivation for the construction of 2-class fields and genus class fields was the desire to prove reciprocity laws, as for example in Skolem [229], Brandt [234, 235], Halter-Koch [87], and Louboutin [299].

1.5 3-Class Fields

1.5.1 Quadratic Number Fields

Of course it was Kronecker and Weber who first constructed unramified cubic extensions of quadratic number fields (using analytic techniques from complex multiplication); the arithmetic construction of such extensions however was studied in the dissertations of Sapolsky [4] and Fueter [5], both supervised by Hilbert. Essentially the same approach was taken in the papers of Herz [24], G. Gras [31, 37], Barrucand [44], Vaughan [81], and Nakahara [97]; see also Gut [20], Honda [27], Uchida [32], Neumann [41], and Williams and Hudson [103]. The following explicit theorem can be found in Herz [24]:

Theorem 1.5.1. *Let $k = \mathbb{Q}(\sqrt{-3d}\,)$ be an imaginary quadratic number field and put $\widetilde{k} = \mathbb{Q}(\sqrt{d}\,)$, where $d = \operatorname{disc}\widetilde{k}$. Let $\varepsilon = \frac{1}{2}(e + f\sqrt{d}\,)$ be the fundamental unit of $\widetilde{k}$, and let $a = N\varepsilon$ and $e = \operatorname{Tr}\varepsilon$ denote its norm and trace, respectively. Then $3 \mid h(k)$ if and only if one of the following assertions holds:*

i) $a = +1, e \equiv \pm 2 \bmod 27$;

ii) $a = -1, e \equiv \pm 4 \bmod 9$;

iii) $e \equiv 0 \bmod 9$;

iv) $3 \mid h(\widetilde{k})$.

In cases i) – iii), the corresponding 3-class field is given by $k(\theta)$, where $\theta = \sqrt[3]{\varepsilon} + \sqrt[3]{\varepsilon'}$ is a root of the polynomial $x^3 - 3ax - e$.

Proof. We will show that

1. if a unit satisfying i), ii) or iii) exists, then $k(\theta)/k$ is an unramified cyclic cubic extension;
2. if $3 \mid h(k)$ and $3 \nmid h(\widetilde{k})$ then there exists a unit satisfying i), ii) or iii);

the implication $3 \mid h(\widetilde{k}) \Longrightarrow 3 \mid h(k)$ is part of Scholz's reflection theorem (Prop. 1.9.34).

From our construction of the Hilbert class field in Section 1.2.3 we deduce the following fact: if $3 \mid h(k)$ and $3 \nmid h(\widetilde{k})$, then the 3-class field of k is a cubic subextension of $K = k'(\sqrt[3]{\eta})$, where η is a unit in $\mathcal{O}_K$. Since $\langle\varepsilon\rangle$ is an ℓ-maximal unit group of $\mathcal{O}_K$ for every $\ell > 2$, we can take $\eta = \varepsilon$. Our claim will follow if we can prove that such a unit ε is primary if and only if one of the conditions i), ii) or iii) is satisfied.

The condition $\varepsilon \equiv \xi^3 \bmod (3\sqrt{-3}\,)$ in $\mathcal{O}_K$ is equivalent to (put $\mathcal{O} = \mathcal{O}_{\widetilde{k}}$)

a) $\varepsilon \equiv \xi^3 \bmod \mathfrak{p}^3$ if $d \equiv 0 \bmod 3$, where $3\mathcal{O} = \mathfrak{p}^2$;

b) $\varepsilon \equiv \xi^3 \bmod \mathfrak{p}_j^2$ $(j = 1, 2)$ if $d \equiv 1 \bmod 3$, where $3\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$;

c) $\varepsilon \equiv \xi^3 \bmod 9$ if $d \equiv 2 \bmod 3$.

Now we look at each case separately:

a) Consider the homomorphism $\Phi : (\mathcal{O}/\mathfrak{p}^3)^\times \longrightarrow (\mathcal{O}/\mathfrak{p}^3)^\times : \xi \longmapsto \xi^3$; since $\#(\mathcal{O}/\mathfrak{p}^3)^\times = 18$ and $\#\ker\Phi = 9$ (note that $\ker\Phi = \langle 4, 1 + \sqrt{d} \bmod \mathfrak{p}^3\rangle$), we conclude that $\varepsilon \equiv \xi^3 \bmod \mathfrak{p}^3$ if and only if $\varepsilon \equiv \pm 1 \bmod \mathfrak{p}^3$. This implies at once that $3 \mid f$, and now $e^2 \equiv 4a \bmod 27$ shows $a = +1$ and $e \equiv \pm 2 \bmod 27$. On the other hand, $a = 1$ and $e \equiv \pm 2 \bmod 27$ imply $3 \mid f$ and $\varepsilon \equiv \pm 1 \bmod \mathfrak{p}^3$.

b) Since $\#(\mathcal{O}/\mathfrak{p}^2)^\times = 6$ and $\#\ker\Phi = 3$ we know that $\varepsilon \equiv \xi^3 \bmod \mathfrak{p}_j^2$ if and only if $\varepsilon \equiv \pm 1 \bmod \mathfrak{p}_j^2$. Now $\varepsilon \equiv \pm 1 \bmod \mathfrak{p}_1^2$ and $\varepsilon \equiv \pm 1 \bmod \mathfrak{p}_2^2$ imply $\varepsilon \equiv \pm 1 \bmod 9$ (i.e. $f \equiv 0 \bmod 9$), and then $e^2 - 4a = df^2 \equiv 0 \bmod 27$ give $a = 1$ and $e \equiv \pm 2 \bmod 27$, whereas $\varepsilon \equiv \pm 1 \bmod \mathfrak{p}_1^2$ and $\varepsilon \equiv \mp 1 \bmod \mathfrak{p}_2^2$ yield $e \equiv 0 \bmod 9$ (and $a = -1$). The other direction is easy to verify.

c) Here $\#(\mathcal{O}/9)^\times = 8 \cdot 9$ and $\#\ker\Phi = 9$ show that $\varepsilon \equiv \xi^3 \bmod 9$ if and only if $\varepsilon \equiv \pm 1,\ \pm d\sqrt{d},\ \pm(1+3d) \pm (d+3)\sqrt{d} \bmod 9$. A few simple computations reveal that $\varepsilon \equiv \pm 1 \bmod 9 \iff 9 \mid f \iff a = 1$ and $e \equiv \pm 2 \bmod 27$; similarly $\varepsilon \equiv \pm d\sqrt{d} \bmod 9$ leads to $e \equiv 0 \bmod 9$, and finally $\varepsilon \equiv \pm(1+3d) \pm (d+3)\sqrt{d} \bmod 9$ implies $\pm e = 2(1+3d) \equiv -4 \bmod 9$ and $a = \frac{1}{4}(e^2 - df^2) \equiv -1 \bmod 9$. Again, the other direction is easily verified.

□

Example 1.5.1. *All the cases in Theorem 1.5.1 do actually occur, as the following examples show:*

a	$d \bmod 3$	d	ε
$+1$	0	69	$\frac{1}{2}(25 + 3\sqrt{69})$
$+1$	1	253	$\frac{1}{2}(1861 + 117\sqrt{253})$
$+1$	2	83	$82 + 9\sqrt{83}$
$+1$	2	77	$\frac{1}{2}(9 + \sqrt{77})$
-1	1	85	$\frac{1}{2}(9 + \sqrt{85})$
-1	2	29	$\frac{1}{2}(5 + \sqrt{29})$

As another illustration, we construct a family of unramified cyclic cubic extensions of quadratic number fields. We start with the following proposition, which can be proved by the method discussed by Lemmermeyer and Pethö [116]:

Proposition 1.5.2. *Let m, n, t be natural numbers such that $m = t^2 - 2$ and $t \geq 12$; if the diophantine equation $N(\xi) = |x^2 - my^2| = n$ has solutions $\xi = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}\,]$, then one of the following assertions holds:*

a) $\xi = r\eta$ for some $r \in \mathbb{Z}$ and a unit $\varepsilon \in \mathbb{Z}[\sqrt{m}\,]$, and $r^2 = n$;

b) $\xi = r\eta\varepsilon$ for some $r \in \mathbb{Z}$, $\eta = t + \sqrt{m}$, and some unit $\varepsilon \in \mathbb{Z}[\sqrt{m}\,]$, and $2r^2 = n$;

c) $n = 2t \pm 3, 4t - 9, 4t - 6$, and ξ is associated to one of the following elements:

$$\{t \pm 1 \pm \sqrt{m},\ t \pm 2 \pm \sqrt{m},\ 2t - 1 \pm 2\sqrt{m},\ 2t \pm 2 \pm 2\sqrt{m}\};$$

d) $n \geq 4t + 6$.

This result allows us to construct quadratic number fields $K = \mathbb{Q}(\sqrt{m}\,)$ with class number divisible by 3; for suppose that $m = t^2 - 2$ is squarefree, and that $4t - 9 = b^3$ for some $b \geq 3$. Then $\alpha = 2t - 1 + 2\sqrt{m}$ has norm b^3, hence $\alpha\mathcal{O}_K = \mathfrak{a}^3$ for some ideal $\mathfrak{a}$ in $\mathbb{Z}[\sqrt{m}\,]$. If $\mathfrak{a}$ were principal, it would have norm b; but $b < 2t - 1$, hence Prop. 1.5.2 implies that b is a square and that $\mathfrak{a}$ is generated by an integer. This contradiction shows that $\mathfrak{a}$ is not principal, hence $h(K) \equiv 0 \bmod 3$. We cannot expect to be able to construct the corresponding unramified cyclic cubic extension of K from these data (this is Leopoldt's Spiegelungssatz at work – see Chapter 2); in fact we will construct such extensions over $L = \mathbb{Q}(\sqrt{-3m}\,)$.

Suppose first that $b \equiv 0 \bmod 3$; then $t \equiv 0 \bmod 9$ and $m \equiv 2 \bmod 3$, hence $\varepsilon = t^2 - 1 + t\sqrt{m} \equiv -1 \equiv (-1)^3 \bmod 27$. From the proof of part a) of Theorem 1.5.1 we deduce that $M(\sqrt[3]{\varepsilon}\,)$ is an unramified cyclic cubic extension of $M = K(\sqrt{-3}\,)$.

Next consider the case $b \equiv \pm 1 \bmod 3$; then $t \equiv \pm 2 \bmod 9$ and $m \equiv 2 \bmod 9$, and we find

$$\begin{aligned} \alpha &= 2t - 1 + 2\sqrt{m} \equiv \begin{cases} 4 + 2\sqrt{m} \bmod 9, & \text{if } b \equiv 1 \bmod 3 \\ 3 + 2\sqrt{m} \bmod 9, & \text{if } b \equiv 2 \bmod 3 \end{cases} \\ \varepsilon &= t^2 - 1 + t\sqrt{m} \equiv \begin{cases} 3 - 2\sqrt{m} \bmod 9, & \text{if } b \equiv 1 \bmod 3 \\ 3 + 2\sqrt{m} \bmod 9, & \text{if } b \equiv 2 \bmod 3 \end{cases} \end{aligned}$$

Let $\varepsilon' = t^2 - 1 - t\sqrt{m}$ denote the conjugate of ε; then we find that $\alpha\varepsilon' \equiv (-1+\sqrt{m})^3 \bmod 9$ if $b \equiv 1 \bmod 3$, and $\alpha\varepsilon' \equiv 1 \bmod 9$ if $b \equiv 2 \bmod 3$. Therefore the polynomials P_t below generate unramified cubic extensions of $\mathbb{Q}(\sqrt{-3m}\,)$, $m = t^2 - 2$, whenever m is squarefree:

$$\begin{aligned} P_t(x) &= x^3 - 3x + 2(1-t^2), && \text{where } t = (b^3+9)/4 \text{ and } b \equiv 3 \bmod 6, \\ P_t(x) &= x^3 + 3bx - 2(1+2t-t^2), && \text{where } t = (b^3+9)/4 \text{ and } b \equiv 7, 11 \bmod 12. \end{aligned}$$

An interesting example is provided by $b = 55$, $t = 41596$, where the cubic extension has class group $(3,3)$; by a result of Callahan (Prop. 1.9.36) this implies that the imaginary quadratic field has a 3-class group of rank 3. Similar families can of course be constructed by replacing $4t-9$ by other norms such as $2t \pm 3$, etc.

Let k be a quadratic number field with discriminant d and 3-rank r; Hasse [10] has shown that there exist $\frac{1}{2}(3^r - 1)$ non-conjugate cubic number fields K with discriminant d such that Kk/k is an unramified cyclic cubic extension. Shanks [51] computed generating polynomials of these cubic fields for $\operatorname{disc} k = -4027$ ($r = 2$) and $\operatorname{disc} k = 44\,806\,173$ ($r = 3$). Diaz y Diaz, Llorente and Quer [91] did the same for $k = \mathbb{Q}(\sqrt{314\,582\,172\,161}\,)$, where $\mathrm{Cl}(k) \simeq (2,3,3,3,3)$.

As already Kummer had shown, the diophantine equation $X^p + Y^p = Z^p$ has no solution in integers $\neq 0$ if the class number of $\mathbb{Q}(\zeta_p)$ is not divisible by p. Fueter looked at such problems from a different angle: he showed [7] that if $X^3 + Y^3 = Z^3$ has nontrivial solutions in certain quadratic number fields k, then these solutions can be used to construct unramified cyclic cubic extensions of k. This subject was also dealt with in papers of Aigner [21], Mirimanoff [17], and Therond [75]. In [9], Fueter studied solutions of the Bachet-Mordell equation $y^2 = x^3 - m$ and showed that the class number of $\mathbb{Q}(\sqrt{m}\,)$, where $m = x^3 - y^2$, $m \equiv 7 \bmod 9$, $m \neq 3 \bmod 4$, and $m \neq -4 \bmod 16$ is $\equiv 0 \bmod 3$ by constructing the corresponding unramified cyclic cubic extension of k. This connection between 3-ranks of quadratic number fields and points on certain elliptic curves was also discussed in Bölling [333]. For the construction of the cyclic unramified extension of degree 9 over $\mathbb{Q}(\sqrt{1129}\,)$ see Kerkour [58].

1.5.2 Cubic Fields

The 3-class fields of cyclic cubic extensions of $\mathbb{Q}$ have been studied by A. Scholz in several papers. In particular, he studied the following case: let $p \equiv 1 \bmod 3$ be prime, and let k_p denote the cubic subfield of $\mathbb{Q}(\zeta_p)$. If q is another prime $\equiv 1 \bmod 3$ (or $q = 9$, k_9 being the cyclic cubic field with discriminant 81), then $K = k_p k_q$ contains four subfields, namely k_p, k_q, and two fields k_{pq} and k'_{pq} of conductor pq. It is easy to see that K/k_{pq} is an unramified cyclic cubic extension, hence K is the 3-class field of k_{pq} if $\mathrm{Cl}_3(k_{pq}) \simeq \mathbb{Z}/3\mathbb{Z}$. Now Scholz (see also Inaba [312], Martinet [250], and Gras [323]) proved

Proposition 1.5.3. *$h_3(k_{pq}) \equiv 0 \bmod 9 \iff (p/q)_3 = (q/p)_3 = 1$, i.e. if p and q are cubic residues of each other.*

Actually, Scholz proved much more, but his paper is hard to understand. His results are related to those of Gillard [322] and Naito [88, 183].

In his dissertation [28], Bauer studied the explicit construction of 3-class fields of cyclic cubic number fields, but could not give an example going beyond the genus class field. He improved Leopoldt's bound $t - 1 \leq \operatorname{rank} \mathrm{Cl}_3(k) \leq 2(t-1)$ by showing that in fact $\operatorname{rank} \mathrm{Cl}_3(k) = 2(t-1) - r$ (he also gave a similar expression for the 3-rank of $\mathrm{Cl}(L)$, $L = k(\sqrt{-3}\,)$) where $r \leq t-1$ is the rank of a certain matrix whose entries are cubic Hilbert symbols. He also showed that an unramified cyclic cubic extension K/k is normal over $\mathbb{Q}$ if and only if K is contained in the genus class field k_{gen} of $k/\mathbb{Q}$.

Quite recently the Stark Conjectures (see e.g. the papers of Stark [595, 596, 597, 598, 599, 600] for the development of these conjectures, or Tate's book [605]; other references are Chinburg [602], Sands [603, 604, 606], Hayes [607], Wiles [608], Wang [609], Rubin [610, 612], or Hayes [614]) have been used for computing the 3-class fields of certain cubic number fields; see e.g. the articles of Dummit and Hayes [121], Dummit, Sands, and Tangedal [613], or [611].

Consider the family of cubic fields K_u generated by a root α of the polynomial $f_u(x) = x^3 + (u+1)x^2 - (u+2)x - 1$ (cf. Buell and Ennola [111]). If $d = \operatorname{disc} f = u^4 + 14u^3 + 67u^2 + 126u + 49 = (u^2 + 7u + 9)^2 - 32$ is squarefree, then K_u is an unramified cyclic cubic extension of $k_u = \mathbb{Q}(\sqrt{d}\,)$. Using the method described in [116] it is easy to show that the minimal nontrivial norm in the order $\mathbb{Z}[\alpha]$ is $2u + 1$.

Assume therefore that d is squarefree and $2u+1=b^3$; then K_u has class number divisible by 3, and Callahan's result (Prop. 1.9.36) shows that $\mathrm{Cl}_3(k_u)$ has rank ≥ 2. The same thing works of course if $2u+7=b^3$; in this case, the value $b=193$ provides us with a real quadratic number field of discriminant $d=166\ 943\ 369\ 675\ 256\ 545\ 872\ 751\ 089$ and a 3-class group of rank 5.

1.6 ℓ-Class Fields

1.6.1 Quadratic Number Fields

For primes $\ell > 3$, the arithmetic construction of ℓ-class fields of quadratic number fields started with the papers of Hasse [26] and of Hasse and Liang [29], who constructed the Hilbert class field of $K=\mathbb{Q}(\sqrt{-47}\,)$ (K has class number 5) and compared its generating polynomial to the one given by Weber using the theory of complex multiplication. Later G. Gras [31, 37] developed the general theory of such constructions, building on the work of Kummer, Hasse, Payan and Martinet. Just as in the Rédei-Reichardt theory, the construction of the ℓ-class field of a number field k can be simplified if k is assumed to be a normal extension of another number field F (in the simplest cases, $k/\mathbb{Q}$ is a quadratic number field). Parry [54] found the following result corresponding to Theorem 1.5.1:

Theorem 1.6.1. *Let $m>0$ be a squarefree integer, and put $\alpha=-\frac{1}{2}(5+\sqrt{5}\,)$. Then $K=\mathbb{Q}(\sqrt{5},\sqrt{m}\,)$, $\widetilde{k}=\mathbb{Q}(\sqrt{5},\sqrt{\alpha m}\,)$ and $\mathbb{Q}'=\mathbb{Q}(\alpha)=\mathbb{Q}(\zeta_5)$ are the three quartic subfields of $\mathbb{Q}(\sqrt{m},\zeta_5)$. Let H and $\widetilde{h}$ denote the class number of K and $\widetilde{k}$, and let $\varepsilon_m=\frac{1}{2}(a+b\sqrt{m}\,)$ and $\varepsilon_{5m}=\frac{1}{2}(c+d\sqrt{5m}\,)$ denote the fundamental units of $\mathbb{Q}(\sqrt{m}\,)$ and $\mathbb{Q}(\sqrt{5m}\,)$, respectively. Then $5\mid\widetilde{h}$ if and only if one of the following conditions holds:*

i) $ab\equiv 0 \bmod 25$;

ii) $m\equiv\pm 2 \bmod 5$ *and* $\mathrm{Tr}\varepsilon_{5m}\equiv\pm 1,\ \pm 7 \bmod 25$;

iii) $d\equiv 0 \bmod 5$;

iv) $5\mid H$.

Gut [23, 40] developed an interesting idea for constructing unramified cyclic ℓ-extensions of certain number fields k, which was taken up again in articles of Satgé and Barrucand [50] and Satgé [55, 64, 65]. In the special case $\ell=5$, these constructions explain numerical results discovered by Parry [54, 59].

Families of unramified cyclic extensions of degree 5 and 7 over quadratic number fields have been constructed by Mestre [63, 71] using the theory of elliptic curves. A very beautiful family of dihedral quintic extensions whose normal closure is unramified over its quadratic subfield is discussed in Kondo's paper [125]; see also Sasajima's dissertation [124].

1.6.2 Cyclic Number Fields

The results of the previous section can be generalized to cyclic fields, and, in particular, to cyclotomic number fields. Much work on the construction of ℓ-class fields of $\mathbb{Q}(\zeta_\ell)$ has been carried out by Pollaczek [8], Herbrand [11], Ribet [47, 49] and Wiles [68]; details will be presented in Chap. ??, after we will have refined Furtwängler's construction of class fields. See also Hasse [13], Morishima [14], Nakagoshi [79, 95, 99, 100], Odai [89], and Gurak [105]

1.7 Separants

Separants were introduced by Lemmermeyer [115] in order to generalize the results of Goldstein, Sunley and Davis (see Thm. 1.3.4) to totally real fields of odd class number in the strict sense.

In fact, assume that F is a number field with odd class number h, and let $k=F(\sqrt{\mu}\,)$ be a quadratic extension. The relative discriminant $\mathfrak{d}=\mathrm{disc}\,(k/F)$ is an integral ideal in $\mathcal{O}_F$, and it is easy to see that $(4\mu)=(\mathrm{disc}\,(\sqrt{\mu}\,))=\mathfrak{a}^2\mathfrak{d}$, for an integral ideal $\mathfrak{a}$ in $\mathcal{O}_F$. Since $\mathfrak{d}^h=(\delta)$ and $\mathfrak{a}^h=(\alpha)$ are principal in

F, we have $(4\mu)^h = (\alpha^2\delta)$, and we can choose $\delta \in \mathcal{O}_F$ in such a way that we have $\mu = \xi^2\delta$ for some $\xi \in F$. Obviously, δ is unique up to squares of units in $\mathcal{O}_F$, i.e. another choice of μ leads to a $\delta_1 \in F$ such that $\delta = \delta_1\varepsilon^2$. The residue class $d = \delta \bmod E_F^2$ is called the *separant* of the quadratic extension, and we will write $d = \mathrm{sep}(k/F)$. Note that expressions like $F(\sqrt{d})$ or $(d/\mathfrak{p})$ (Legendre-symbol) etc. make perfect sense, because they do not depend on the choice of a representative. Moreover, we always have $k = F(\sqrt{d})$, hence the separant does indeed characterize quadratic extensions.

Let $\mathfrak{u}$ be an infinite prime in F; $\mathfrak{u}$ is called *ramified* in F/k if $\mathfrak{u}$ is real and its extension in F is complex. We will write $\mathfrak{u} \nmid d$ if $d \equiv 1 \bmod \mathfrak{u}$, or more exactly, if a representative δ of d is positive at $\mathfrak{u}$ (since representatives differ at most by squares, this is well defined). We will call two separants d_1, d_2 *relatively prime* (and write $(d_1, d_2)|\infty$) if there is no finite prime $\mathfrak{p}$ dividing both d_1 and d_2; we will call them *relatively prime* at ∞ if there is no infinite prime dividing both d_1 and d_2. If two separants are relatively prime both at the finite and infinite primes, we will write $(d_1, d_2) = 1$.

For fields with class number 1, separants and Goldstein's generalized discriminants are essentially the same. The introduction of separants is justified by the fact that Thm. 1.3.4 as well as the whole Rédei-Reichardt theory (Thm. 1.4.1 in particular, but also the whole discussion on the construction of cyclic unramified 2-extensions and governing fields) generalizes if only F has odd class number in the strict sense:

Theorem 1.7.1. *Let F be a number field with odd class number, k/F a quadratic extension, and L/k an unramified C_4-extension. Then*

i) L/F is normal with Galois group $\mathrm{Gal}\,(L/F) \simeq D_4$, and L/k is the cyclic quartic extension in L/F;

ii) there exists a "C_4-factorization" $d = \mathrm{sep}(k/F) = d_1 \cdot d_2$ of d into separants d_1, d_2 such that

a) $(d_1, d_2) = 1$;

b) $(d_1/\mathfrak{p}_2) = (d_2/\mathfrak{p}_1) = +1$ for all prime ideals $\mathfrak{p}_1 \mid d_1$ and $\mathfrak{p}_2 \mid d_2$.

On the other hand, if $d = d_1 \cdot d_2$ is a C_4-factorization, let δ_j be a representative of d_j, $j = 1, 2$; then the diophantine equation

$$X^2 - \delta_1 Y^2 - \delta_2 Z^2 = 0 \tag{1.5}$$

is solvable in $\mathcal{O}_F$. For any solution $(x, y, z) \in \mathcal{O}_F^3$ of (1.5), put $\mu = x + y\sqrt{\delta_1}$ and $\nu = 2(x - z\sqrt{\delta_2})$; then $L = k(\sqrt{d_1}, \sqrt{\mu}) = k(\sqrt{d_2}, \sqrt{\nu})$ is a cyclic quartic extension of k, which is unramified outside 2∞; moreover, L/F is normal and $\mathrm{Gal}\,(L/F) \simeq D_4$.

If F is totally real and has odd class number in the strict sense, we can choose the solutions to (1.5) in such a way that L/k becomes unramified at all finite primes.

An explanation of why this works exactly for totally real fields with odd class number in the strict sense was provided by the introduction of the separant class group $\mathrm{SCl}(F)$ in [300]; we will give a new approach to $\mathrm{SCl}(F)$ in Chapter 3.

1.8 Capitulation of Ideal Classes

There are three excellent surveys on the capitulation of ideal classes: Adachi [426], Jaulent [450], and Miyake [452].

1.8.1 Hilbert's Theorem 94

Let k be a number field and let $\mathfrak{a}$ be an ideal in $\mathcal{O}_k$; then $\mathfrak{a}$ is said to *capitulate* in an extension K/k if $\mathfrak{a}\mathcal{O}_K = \alpha\mathcal{O}_K$ for some $\alpha \in \mathcal{O}_K$, i.e. if $\mathfrak{a}$ becomes principal. It is easy to see that the capitulation of $\mathfrak{a}$ only depends on its ideal class. Already Kronecker noticed connections between unramified abelian extensions of number fields and the capitulation of ideal classes, and in his Zahlbericht, Hilbert proved

Theorem 1.8.1. *Let K/k be a cyclic unramified extension of prime degree ℓ. Then there is a non-principal ideal $\mathfrak{a}$ in k which capitulates in K. In particular, the class number of k is divisible by ℓ.*

The last remark stems from the rather obvious observation that ideal classes capitulating in K/k must have order dividing $(K:k)$. The generalization of Hilbert's Theorem 94 to cyclic extensions of prime power degree presented no problem. In contrast to other theorems in class field theory, however, no one saw how to reduce the (conjectured) principal ideal theorem to cyclic extensions. It is not hard to show (see Furtwängler [378]) that Theorem 94 also holds for unramified extensions with Galois group $\simeq (\ell^a, \ell)$, but this seems to be all that can be achieved by using the (essentially cohomological) direct approach used by Hilbert.

In the following, let $\kappa_{K/k}$ denote the kernel of the conorm of K/k, i.e. the subgroup of $\mathrm{Cl}(k)$ capitulating in K. A standard cohomological argument ([420]) shows readily that, for cyclic unramified extensions K/k of prime power degree, we have $\#\,\kappa_{K/k} = (K:k)(E_k : N_{K/k}E_K)$, where E_k denotes the unit group of $\mathcal{O}_k$.

In the first attack on the capitulation problem after Hilbert, Furtwängler [378] used "Hilbert's Theorem 90 for ideal classes", which he had proved earlier in his work on Hilbert class fields:

Theorem 1.8.2. *Let K/k be a cyclic unramified extension such that $\mathrm{Gal}\,(K/k) = \langle\sigma\rangle$, and let $c \in \mathrm{Cl}(K)$. Then $N_{K/k}c = 1$ if and only if there is a $C \in \mathrm{Cl}(K)$ such that $c = C^{1-\sigma}$.*

This theorem fails to hold if one replaces the norm $N_{K/k}$ by the 'algebraic norm' $\nu = 1 + \sigma + \ldots + \sigma^{(K:k)-1}$; in fact, let ${}_\nu C = \{c \in \mathrm{Cl}(K) : c^\nu = 1\}$ be the subgroup of $\mathrm{Cl}(K)$ annihilated by ν (this means that taking the norm to k of $c \in {}_\nu C$ and lifting it back to K yields the trivial ideal class). Hilbert's Theorem 90 in the strong sense would assert that ${}_\nu C = C^{1-\sigma}$, but this is not true in general (cf. Kisilevsky [423]):

Corollary 1.8.3. *If K/k is a cyclic unramified extension, then $({}_\nu C : C^{1-\sigma}) = \#\,\kappa_{K/k} \cap N_{K/k}\mathrm{Cl}(K)$.*

Proof. This follows at once from Theorem 1.8.2 and the exactness of the sequence

$$1 \longrightarrow {}_N C \longrightarrow {}_\nu C \xrightarrow{N_{K/k}} \kappa_{K/k} \cap N_{K/k}\mathrm{Cl}(K) \longrightarrow 1$$

which is an immediate consequence of the definitions of the groups involved. □

O. Taussky [424] called unramified cyclic ℓ-extensions K/k 'of type B' if $\kappa_{K/k} \cap N_{K/k}\mathrm{Cl}(K) = 1$, and of type A otherwise.

1.8.2 Artin's Reduction

Let K/k be an unramified abelian extension; let k^1 and K^1 denote the Hilbert class field of k and K, respectively (the following results continue to hold if one replaces Hilbert class fields by p-class fields). Put $L = k^2$ (the Hilbert class field of k^1), $G = \mathrm{Gal}\,(k^2/k)$, and let $H \leq G$ be the subgroup corresponding to K. Then $G/G' \simeq \mathrm{Gal}\,(k^1/k)$ and $H/H' \simeq Gal(K^2/K)$; the Artin isomorphism shows $G/G' \simeq \mathrm{Cl}(k)$ and $H/H' \simeq \mathrm{Cl}(K)$. Let $j = j_{k\to K}$ denote the conorm of K/k, i.e. the transfer of ideal classes. Artin proved

Proposition 1.8.4. *There exists a group homomorphism $\mathrm{Ver} : G/G' \longrightarrow H/H'$ such that the following diagram commutes:*

$$\begin{array}{ccc} \mathrm{Cl}(k) & \xrightarrow{\ j\ } & \mathrm{Cl}(K) \\ \Big(\frac{L/k}{\cdot}\Big)\Big\downarrow & & \Big\downarrow\Big(\frac{L/K}{\cdot}\Big) \\ G/G' & \xrightarrow{\ \mathrm{Ver}\ } & H/H' \end{array}$$

This diagram allows us to study the capitulation kernel $\kappa_{K/k} = \ker j$ by computing the kernel of the map $\mathrm{Ver} : G/G' \longrightarrow H/H'$, which is defined (for groups $H \subseteq G$ such that the index $n = (G:H)$ is finite) as follows: let $G = \bigcup_{j=1}^n g_j H$ be a decomposition of G into left cosets; for every $g \in G$ and every g_i there exists an $i' \leq n$ such that $gg_iH = g_{i'}H$. The map $V : g \longmapsto \prod_{i=1}^r g_{i'}^{-1} g g_i \cdot H'$ is easily shown to be a homomorphism $V : G \longrightarrow H/H'$ which does not depend on the choice of the g_j. Since H/H'

is abelian, the kernel of V contains G', hence V induces a homomorphism $G/G' \longrightarrow H/H'$ called the transfer (Verlagerung) which we will denote by $\mathrm{Ver}_{G,H}$.

As an illustration, let G be a 2-group, and H be a subgroup of G with index 2. Let z be any element in $G \setminus H$. Then

$$\mathrm{Ver}_{G,H}(g) = \begin{cases} g^2 H' & \text{if} \quad g \in G \setminus H, \\ z^{-1} g z g H' & \text{if} \quad g \in H. \end{cases}$$

If we put $K = k^1$, then it is clear that every ideal of k becomes principal in K if and only if $\mathrm{Ver}_{G,G'}$ is the trivial map; therefore, the Principal Ideal Theorem follows from the

Theorem 1.8.5. *(Principal Ideal Theorem of Group Theory) For finite groups G, the transfer* Ver : $G/G' \longrightarrow G'/G''$ *is the trivial map.*

It was this group theoretic theorem which Furtwängler could prove in [382] by a massive computation. Later, simpler proofs were given by Iyanaga [383, 390], Taketa [386], Magnus [391], Witt [395, 406], and Schumann and Franz [396]. An immediate corollary of Thm. 1.8.5 is the following observation of Scholz [136]:

Corollary 1.8.6. *If the class field tower of a number field k terminates at k^1, then $\kappa_{K/k} = \{c \in \mathrm{Cl}(k) : c^{(K:k)} = 1\}$ for any subfield $k \subseteq K \subseteq k^1$.*

Proof. If G is an (additively written) abelian group, then the transfer $\mathrm{Ver}_{G,H}$ is easily seen to be just multiplication by the index $(G : H)$. In particular, the kernel of the transfer $G \longrightarrow H$ is just the subgroup of G killed by $(G : H)$, which corresponds via Artin's isomorphism to the subgroup of ideal classes of $\mathrm{Cl}(k)$ of order dividing $(G : H) = (K : k)$. □

Furtwängler [385] gave a stronger principal ideal theorem for number fields with elementary abelian 2-class groups:

Proposition 1.8.7. *Let k be a number field, and assume that $\mathrm{Cl}_2(k) \simeq (\mathbb{Z}/2\mathbb{Z})^t$ for some $t \geq 1$. Then there exist generators $c_1, \ldots, c_t$ of $\mathrm{Cl}_2(k)$ such that each c_j capitulates in at least one of the quadratic unramified extensions of k.*

Taussky [380, 387] showed that the corresponding result for p-class fields, $p \geq 3$, fails to hold in general.

1.8.3 Scholz and Taussky

Before we present some of the results of Scholz and Taussky on the capitulation of 3-class groups, we will describe their counterparts for 2-class groups. To this end, let k be a number field with $C_0 = \mathrm{Cl}_2(k) \simeq (2, 2)$. Then C_0 has three subgroups C_1, C_2, C_3 of order 2, and these correspond to the three unramified quadratic extensions k_j/k via Artin's reciprocity law: $C_i = N_{k_j/k}\mathrm{Cl}_2(k_j)$. We will say that k has capitulation type $[i_1\ i_2\ i_3]$ if $\kappa_j = C_{i_j}$. We will not distinguish between capitulation types which coincide upon a suitable permutation of the fields k_i; if, for example, k has capitulation type [1 0 0] (exactly the subgroup C_1 capitulates in k_1/k, whereas in k_2/k and k_3/k the whole 2-class group $\mathrm{Cl}_2(k)$ capitulates), then changing the roles of k_1 and k_2 shows that k also has capitulation type [0 2 0]; we will indicate this by [1 0 0] $\sim$ [0 2 0]. The work of Furtwängler [378] and Kisilevsky [429] can then be subsumed into the following table, relating capitulation type and $\Gamma = \mathrm{Gal}\,(k^2_{(2)}/k)$:

Before we explain the method of Scholz and Taussky by verifying this table, we give a related theorem containing results of Furtwängler [378], Kisilevsky [429], and Couture and Derhem [460]:

Theorem 1.8.8. *Let k be a number field, and assume that $\mathrm{Cl}_2(k) \simeq (2, 2)$. Let k^1 be the 2-class field of k, k_i $(1 \leq i \leq 3)$ the three quadratic subextensions in k^1/k, and κ_i the subgroup of $\mathrm{Cl}(k)$ which capitulates in k_i/k. Then k_i is the class field of k for the class group $C_i = N_{k_i/k}\mathrm{Cl}_2(k_i)$. Let k^2 denote the 2-class field of k^1, and put $G = \mathrm{Gal}\,(k^2/k)$. Then the 2-class field tower of k has at most length 2, and G is either $\simeq (2, 2)$ or isomorphic to a dihedral, semidihedral or quaternionic 2-group. In fact:*

1. *$G \simeq (2, 2) \iff \kappa_i = \mathrm{Cl}_2(k)$ $(i = 1, 2, 3)$, i.e. in every extension k_i/k the whole 2-class group $\mathrm{Cl}_2(k)$ capitulates;*

Table 1.2:

$[0\ 0\ 0]$	$(2,2)$
$[1\ 0\ 0] \sim [0\ 2\ 0] \sim [0\ 0\ 3]$	$-$
$[2\ 0\ 0] \sim [3\ 0\ 0] \sim [0\ 1\ 0] \sim [0\ 3\ 0] \sim [0\ 0\ 1] \sim [0\ 0\ 2]$	$-$
$[0\ 2\ 3] \sim [1\ 0\ 3] \sim [1\ 2\ 0]$	$-$
$[0\ 2\ 1] \sim [0\ 1\ 3] \sim [1\ 0\ 2] \sim [2\ 0\ 3] \sim [1\ 3\ 0] \sim [3\ 2\ 0]$	$-$
$[0\ 1\ 2] \sim [0\ 3\ 1] \sim [2\ 0\ 1] \sim [3\ 0\ 2] \sim [3\ 1\ 0] \sim [2\ 3\ 0]$	$-$
$[0\ 1\ 1] \sim [2\ 0\ 2] \sim [3\ 3\ 0]$	$-$
$[0\ 2\ 2] \sim [0\ 3\ 3] \sim [1\ 0\ 1] \sim [3\ 0\ 3] \sim [1\ 1\ 0] \sim [2\ 2\ 0]$	$-$
$[0\ 3\ 2] \sim [3\ 0\ 1] \sim [2\ 1\ 0]$	D_m, $m \geq 4$
$[1\ 1\ 1] \sim [2\ 2\ 2] \sim [3\ 3\ 3]$	$-$
$[1\ 1\ 2] \sim [1\ 3\ 1] \sim [2\ 2\ 1] \sim [3\ 2\ 2] \sim [3\ 1\ 3] \sim [2\ 3\ 3]$	$-$
$[1\ 2\ 2] \sim [1\ 2\ 1] \sim [1\ 1\ 3] \sim [1\ 3\ 3] \sim [2\ 2\ 3] \sim [3\ 2\ 3]$	$-$
$[2\ 1\ 1] \sim [2\ 1\ 2] \sim [2\ 3\ 2] \sim [3\ 1\ 1] \sim [3\ 3\ 1] \sim [3\ 3\ 2]$	SD_{2m}, $m \geq 8$
$[2\ 3\ 1] \sim [3\ 1\ 2]$	$-$
$[1\ 2\ 3]$	H_8
$[1\ 3\ 2] \sim [2\ 1\ 3] \sim [3\ 2\ 1]$	H_{2m}, $m \geq 8$

2. $G \simeq H_8 \iff \kappa_i = C_i$ *for* $i = 1, 2, 3$.

In all other cases, k^2 *is cyclic over exactly one of the* k_i*, say* k_1*. Then* $\mathrm{Cl}_2(k_1) \simeq \mathbb{Z}/m\mathbb{Z}$ *for some* 2*-power* m*, and we have*

3. $G \simeq D_m \iff \kappa_1 = \mathrm{Cl}_2(k), \kappa_2 = C_3, \kappa_3 = C_2$;

4. $G \simeq SD_{2m}$, $m \geq 8 \iff \kappa_1 \cap C_1 = 1, \kappa_2 = C_3, \kappa_3 = C_2$;

5. $G \simeq H_{2m}$, $m \geq 8 \iff \kappa_1 = C_1, \kappa_2 = C_3, \kappa_3 = C_2$.

If $G \simeq SD_{2m}$ *then* $\kappa_1 = C_2$*, where* k_2 *is the unique* k_i *over which* k^2 *is dihedral; moreover, in this case there is a unit* $\varepsilon \in E_k \setminus E_k^2$ *such that* $\varepsilon \equiv \xi^2 \bmod 4$.

Let us come back to the paper of Scholz and Taussky. Let ℓ be a prime, and let k be a number field with $\mathrm{Cl}_\ell(k) \simeq (\ell, \ell)$. Let k^1 and k^2 denote the first and second Hilbert ℓ-class field of k, and put $\Gamma = \mathrm{Gal}\,(k^2/k)$. Then Γ is a metabelian ℓ-group, i.e. the derived group Γ' is abelian. For $R, S, T \in \Gamma$ define $S^T := T^{-1}ST$, $R^{S+T} = R^S R^T$ and $R^{nS} = (R^n)^S$. Then for all $A, B \in \Gamma'$ and all $R, S, T \in \Gamma$, the following relations are valid:

$$\begin{array}{llll} (1) & A^{S+T} = A^{T+S}; & (2) & A^{ST} = A^{TS}; \\ (3) & (AB)^S = A^S B^S; & (4) & A^{(R+S)T} = A^{RT+ST}. \end{array}$$

Their verification is straightforward.

Now assume in addition that $\Gamma = \langle S, T \rangle$ is an ℓ-group of rank 2; the next three propositions are formulated only for the special case $\Gamma/\Gamma' \simeq (\ell, \ell)$ but can actually be generalized to all ℓ-groups of rank 2 (cf. Furtwängler [382]):

Proposition 1.8.9. Γ' *is generated as a* G*-module by the commutator* $A = [S, T] = S^{-1}T^{-1}ST$*, i.e. every* $B \in \Gamma'$ *can be written in the form* $B = A^{F(S,T)}$*, where the symbolic exponent* $F(S, T) \in \mathbb{Z}[S, T]$ *is a polynomial in* S *and* T.

Proof. Put $\{A\} = \{A^{F(S,T)}, F \in \mathbb{Z}[S, T]\}$. Then we obviously have $\{A\} \subseteq \Gamma'$. On the other hand, every commutator in Γ has the form $[S^i, T^j]$. The claim now follows from the identity given in the next proposition. □

Proposition 1.8.10. $[S^i, T^j] = [S, T]^{(1+S+S^2+\ldots+S^{i-1})(1+T+T^2+\ldots T^{j-1})}$.

Proof. Put $A = [S,T] = S^{-1}T^{-1}ST$; from $T^{-1}ST = SA$ we get $T^{-1}S^2T = SASA = S^2A^{S+1}$, and induction shows

$$T^{-1}S^iT = (T^{-1}ST)^i = S^iA^{1+S+S^2+\ldots+S^{i-1}}.$$

Now we find

$$\begin{aligned} T^{-2}S^iT^2 &= T^{-1}S^iA^{1+S+S^2+\ldots+S^{i-1}}T \\ &= T^{-1}S^iTA^{(1+S+S^2+\ldots+S^{i-1})T} \\ &= S^iA^{(1+S+S^2+\ldots+S^{i-1})(1+T)} \end{aligned}$$

etc. □

It follows from (1) – (4) that the set $\mathfrak{M} = \{f \in \mathbb{Z}[S,T] : A^f = 1\} = \mathrm{Ann}(A)$ is an ideal in the polynomial ring $\mathbb{Z}[S,T]$. It is clear that $\mathfrak{M} = (1)$ if and only if $A = 1$, i.e. iff Γ is abelian. The ideal $\mathfrak{M}$ contains much information about the structure of Γ. For example, Γ' is cyclic as a group if and only if $X, Y \in \mathfrak{M}$ (here $X = S - 1$ and $Y = T - 1$), and that $\Gamma' \simeq \mathbb{Z}/\ell\mathbb{Z}$ if and only if $\mathfrak{M} = (\ell, X, Y)$. More generally we have

Proposition 1.8.11. *$\mathbb{Z}[X,Y] = \mathbb{Z}[S,T]$ and $\Gamma' \simeq \mathbb{Z}[X,Y]/\mathfrak{M}$.*

Proof. The claim $\mathbb{Z}[X,Y] = \mathbb{Z}[S,T]$ is trivially true. Now the group homomorphism $\mathbb{Z}[X,Y] \longrightarrow \Gamma' : F(X,Y) \longmapsto A^{F(X,Y)}$ (from the additive group $\mathbb{Z}[X,Y]$ to the multiplicative group Γ') is onto, and its kernel is $\mathfrak{M}$ by definition. □

The following result will turn out to be quite useful:

Proposition 1.8.12. *If $\mathfrak{M} \neq (1)$ then $\mathfrak{L} = (\ell, X, Y) \mid \mathfrak{M}$.*

Proof. First we notice that there must be an integer $a \in \mathbb{N}$ such that $\ell^a \in \mathfrak{M}$: this follows from the fact that Γ' is a finite ℓ-group. Since $S^\ell \in A$, we have $A^{S^\ell} = A$ and consequently $S^\ell - 1 \in \mathfrak{M}$. But now the congruence $0 \equiv S^\ell - 1 = (X+1)^\ell - 1 = X^\ell - \ell P(X) \bmod \mathfrak{M}$ for some $P(X) \in \mathbb{Z}[X]$ shows that $X^\ell \equiv \ell P(X) \bmod \mathfrak{M}$. Therefore, there is a $b \in \mathbb{N}$ such that $X^{\ell^b} \in \mathfrak{M}$ and $Y^{\ell^b} \in \mathfrak{M}$.

Now let $L = r\ell + sX + tY$ be any polynomial in $\mathfrak{L}$. Using what we have proved so far we see that $L^{\ell^m} \equiv 0 \bmod \mathfrak{M}$ for some $m \in \mathbb{N}$. But now

$$(1+L)^{-1} \equiv 1 - L + L^2 - L^3 + L^4 \pm \ldots \bmod \mathfrak{M}$$

shows that $1 + L$ is a unit modulo $\mathfrak{M}$, since the geometric series on the right hand side is finite.

Similarly one proves that $a + L$ is a unit if $\ell \nmid a$; this shows that every element of $\mathbb{Z}[X,Y] \setminus \mathfrak{L}$ is a unit modulo $\mathfrak{M}$, hence we have $\mathfrak{L} \supseteq \mathfrak{M}$. □

Next we study the subgroups of index ℓ in Γ. Assuming for the sake of simplicity that Γ/Γ' is elementary abelian, these subgroups are

$$C_S = \langle S, \Gamma' \rangle,\ C_T = \langle T, \Gamma' \rangle,\ C_{ST} = \langle ST,\ \Gamma' \rangle, \ldots, C_{ST^{\ell-1}} = \langle ST^{\ell-1}, \Gamma' \rangle.$$

By Artin's reciprocity theorem, these subgroups of index ℓ in Γ correspond to subgroups of order ℓ in $\mathrm{Cl}_\ell(k)$; following Scholz and Taussky, the ideal class corresponding to the coset $S^aT^b\Gamma'$ will be denoted by S^aT^b. Moreover, let κ_S denote the subgroup of ideal classes in $\mathrm{Cl}_\ell(k)$ which capitulate in the extension fixed by C_S, and let κ_T etc. be defined accordingly.

$\ell = 2$

From now on we assume that $\ell = 2$ and $\mathrm{Cl}_2(k) \simeq (2,2)$. We will need the following definitions and relations in addition to those already given:

S^2	$=$	A^{F_S}	T^2	$=$	A^{F_T}	$(ST)^2$	$=$	$A^{F_{ST}}$
X	$=$	$S-1$	Y	$=$	$T-1$	Z	$=$	$ST-1$
$X\,F_S$	$\equiv$	0	$Y\,F_T$	$\equiv$	0	$Z\,F_{ST}$	$\equiv$	0
$Y\,F_S$	$\equiv$	$2+X$	$X\,F_T$	$\equiv$	$-2-Y$	F_{ST}	$\equiv$	F_S+F_T-1-Y
X^2	$\equiv$	$-2X$	Y^2	$\equiv$	$-2Y$	Z^2	$\equiv$	$-2Z$

The formulas for the transfer which we have given above show that

$$\begin{aligned} S \in \kappa_S &\implies \mathrm{Ver}(S) = S^{T+1} = A^{F_S+1} \in C'_S, \\ S \in \kappa_T &\implies \mathrm{Ver}(S) = S^2 = A^{F_S} \in C'_T, \\ S \in \kappa_{ST} &\implies \mathrm{Ver}(S) = S^2 = A^{F_S} \in C'_{ST}. \end{aligned}$$

But C'_S is generated by commutators of the form $[S, A^F] = A^{FX}$, and we conclude that $C'_S = \{A^X\}$. Therefore $A^{F_S+1} \in C'_S$ if and only if $F_S + 1 \equiv 0 \bmod (\mathfrak{M}, X)$. Similarly, $A^{F_S} \in C'_T$ is equivalent to $F_S \equiv 0 \bmod (\mathfrak{M}, Y)$ etc.

Proposition 1.8.13. *Let the notation be as above.*

a) If $S \in \kappa_S$ and $S \in \kappa_T$ then k has capitulation type [0 0 0]*;*

b) $\kappa = [2\ 3\ 1]$ is impossible;

c) $S \in \kappa_S \implies X \in \mathfrak{M}$ and $F_S \equiv -1 \bmod \mathfrak{M}$

d) $S \in \kappa_S$ and $T \in \kappa_T$ implies $\mathfrak{M} = \mathfrak{L}$ and $\Gamma = H_8$;

e) $T \in \kappa_S \cap \kappa_{ST} \implies Y + 2 \in \mathfrak{M}$;

f) $T \in \kappa_S \cap \kappa_{ST}$ and $ST \in \kappa_T$ lead to $\mathfrak{M} = (2^n, X, Y + 2)$ for some $n \geq 1$;

g) If $\kappa = [0\ 3\ 2]$ or $\kappa = [2\ 3\ 2]$ then $\mathfrak{M} = (2^n, X, Y + 2)$ and $F_T \equiv 0 \bmod \mathfrak{M}$; moreover, if $\kappa = [0\ 3\ 2]$ then $F_S \equiv -1 \bmod \mathfrak{M}$, and if $\kappa = [2\ 3\ 2]$ then $F_S \equiv -1 + 2^{n-1} \bmod \mathfrak{M}$.

Proof. We know that $S \in \kappa_S \iff A^{F_S+1} \in \{A^X\}$, and that $S \in \kappa_T \iff A^{F_S} \in \{A^Y\}$. This implies that $F_S + 1 \equiv 0 \bmod (\mathfrak{M}, X)$ and $F_S \equiv 0 \bmod (\mathfrak{M}, T - 1)$. If $\mathfrak{M} \neq (1)$, then $\mathfrak{L} \mid \mathfrak{M}$ implies $1 = F_S + 1 - F_S \equiv 0 \bmod \mathfrak{L}$: this is a contradiction.

Note that a) explains all the forbidden capitulation types except $[2\ 3\ 1] \sim [3\ 1\ 2]$. It is quite easy to exclude this possibility, too: $\kappa = [2\ 3\ 1]$ clearly implies the congruences $F_T \equiv 0 \bmod (\mathfrak{M}, X)$, $F_{ST} \equiv 0 \bmod (\mathfrak{M}, Y)$, $F_S \equiv 0 \bmod (\mathfrak{M}, Z)$. In particular we have $F_S \equiv F_T \equiv F_{ST} \equiv 0 \bmod \mathfrak{L}$, because $\mathfrak{M} \neq (1)$ implies $\mathfrak{L} \mid \mathfrak{M}$. But now $0 \equiv F_{ST} \equiv F_S + F_T - 1 - Y \equiv -1 \bmod \mathfrak{L}$ yields the desired contradiction. This proves b).

c) Next we will show that $S \in \kappa_S$ implies $X \in \mathfrak{M}$. In fact, from the congruence $F_S + 1 \equiv 0 \bmod (\mathfrak{M}, X)$ we deduce that $F_S \equiv -1 + XG \bmod \mathfrak{M}$ for some $G \in \mathbb{Z}[S, T]$. Using $X^2 \equiv -2X \bmod \mathfrak{M}$ we find $0 \equiv XF_S \equiv -X - X^2G \equiv -X(1 - 2G) \bmod \mathfrak{M}$. But $1 - 2G$ is a unit in $\mathfrak{M}$, hence we get $X \equiv 0 \bmod \mathfrak{M}$ as claimed.

d) Now we claim that $S \in \kappa_S$ and $T \in \kappa_T$ leads to $\mathfrak{M} = \mathfrak{L}$ and $\Gamma = H_8$. In fact, we know that $X, Y \in \mathfrak{M}$, and we have the congruences $F_S + 1 \equiv F_T + 1 \equiv 0 \bmod \mathfrak{M}$. This gives $0 \equiv XF_T \equiv -2 - Y \equiv -2 \bmod \mathfrak{M}$, and we find $\mathfrak{M} = \mathfrak{L}$. Moreover we get $S^2 = A^{F_S} = A^{-1}$ and $T^2 = A^{-1}$ as well as $A^2 = 1 = [A, S] = [A, T]$. The group defined by these relations is the quaternion group of order 8.

e) $T \in \kappa_S \cap \kappa_{ST}$ implies $Y + 2 \in \mathfrak{M}$. In fact we have $F_T \equiv 0 \bmod (\mathfrak{M}, X)$ and $F_T \equiv 0 \bmod (\mathfrak{M}, Z)$, where $Z = XY = XY + X + Y$. This shows that $F_T \equiv XZG \bmod \mathfrak{M}$ for some $G \in \mathbb{Z}[X, Y]$. Replacing Z by XY and using $X^2 + 2X \equiv 0 \bmod \mathfrak{M}$ we get $F_T \equiv -X(2 + Y) \bmod \mathfrak{M}$. Next we find $-2 - Y \equiv XF_T \equiv -X^2(2 + Y)G \bmod \mathfrak{M}$, hence $0 \equiv (2 + Y)(1 + X^2G) \bmod \mathfrak{M}$. But $1 + X^2G$ is a unit modulo $\mathfrak{M}$, therefore we must have $Y + 2 \in \mathfrak{M}$.

f) $T \in \kappa_S \cap \kappa_{ST}$ and $ST \in \kappa_T$ lead to $\mathfrak{M} = (2^n, X, Y + 2)$ for some $n \geq 1$. From $F_{ST} \equiv 0 \bmod (\mathfrak{M}, Y)$ we get $F_{ST} \equiv YG \equiv -2G \bmod \mathfrak{M}$ for some $G \in \mathbb{Z}[X, Y]$. But $Y + 2 \in \mathfrak{M}$ shows $F_{ST} \equiv F_S + F_T - 1 - Y \equiv F_S + 1 \bmod \mathfrak{M}$. Using $XF_S \in \mathfrak{M}$ we finally get $X \equiv -2GX \bmod \mathfrak{M}$ and $X(1 + 2G) \in \mathfrak{M}$. Since $1 + 2G$ is a unit, our claim $X \in \mathfrak{M}$ is proved.

g) If $\kappa = [0\ 3\ 2]$ or $\kappa = [2\ 3\ 2]$ then $\mathfrak{M} = (2^n, X, Y + 2)$ and $F_T \equiv 0 \bmod \mathfrak{M}$. This follows from what we just have proved.

If $\kappa = [0\ 3\ 2]$ then $F_S \equiv -1 \bmod \mathfrak{M}$. This follows from part c).

If $\kappa = [2\ 3\ 2]$ then $F_S \equiv -1 + 2^{n-1} \bmod \mathfrak{M}$. In fact we have $2F_{ST} \equiv -YF_{ST} \equiv -Y(F_S + 1) \equiv -2 - Y - X \equiv 0 \bmod \mathfrak{M}$ as well as $F_{ST} \equiv F_S + 1 \bmod \mathfrak{M}$. The possibility $F_{ST} \equiv 0 \bmod \mathfrak{M}$ would imply $F_S \equiv -1 \bmod \mathfrak{M}$ and $S \in \kappa_S$; this shows that we must have $F_{ST} \equiv 2^{n-1} \bmod \mathfrak{M}$ and, therefore, $F_S \equiv -1 + 2^{n-1} \bmod \mathfrak{M}$ as claimed. □

The following proposition is taken from Taussky's paper [141]:

Proposition 1.8.14. *If $\mathfrak{M} \neq (1)$ then we can choose S and T in such a way that $X \in \mathfrak{M}$ and $Y \equiv 2u \bmod \mathfrak{M}$, where u is some odd integer. In particular, if G is a 2-group such that $G/G' \simeq (2,2)$ then G' is cyclic.*

Proof. If $\mathfrak{M} = (1)$ there is nothing to prove. If not then $\mathfrak{L} \mid \mathfrak{M}$, and the congruence $F_{ST} \equiv F_S + F_T - 1 - Y \bmod \mathfrak{M}$ shows that we may assume without loss of generality that $F_S(0,0) \not\equiv 0 \bmod 2$ (otherwise we just replace T by ST and observe that this leaves $A = [S,T] = [S,ST]$ invariant).

From the congruences (all taken modulo $\mathfrak{M}$) $XF_S \equiv 0$ and $YF_S \equiv 2 + X$ we get $XYF_S \equiv 0$ and $X^2 \equiv -2X$; similarly we can derive $Y^2 \equiv -2Y$. This shows that every polynomial in X, Y can be written as a $\mathbb{Z}$-linear combination of X, Y, and XY. We can therefore write

$$F_S = u + aX + bY + cXY$$

for $u, a, b, c \in \mathbb{Z}$ and u odd. Multiplying this equation by X we get

$$0 \equiv XF_S \equiv (u - 2a)X + (b - 2c)XY, \tag{1.6}$$

and, similarly,

$$2 + X \equiv Y\,F_S \equiv (u - 2b)Y + (a - 2c)XY. \tag{1.7}$$

Let k be the smallest integer such that $XY^k \equiv 0$ (such a k exists since $Y^2 \equiv 2Y$ and because the order of A is a power of 2).

Multiplying XF_S by Y^{k-1} we find $0 \equiv (u - 2a)XY^{k-1}$; since u is odd, $u - 2a$ is a unit mod $\mathfrak{M}$, and we must have XY^{k-1}. This gives $XY \in \mathfrak{M}$, and from (1.6) we read off that $X \in \mathfrak{M}$. But now (1.7) shows that $Y \equiv 2u'$ for some odd integer u', hence we have $Y \sim 2$ as claimed.

Therefore every polynomial in $\mathbb{Z}[X, Y]$ is congruent modulo $\mathfrak{M}$ to an integer: every symbolical power of A is therefore a common power, and in particular, G' is cyclic. □

$\ell = 3$

Next we will describe the results of Scholz and Taussky [392]. The capitulation types are defined as above; since the paper only treats imaginary quadratic base fields, Scholz and Taussky need not consider capitulation types containing a 0. Here's what they found:

1. If k is imaginary quadratic, then $\mathfrak{M} \neq (1)$;
2. If $\mathfrak{M} \neq (1)$, then $\mathfrak{M} \equiv 0 \bmod \mathfrak{L}$;
3. If $\mathfrak{M} \not\equiv 0 \bmod \mathfrak{L}_2 = (3, X^2, XY, Y^2)$ then in all four cubic unramified extensions the same ideal class (say S_1) capitulates, and we have $\mathfrak{M} = \mathfrak{L}, S_1^3 = 1$, and $S_2^3 = A$.
4. If k is imaginary quadratic, then $\mathfrak{M} \neq \mathfrak{L}$.
5. If k has capitulation type [1 1 2 3] (i.e. if the ideal class S_1 capitulate in the fixed fields of S_1 and S_2, and if S_2 and S_1S_2 capitulate in the fixed fields of S_1S_2 and $S_1^2S_2$, respectively) then $\mathfrak{M} = \mathfrak{L}_2$, $F_1 = F_2 = X$.

The knowledge of $\mathfrak{M}$ is not sufficient for determining the group structure of $\Gamma = \mathrm{Gal}\,(k^2/k)$, but we can at least see that

a) if $\mathfrak{M} = \mathfrak{L}$, then $\#\Gamma = 3^3$ and $\Gamma' = \langle A \rangle$, i.e. Γ is one of the two non-abelian groups of order 27;

b) if $\mathfrak{M} = \mathfrak{L}_2$, then $\#\Gamma = 3^5$ and $\Gamma' = \langle A, A^X, A^Y \rangle \simeq (3,3,3)$; moreover, $\Gamma/\Gamma' \simeq (3,3)$.

In both cases, the complete structure can be deduced from F_1 and F_2. In (5), for example, we find

$$\Gamma = \langle S_1, S_2 : S_1^9 = S_2^9 = 1, [S_2, S_1] = A, A^X = [S_1, A^{-1}] = S_1^3 = S_2^3, A^3 = 1, * \rangle,$$

where $*$ stands for the relations coming from $\langle A, A^X, A^Y\rangle \simeq (3,3,3)$.

If k is imaginary quadratic, then (1) – (4) imply that $\mathfrak{M} \equiv 0 \bmod \mathfrak{L}_2$, i.e. that $\mathrm{Gal}\,(k^2/k)$ is a 3-group of order at least 3^5.

The work of Scholz and Taussky was extended in a number of papers. Taussky [422, 424] proved results like

Proposition 1.8.15. *Let $p > 3$ be an odd prime, and put $X = S - 1$, $Y = T - 1$. Let Γ be the ℓ-group of order p^5 defined by $\mathfrak{M} = (p, X^2, XY, Y^2)$. If k is a number field such that $\mathrm{Gal}\,(k^2_{(p)}/k) \simeq \Gamma$, then all cyclic unramified p-extensions K/k are of type A.*

Chang and Foote [433] (see also [430]) introduced the *capitulation number* ν for fields k with $\mathrm{Cl}_p(k) \simeq (p,p)$: this is the number of unramified cyclic p-extensions K/k such that $\kappa_{K/k} = \mathrm{Cl}_p(k)$ (i.e. such that the whole p-class group capitulates). Clearly $\nu \in \{0, 1, \ldots, p+1\}$. For $p = 2$ we have seen that $\nu \in \{0, 1, 3\}$; Chang and Foote showed that, for $p \geq 3$ and for any $\nu \in \{0, 1, \ldots, p+1\}$, there are p-groups Γ_ν such that any field k with $\mathrm{Gal}\,(k^2_{(p)}/k) \simeq \Gamma_\nu$ has capitulation number ν.

In [392], Scholz and Taussky claimed that the p-class field tower of an imaginary quadratic number field k with capitulation type $\mathfrak{A}_\alpha$ has length 2; their proof (or rather its sketch) was shown to be erroneous by Brink and Gold [182] (cf. also Brink [175]).

Related articles are Browkin [145, 146], Schmithals [440], Heider and Schmithals [441], Nebelung [453], Mayer [457] and Miyake [188], who studied p-groups with the following property: for every normal subgroup H of G such that G/H is cyclic, the kernel of the transfer map $G/G' \longrightarrow H/H'$ has order $(G : H)$. If $G = \mathrm{Gal}\,(k^2/k)$, where k^2 is the second p-class field of an imaginary quadratic number field k, then G clearly has this property, since the capitulation kernel in cyclic unramified extensions K/k equals $(K : k)$.

Arrigoni [195] showed that this condition follows from G being a Schur σ-group and proved the following generalization of a result of Scholz and Taussky:

Theorem 1.8.16. *Let k be an imaginary quadratic number field and p and odd prime. If $\mathrm{Cl}_p(k) \simeq (q_1, q_2)$, where q_1 and q_2 are powers of p such that $q_1 \mid q_2$, then q_1^3 divides the class number $h(k^1)$ of the Hilbert p-class field k^1 of k. If $h(k^1) = q_1^3$, then $\mathrm{Cl}_p(k^1) \simeq (q_1, q_1, q_1)$, and the p-class field tower of k is finite.*

For capitulation in $\mathbb{Z}_p$-extensions, see Kida [434] and Fukuda and Komatsu [466].

1.8.4 Principal Ideal Theorems

Furtwängler's principal ideal theorem was subsequently generalized, for example by Terada [402]:

Proposition 1.8.17. *If K/k is cyclic and unramified, then the ambiguous ideal classes of K capitulate already in k^1.*

Another result also due to Terada which contains Prop. 1.8.17 as a special case is

Proposition 1.8.18. *If K/k is cyclic, then the ambiguous ideal classes of K capitulate already in K_{gen}.*

Adachi [426] conjectured that this theorem can be generalized to abelian extensions K/k, i.e. that the ambiguous ideal classes of K capitulate in K_{cen}. Miyake [452], however, gave a group theoretical counterexample. Nevertheless, the following theorem holds:

Proposition 1.8.19. *Let K/k be a finite abelian extension; then the strongly ambiguous ideal classes of K capitulate in K_{gen}.*

The following result due to Miyake is a mild generalization of Hilbert's Theorem 94 to abelian extensions:

Proposition 1.8.20. *Let $k \subseteq K \subseteq k^1$; if $K_{gen} = K_{cen}$ (this implies $K_{gen} = k^1$) then $(K : k) \mid \#\,\kappa_{K/k}$.*

In fact, if K/k is cyclic, then $K_{\mathrm{gen}} = K_{\mathrm{cen}}$, and Theorem 94 results. Suzuki [459] finally proved that Theorem 94 also holds in abelian extensions by reducing it to a group theoretical statement via Artin's reciprocity law:

Theorem 1.8.21. *For unramified abelian extensions K/k, the order of the capitulation kernel $\kappa_{K/k}$ is divisible by $(K:k)$.*

Families of number fields whose ideal class group capitulates in a subfield of the Hilbert class field have been studied by Iwasawa [451, 456], Fujisaki [455], and Benjamin, Sanborn and Snyder [463]. Necessary conditions for a p-class field tower to be abelian have been given by Bond [436]; Hilbert's Theorem 94 for extensions of type (p^n, p) was proved by Schipper [427] and Bond [294].

1.9 Class Field Towers

1.9.1 Terminating Class Field Towers

We start with one of the simplest means to decide whether the p-class field tower of a given field k terminates:

Proposition 1.9.1. *If K/k is an unramified p-extension such that $k^1_{(p)} \subset K$, and if $\mathfrak{M}(G) = 1$, where $G = \mathrm{Gal}\,(K/k)$, then the p-class field tower of k terminates with K.*

Proof. Let L be the central p-class field of K with respect to k; Galois theory and Artin's reciprocity law show that $k^1_{(p)}$ is the fixed field of G', and the maximality of the p-class field implies that $k^1_{(p)}$ is also the fixed field of Γ'. Now $k^1_{(p)} \subset K$ shows that $\mathrm{Gal}\,(L/K) \subset \Gamma'$, hence $\mathrm{Gal}\,(L/K) \subset \Gamma' \cap Z(\Gamma)$, contradicting the assumption $\mathfrak{M}(G) = 1$. □

As a corollary of Prop. 1.9.1 we get the well known

Proposition 1.9.2. *If k is a number field with cyclic p-class group, then its p-class field tower terminates with $k^1_{(p)}$, and we have $E_k = N_{K/k}E_K$ and $\mathrm{Cl}_p(K) \simeq \mathrm{Cl}_p(k)^{(K:k)}$ for every subfield K of $k^1_{(p)}/k$.*

Proof. $k^1_{(p)}/k$ is cyclic, hence $\mathfrak{M}(\mathrm{Gal}\,(k^1_{(p)}/k)) = 1$. Now Prop. 1.9.1 shows that every unit in k is the norm of a unit in $k^1_{(p)}$, and the formula $N_{L/k}\eta = N_{L/K}\left(N_{K/k}\eta\right)$ proves the second claim. Since $N_{K/k}\mathrm{Cl}_p(K)$ has index $(K:k)$ in $\mathrm{Cl}_p(k)$ (cf. Takagi's main theorem), we conclude that $\#\mathrm{Cl}_p(k)^{(K:k)}$ divides the class number of K. On the other hand we know that $1 = N_{k^1/K}\mathrm{Cl}_p(k^1)$ has index $(k^1 : K)$ in $\mathrm{Cl}_p(K)$, thus the p-class number of K divides $\#\mathrm{Cl}_p(k)^{(K:k)}$. □

Next we study groups with two generators. The following result due to O. Taussky is well known (Thm. 1.8.8); we will nevertheless give a proof, mainly in order to demonstrate how to use the concept of the Schur multiplier. We also remark that D_n will denote the dihedral group of order $2n$.

Proposition 1.9.3. *Let G be a 2-group of order 2^m such that $G/G' \simeq (2,2)$. Then either $G \simeq (2,2)$, or G is a dihedral, semidihedral or quaternion group of order $2^m, m \geq 3$.*

Proof. If $G' = 1$ there is nothing to prove, so assume that $G' \neq 1$. Then by a well known property of p-groups there is a normal subgroup $N_1 \lhd G$ such that N_1 is a subgroup of index 2 in G' and $G'/N_1 \subseteq Z(G/N_1)$. Hence $1 \longrightarrow G'/N_1 \longrightarrow G_1 = G/N_1 \longrightarrow G_0 = (2,2) \longrightarrow 1$ is a covering of G_0: it suffices to check that we have $G_1' \simeq G'N_1/N_1 = G'/N_1$ and $G'/N_1 \subseteq Z(G_1) \cap G_1'$. Now $\mathfrak{M}(G_0) \simeq \mathbb{Z}/2\mathbb{Z}$ implies that G_1 is a covering group of G_0, so either $G \simeq H_8$ (quaternion group of order 8) or $G_1 \simeq D_4$ (dihedral group of order 8).

In case $|G| = 8$ we are done; otherwise N_1 contains a subgroup N_2 such that $N_2 \lhd G$ and $N_1/N_2 \subseteq Z(G/N_2)$. Therefore $1 \longrightarrow N_1/N_2 \longrightarrow G_2 = G/N_2 \longrightarrow G_1 = G/N_1 \longrightarrow 1$ is a covering, and since $\mathfrak{M}(H_8) = 1$, we must have $G_1 \simeq D_4$. Now $\mathfrak{M}(D_4) \simeq \mathbb{Z}/2\mathbb{Z}$ shows that the covering is maximal, hence G_2 is a covering group of G_1, and we must have $G_2 \simeq H_{16}$, $G_2 \simeq SD_{16}$ (semidihedral group of order 16), or $G_2 \simeq D_8$.

The assertion now follows by induction, noting that $\mathfrak{M}(SD_{2n}) \simeq \mathfrak{M}(H_n) = 1$ for all $n = 2^m \geq 8$, $\mathfrak{M}(D_n) \simeq \mathbb{Z}/2\mathbb{Z}$ for $n = 2^m \geq 4$, and that these are the only covering groups of D_n (cf. Schur [563] or Karpilovsky [590]). □

This proof also sheds some light on the group-theoretical background of the following result of Furtwängler [378]. In this paper, he proved the existence of number fields k such that their 2-class field k_2^1 has even class number: this discovery led Furtwängler to the question whether there are number fields whose class field towers do not terminate, and so gave rise to the "class field tower problem" solved later by Golod and Shafarevic.

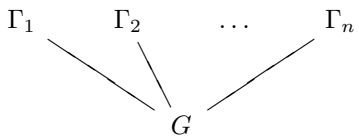
Proposition 1.9.4. *Let k be a number field such that $Cl_2(k) \simeq (2,2)$. Then, $Cl_2(k_2^1)$ is cyclic, and the 2-class field tower of k terminates with k_2^2.*

Proof. Let $K = k_2^2$; then $G = \mathrm{Gal}\,(K/k)$ is a 2-group such that $G/G' \simeq (2,2)$, hence is one of the groups listed in Prop. 1.9.3. If $G \simeq H_m$ or $G \simeq SD_m$, then we have $\mathfrak{M}(G) = 1$, and Proposition 2 proves our claim. If $G \simeq SD_m$, however, either $h(K)$ is odd (and there is nothing to prove), or $h(K)$ is even; in this case, there is an unramified quadratic central extension L/K such that

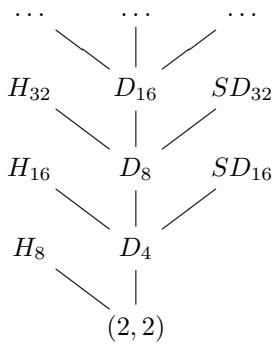
$$1 \longrightarrow \mathrm{Gal}\,(L/K) \longrightarrow \mathrm{Gal}\,(L/k) \longrightarrow G = \mathrm{Gal}\,(K/k) \longrightarrow 1$$

is a covering. This implies that $\mathrm{Gal}\,(L/k)$ is isomorphic to one of the groups listed in 2.2, hence L/k_2^1 is an unramified cyclic 2-extension contradicting the fact that $K = k_2^2$ is the maximal unramified extension of k. v The fact that $Cl_2(k_2^1)$ is cyclic follows from Artin's isomorphism $Cl_2(k_2^1) \simeq G'$ and the fact that the 2-groups D_n, H_n, and SD_n have cyclic commutator groups. □

Suppose that a p-group G has covering groups $\Gamma_1, \Gamma_2, \ldots, \Gamma_n$, and look at the graph



The Γ_i are p-groups, hence we can define inductively a (possibly infinite) graph by inserting the covering groups of the Γ_i etc. The final result is called the *covering tree* of G and will be denoted by $\mathfrak{D}(G)$. A cyclic groups has trivial covering tree, and it follows from the work of Schur that



is the covering tree of $G = (2,2)$. Obviously, $\mathfrak{D}(G)$ contains only metabelian groups, i.e. groups with $G'' = 1$. Let the length of a p-group be the smallest integer n such that $G^{(n)} = 1$, where the nth derived group $G^{(n)}$ is defined inductively by $G^{(0)} = G$ and $G^{(n+1)} = [G^{(n)}, G^{(n)}]$. O. Taussky asked for all p-groups such that $\mathfrak{D}(G)$ contains only groups of bounded length; Hobby [492] obtained partial results, and Serre [499] succeeded in proving that only cyclic groups and $(2,2)$ have this property. This seems to be the only non-trivial result on covering trees of p-groups; it would be highly desirable to have a description even of the lower layers of $\mathfrak{D}(G)$ for $G = (2,4)$.

If k is a number field with 2-class field k_2^1, and if $\mathrm{Cl}_2(k_2^1) \simeq (2,2)$, then 1.9.3 shows that the 2-class field tower of k terminates with k_2^3; actually, a little bit more is true:

Proposition 1.9.5. *If k is a number field such that $\mathrm{Cl}_2(k_2^1) \simeq (2,2)$, then we have $k_2^3 = k_2^2$.*

Table 1.3:

p	f	h
163	$y^4 - y^3 - 7y^2 + 2y + 9$	1
277	$y^4 - y^3 - 11y^2 + 4y + 12$	2
349	$y^4 - y^3 - 10y^2 + 3y + 20$	1
397	$y^4 - 13y^2 - 2y + 19$	1
547	$y^4 - 2y^3 - 19y^2 + 11y + 10$	1
607	$y^4 - 2y^3 - 13y^2 + 7y + 33$	2
709	$y^4 - 17y^2 - 13y + 35$	1
853	$y^4 - y^3 - 28y^2 + 31y - 2$	1
937	$y^4 - y^3 - 16y^2 + 11y + 54$	1

Proof. Suppose that $k_2^3 \neq k_2^2$ and let $G = \mathrm{Gal}\,(k_2^3/k)$; then 1.9.3 shows that $G' \simeq \mathrm{Gal}\,(k_2^3/k_2^1)$ is dihedral, semidihedral or quaternionic, and all these groups have cyclic centers. Burnside has shown that p-groups G with cyclic $Z(G')$ have cyclic G'. But if k_2^3/k_2^1 is cyclic, we must have $k_2^3 = k_2^2$ in contradiction to our assumption. □

In some special cases we can improve Prop. 1.9.4:

Proposition 1.9.6. *Suppose that k is a number field with odd class number, and let K/k be a cyclic cubic extension such that $\mathrm{Cl}_2(K) \simeq (2,2)$. Then $\mathrm{Gal}\,(K_2^1/k) \simeq A_4 \simeq PSL(2,3)$, where either*

a) K_2^1 has odd class number; or

b) $\mathrm{Cl}_2(K_2^1) \simeq \mathbb{Z}/2\mathbb{Z}$, and $\mathrm{Gal}\,(K_2^1/k) \simeq \widetilde{A}_4 \simeq SL(2,3)$.

Proof. If there were an ideal class $c \in \mathrm{Cl}_2(K)$ fixed by $\mathrm{Gal}\,(K/k)$, then the norm to k of c would not be trivial in contradiction to our assumption that k has odd class number. Now let $\sigma \in \mathrm{Gal}\,(K/k) \setminus \{1\}$; we can choose ideal classes $a, b \in \mathrm{Cl}_2(K)$ such that $\mathrm{Cl}_2(K) = \langle a,\, b\rangle$ and $\sigma(a) = b, \sigma(b) = ab, \sigma(ab) = a$. This implies that $\mathrm{Gal}\,(K^1/k) \simeq A_4$, because $1 \longrightarrow \langle a,\, b\rangle \longrightarrow A_4 \longrightarrow \langle\sigma\rangle \longrightarrow 1$ is the extension which corresponds to this action.

Now suppose that $K_2^2 \neq K_2^1$, and let L be the unramified quadratic extension of K_2^1 (recall that, by 1.9.3, $\mathrm{Cl}_2(K_2^1)$ is cyclic). Let L'/K_2^1 be any extension conjugated to L/K_2^1 over k; then L'/K_2^1 is an unramified quadratic extension, and since $\mathrm{Cl}_2(K_2^1)$ is cyclic, we must have $L = L'$, i.e. L/k is normal. Moreover, $\mathrm{Gal}\,(L/K_2^1)$ is central in $\mathrm{Gal}\,(L/k)$, because any normal subgroup of order 2 is contained in the center of a group. Therefore, G is a covering group of A_4; Schur has shown that $\widetilde{A}_4$ is the only covering group of A_4. We conclude that $G' \simeq H_8$, and since $\mathfrak{M}(H_8) = 1$, the 2-class field tower of K terminates with K_2^2. □

Table 1.4 gives the cyclic cubic fields k of prime conductor $p < 1000$ with even class number, a polynomial of degree 4 whose roots generate the 2-class field of k, and the class number of the quartic field generated by a root of f. Table 1.4 contains some examples of cyclic cubic fields of prime conductor p whose 2-class field tower is generated by the roots of a polynomial g of degree 8 with Galois group $\widetilde{A}_4$; the last column h gives the class number of this octic extension.

Example 1.9.1. *Let $d = -283$ and $k = \mathbb{Q}(\sqrt{d}\,)$; k has class number 3, hence there is an unramified cubic cyclic extension K/k. The three cubic subfields of $K/\mathbb{Q}$ have class number 2, and this implies that $\mathrm{Cl}(K) \simeq (2,2)$. Let F denote one of the (conjugate) number fields of degree $(F : \mathbb{Q}) = 4$ with $\mathrm{disc}\, F = -283$; then the normal closure of $F/\mathbb{Q}$ is the class field K^1 of K. A computation of the number of ambiguous ideal classes in $F(\sqrt{d}\,)/F$ yields that $F(\sqrt{d}\,)$ and hence K^1 have even class number (recall that $(K^1 : F(\sqrt{d}\,)) = 3$, so no ideal class of even order capitulates in $K^1/F(\sqrt{d}\,)$). Using Odlyzko bounds, one easily shows that $h(K^1) = 2$ and that $K^2 = k^3 = k^4$. Now Prop. 1.9.6 tells us $\mathrm{Gal}\,(K^1/k) \simeq \widetilde{A}_4$. The case $d = -331$ can be treated in a similar way.*

Table 1.4:

p	g	h
163	$x^8+9x^6+23x^4+14x^2+1$	1
349	$x^8+18x^6+75x^4+85x^2+1$	1
397	$x^8+150x^6+135x^4+22x^2+1$	1
547	$x^8+1057x^6+1739x^4+554x^2+1$	3
709	$x^8+125x^6+215x^4+42x^2+1$	7
853	$x^8+93x^6+1755x^4+3546x^2+1$	1
937	$x^8+1486x^6+341591x^4+13077x^2+1$	1

It is possible to find explicit generators:

$$\begin{array}{llll} & k=\mathbb{Q}(\sqrt{-283}\,) & & k=\mathbb{Q}(\sqrt{-331}\,) \\ k^1= & k(\alpha),\ \alpha^3+4\alpha-1=0, & k^1= & k(\alpha),\ \alpha^3-4\alpha^2+8\alpha-9=0, \\ k^2= & k^1(\beta),\ \beta^4-\beta-1=0, & k^2= & k^1(\beta),\ \beta^4-2\beta^2-3\beta-1=0, \\ k^3= & k^2(\gamma),\ \gamma^2=-3+4\beta^2-4\beta^3, & k^3= & k^2(\gamma),\ \gamma^2=-3-4\beta+4\beta^3. \end{array}$$

The existence of these unramified $\widetilde{A}_4$-extensions of k has already been proved by Tate (cf. Serre [56], as well as Honda [25], Jehanne [531], in particular his thesis [532]).

Proposition 1.9.7. *Let k be a number field with p-class field tower $k^n_{(p)}$; if $\mathrm{Cl}_p(k^1_{(p)})$ has rank ≤ 2, then $\mathrm{Cl}_p(k^2_{(p)})$ is cyclic, and $k^3_{(p)}=k^4_{(p)}$. If, moreover, $\mathrm{Cl}_p(k)$ has rank ≤ 2, then $k^2_{(p)}=k^3_{(p)}$.*

Proof. This is a translation of the following group-theoretical result due to Blackburn: let $d(G)$ denote the number of generators of G, i.e. the rank of the elementary abelian p-group $G/G'G^p$. If G is a p-group such that $d(G')\leq 2$, then G'' is cyclic, and G' has class at most 2. If moreover $d(G)\leq 2$, then G' is abelian. □

We know the following bounds of the p-rank of $\mathrm{Cl}_p(k^1_{(p)})$:

Proposition 1.9.8. *If $\mathrm{Cl}_p(k)\simeq(p^m,p^n)$, then $\operatorname{rank}\mathrm{Cl}_p(k^1_{(p)})\leq(p^m-1)(p^n-1)$.*

Obviously, Prop. 1.9.8 contains Prop. 1.9.4 as a special case. If $\mathrm{Cl}_2(k)\simeq(2,4)$, then the 2-rank $r_2(k^1_2)$ of $\mathrm{Cl}_2(k^1_2)$ is bounded by $0\leq r_2(k^1_2)\leq 3$, and all these values actually occur:

$\operatorname{disc}k$	$\operatorname{rank}\mathrm{Cl}_2(k^1_2)$	$\mathrm{Cl}_2(k^1_2)$	$\mathrm{Gal}\,(k^2_2/k)$
-264	0	1	$(2,4)$
-260	1	$\mathbb{Z}/2\mathbb{Z}$	M_{16}
-580	1	$\mathbb{Z}/4\mathbb{Z}$	32.032
-820	1	$\mathbb{Z}/8\mathbb{Z}$	64.139
-1443	2	$(2,8)$	128.?
$-25\ 355$	3	?	?

The example with discriminant $d=-1443$ has been computed using pari; the fact that $\operatorname{rank}\mathrm{Cl}_2(k^1_2)=3$ for $k=\mathbb{Q}(\sqrt{-25\ 355}\,)$ follows from Prop. 1.9.7 and the result of Schmithals [170] which says that k has an infinite 2-class field tower.

The proof of Prop. 1.9.8 consists once more of a reduction to a group-theoretical result due to Blackburn via Artin's reciprocity law:

> Let G be a p-group such that $G/G'\simeq(p^m,p^n)$; then G' can be generated by $(p^m-1)(p^n-1)$ elements.

Another quite useful criterium to prove the finiteness of 2-class field towers is the following:

Proposition 1.9.9. *([214]) Let k be a number field with $\mathrm{Cl}_{k,2} \simeq (2^m, 2^n)$. If there is an unramified quadratic extension of k with 2-class number 2^{m+n-1}, then all three unramified quadratic extensions of k have 2-class number 2^{m+n-1}, and the 2-class field tower of k terminates with k^1.*

A criterium going in the other direction was proved by Benjamin [189] as well as in [214] (compare the discussion after Cor. 1.3.14):

Proposition 1.9.10. *If k is an imaginary quadratic number field whose 2-class group contains a subgroup of type $(2,2,2)$, then $\mathrm{Cl}_2(k^1)$ has rank ≥ 2.*

1.9.2 Golod-Shafarevic: Infinite Class Field Towers

The first result on 'large' class field towers is due to Scholz [136], who proved that p-class field towers can be arbitrarily large:

Proposition 1.9.11. *For any prime p and every integer $n \in \mathbb{N}$ there exists a cyclic extension $k/\mathbb{Q}$ of degree p such that $k_{(p)}^{n+1} \neq k_{(p)}^n$.*

Moriya [138] proved that the class number of $k_{(p)}^1$ is divisible by p if $\operatorname{rank} \mathrm{Cl}_p(k) \geq 1 + \operatorname{rank} E/E^p$. Finally Fröhlich discovered the following result:

Proposition 1.9.12. *Let $k/\mathbb{Q}$ be a cyclic extension of prime degree p; if $\#\mathrm{Ram}(k/\mathbb{Q}) \geq 4$ then $k_{(p)}^2 \neq k_{(p)}^1$. Moreover, this is best possible, since there exist cyclic extensions $k/\mathbb{Q}$ with $\#\mathrm{Ram}(k/\mathbb{Q}) \leq 3$ such that $\mathrm{Cl}_p(k^1) = 1$.*

The conjecture that class field towers are always finite was disproved by Golod and Shafarevic [148]; the following inequality of Vinberg and Gaschütz is slightly sharper than the original (see also Serre [153], Panella [152], and Roquette [155]):

Theorem 1.9.13. *Let k be an algebraic number field, p a prime number, and suppose that the p-class field tower is finite and terminates with $K = k_{(p)}^\infty$. Put $d = \operatorname{rank} \mathrm{Cl}_p(k)$ and $r = d + \dim_p E_k/N_{K/k}E_K$; then $d^2 < 4r$.*

(Here, $\dim_p G$ denotes the dimension of the $\mathbb{F}_p$-vector space G/G^p for any abelian group G). In particular, if the p-rank of the class group is large compared to the unit group, then the p-class field tower of k must be infinite. More exactly:

Corollary 1.9.14. *Let κ denote the $\mathbb{Z}$-rank of the unit group E_k, und put $\delta = 1$ if $\zeta_p \in k$ and $\delta = 0$ otherwise. If*

$$d \geq 2 + 2\sqrt{\kappa + \delta + 1} \tag{1.8}$$

then k has infinite p-class field tower.

Refinements of the theorem of Golod and Shafarevic have been obtained by Koch [156], Vinberg [151], and Schoof [179]. Before we can give Schoof's version, we have to introduce some notation. For a p-group G, let I denote the augmentation ideal of the group ring $\mathbb{F}_p[G]$. The exact sequence $0 \longrightarrow I \longrightarrow \mathbb{F}_p[G] \longrightarrow \mathbb{F}_p \longrightarrow 0$ induces a canonical isomorphism $H_2(G, \mathbb{F}_p) \simeq H_1(G, I)$. The natural maps

$$\ldots \longrightarrow H_1(G, I^3) \longrightarrow H_1(G, I^2) \longrightarrow H_1(G, I)$$

allow us to define factor groups

$$R_k \;=\; \frac{\mathrm{im}\,(H_1(G, I^{k-1}) \longrightarrow H_1(G, I))}{\mathrm{im}\,(H_1(G, I^k) \longrightarrow H_1(G, I))}, \quad (k \geq 2).$$

Put $r_k = \dim_p R_k$; then there is only a finite number of nonzero r_k's, and we have $\sum_{k\geq 2} r_k = r$. Schoof proved

Theorem 1.9.15. *If G is a finite p-group, then $\sum_{k\geq 2} r_k t^k - dt + 1 \;>\; 0 \quad$ for $\quad 0 < t < 1$.*

Substituting $t = d/2r$ in the inequality $rt^2 - dt + 1 \geq \sum_{k\geq 2} r_k t^k - dt + 1 > 0$ we get back the inequality of Vinberg and Gaschütz.

Another refinement of this inequality is due to Gaschütz and Newman [158]. For finite p-groups G they used the dimension subgroups $G_1 = [G,G]G^p$ and $G_2 = [G,G_1]G_1^p$ (for $p = 2$), $G_2 = [G,G_1]G^p$ (for $p \geq 3$) introduced by Gruenberg, put $d = \operatorname{rank} G_1$ and $e = \operatorname{rank} G_2$ and proved

Theorem 1.9.16. *If G is a finite p-group, then*

$$r \geq \frac{1}{2}d^2 - (-1)^{p-1}\frac{d}{2} - e \tag{1.9}$$

and

$$r > \frac{1}{2}d^2 - (-1)^{p-1}\frac{d}{2} - e + (e + (-1)^{p-1}\frac{d}{2} - \frac{1}{4}d^2)\frac{d}{2}. \tag{1.10}$$

It is an elementary exercise to deduce $r > d^2/4$ from these two inequalities. If $G = \operatorname{Gal}(K/k)$, then the fixed field of G_1 is the maximal elementary abelian unramified extension L of k, and the fixed field of G_2 is the maximal elementary abelian extension of L contained in L_{cen}.

For quadratic number fields and odd primes p, Koch and Venkov [163] and Schoof [179] improved the result of Golod and Shafarevic by showing

Proposition 1.9.17. *Let k be a quadratic number field or a quadratic extension of an imaginary quadratic number field F with class number $h(F) \not\equiv 0 \bmod p$. If $\operatorname{rank} \mathrm{Cl}_p(k) \geq 3$ and p is an odd prime, then k has infinite p-class field tower.*

This can be deduced from Thm. 1.9.15 by proving that $r_k = 0$ for all even $k \geq 2$ in this case, using the action of $\operatorname{Gal}(k/F)$ on the groups R_k. Observing $r_2 = 0$ and $r - d \leq 1$ we find $(d+1)t^3 - dt + 1 \geq \sum_{k\geq 2} r_k t^k - dt + 1 > 0$, and substituting $t = \frac{1}{2}$ gives the result.

This proposition fails to hold for $p = 2$, as Martinet [166] noticed: the field $k = \mathbb{Q}(\sqrt{-105})$ has $\mathrm{Cl}(k) \simeq (2,2,2)$ and finite class field tower. There is, however, an analogue for $p = 4$ due to Koch [147] and Hajir [199]:

Proposition 1.9.18. *Let k be an imaginary quadratic number field. If $\operatorname{rank} \mathrm{Cl}_4(k) \geq 3$, then k has infinite 2-class field tower.*

The corresponding result for real quadratic number fields was obtained by Maire [209]:

Proposition 1.9.19. *Let k be a real quadratic number field. If $\operatorname{rank} \mathrm{Cl}_4(k) \geq 4$, then k has infinite 2-class field tower.*

For other refinements of (1.8) for certain Galois extensions of $\mathbb{Q}$, see [207], where e.g. the following result is proved using Thm. 1.9.15:

Proposition 1.9.20. *Let k be a cyclic cubic extension of $\mathbb{Q}$, and let $p \geq 5$ be a prime. If $\operatorname{rank} \mathrm{Cl}_p(k) \geq 4$, then k has infinite p-class field tower.*

Besides class field towers of quadratic number fields, those of cyclotomic number fields have been studied extensively. Sufficient criteria for the ℓ-class field of $\mathbb{Q}(\zeta_m)$ to be infinite have been given by Furuta [159], Cornell [173], and Schoof [179]. Wingberg [191] found that the p-class field tower of $k = \mathbb{Q}(\zeta_p)$ is infinite if $p \nmid h(k^+)$ and $\mathrm{Cl}_p(k)$ has rank ≥ 3, and he gave a sufficient criterium in the case $\operatorname{rank} \mathrm{Cl}_p(k) = 2$.

Often one can obtain better results by applying the inequality 1.9.13 not to the base field k but to one of its unramified extensions. Martinet [166], for example, observed the following

Proposition 1.9.21. *Let K/k be a cyclic extension of prime degree p; let t and u denote the number of finite and infinite primes of k ramifying in K/k. Moreover, let r denote the number of all inifinite primes of k and put $\delta_k = 1$ if $\zeta_p \in k$, and $\delta_k = 0$ otherwise. Then K has an infinite p-class field tower if*

$$t \;\geq\; r + \delta_k + 2 - u + 2\sqrt{p(r - u/2) + \delta_k}.$$

Another result in this direction was given by Schoof [179]:

Proposition 1.9.22. *Let K/k be a cyclic extension of prime degree p, and let ρ denote the number of finite and infinite primes ramifying in K/k. Then the p-class field tower of K is infinite if*

$$\rho \;\geq\; 3 + \mathrm{rank}_p E_k/H + 2\sqrt{\mathrm{rank}_p E_K + 1}.$$

Here H is the subgroup of E_k consisting of units which are norms of elements from K, and $\mathrm{rank}_p G$ denotes the $p-$rank of G/G^p.

These ideas were used by Martinet [166], Schmithals [170], and Schoof [179] to construct fields with infinite 2-class field tower and small discriminant. Note, however, that the construction of Matsumura [165] is incorrect: his error occurs in his proof of Lemma 4: he considers an unramified cyclic extension k/M of odd relative degree ℓ, a prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$, and a congruence $\varepsilon \equiv -1 \bmod \mathfrak{p}$. Then he takes the norm to M and concludes that $N\varepsilon \equiv N(-1) \bmod N(\mathfrak{p})$: but this is only allowed if $\mathfrak{p}$ is totally ramified in k/M. In fact, here is a counterexample to his Theorem 1: Take $p = 17$, $q = -23$, $\ell = 3$; his claim is that the compositum K of $\mathbb{Q}(\sqrt{-23}, \sqrt{17})$ and the cubic field of discriminant -23 has an ideal class group with subgroup $(2, 2)$. However, $\mathrm{Cl}(K) \simeq Z/7\mathbb{Z}$ by direct computation (see our Tables in the appendix, where the class field tower of $\mathbb{Q}(\sqrt{-17 \cdot 23}\,)$ is given).

This approach suggests the following question: suppose that k has an infinite p-class field tower. Does there exist a finite subextension $K \subset k_{(p)}^{\infty}$ such that K satisfies (1.8)? If this is true, then the p-ranks of the class groups in the p-class field tower should grow; in [198], Hajir showed that for fields satisfying (1.8) the p-ranks of the class groups in the tower tend to infinity:

Theorem 1.9.23. *For a number field and a prime p, put $d = \mathrm{rank}\,\mathrm{Cl}_p(k)$ and $r = d + \dim_p E_k/N_{K/k}E_K$; if $d^2 \geq 4r$, then*

(a) $\Gamma = \mathrm{Gal}\,(k_{(p)}^{\infty}/k)$ is a pro-p group which is not p-adic analytic;

(b) $\lim_{m\to\infty} \mathrm{rank}\,\mathrm{Cl}_p(k_{(p)}^{m}) = \infty$.

Part (a) contains the theorem of Golod and Shafarevic as a special case, since all finite p-groups are p-adic analytic. Weaker results in this direction have been obtained before by Furuta [159] and Shirai [164]. Hajir also established an upper bound on the p-ranks of class groups in the class field tower by improving slightly on an inequality due to Iwasawa:

Proposition 1.9.24. *Let K/k be an unramified p-extension. Then*

$$\mathrm{rank}\,\mathrm{Cl}_p(K) - 1 \leq (K : k)(\mathrm{rank}\,\mathrm{Cl}_p(k) - 1). \tag{1.11}$$

Hajir gave examples with n prime where we have equality in (1.11). The inequality can also be used to show that constructing infinite 2-class field towers of imaginary quadratic number fields k whose 2-class group have rank 2 is not too easy: if K/k is an unramified 2-extension such that K satisfies (1.8) then $(K : k) \geq 8$.

Fontaine and Mazur came forward with the following

Conjecture 1. *Let k be a number field and put $K = k_{(p)}^{\infty}$. If $(K : k)$ is infinite, then $\mathrm{Gal}\,(K/k)$ is a pro-p group which is not p-adic analytic.*

See Boston [185, 197], Hajir [198] and Nomura [200] for proofs of this conjecture in special cases. The arithmetic side of the conjecture says that the p-ranks of the class groups in the p-class field tower of k are bounded if and only if the p-class field tower terminates.

Another generalization of the theorem of Golod-Shafarevic is due to Maire [206]: Let S and T denote finite sets of primes of a number field k; a T-S-extension is an extension of number fields such that the primes in S split completely, and such that those in T are at most tamely ramified. He then develops criteria of Golod-Shafarevic-type for infinite T-S-towers. By putting $T = \varnothing$ and $S = \{\mathfrak{p} : \mathfrak{p} \mid \infty\}$ he is able to construct number fields with infinite 2-class field tower in the strict and finite 2-class field tower in the wide sense.

1.9.3 Odlyzko Bounds

Exploiting an idea of Stark [546, 547], Odlyzko [548, 551, 552, 553] proved lower bounds for discriminants which were considerably stronger than those obtained using geometry of numbers by Minkowski. Since this topic has been surveyed by Poitou [554] and Odlyzko [559], we will be very brief here.

Minkowski proved the following: if K is an algebraic number field of degree $n = r + 2s$, where r denotes the number of real and s the number of pairs of complex embeddings, then every ideal class of $\mathrm{Cl}(K)$ contains an integral ideal $\mathfrak{a}$ such that

$$N_{K/\mathbb{Q}}\mathfrak{a} \ < \ \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s\sqrt{d}, \quad \text{where } d = |\mathrm{disc}\, K|.$$

Since every integral ideal has norm ≥ 1, this implies

$$|\mathrm{disc}\, K| \geq \Big(\frac{\pi}{4}\Big)^{2s}\Big(\frac{n^n}{n!}\Big)^2.$$

If we introduce the root discriminant rd_K of K by $\mathrm{rd}_K = |\mathrm{disc}\, K|^{1/n}$ (it was called 'Differentenwert' by Scholz in [545]), then this implies that, asymptotically,

$$\mathrm{rd}_K \ > \ (7.3)^{r/n}(5.8)^{2s/n}.$$

Artin and Hasse cherished the dream that an improvement of the Minkowski bound might lead to a proof that $\mathrm{rd}_K \longmapsto \infty$ as $n \longmapsto \infty$; this would have settled the class field tower problem positively, i.e. it would imply that the class field tower of every number field eventually terminates.

Let d_n denote the root discriminant of the number field(s) of degree n with minimal discriminant; then Scholz noticed that the example $\mathbb{Q}(\sqrt[n]{2}\,)$ gave $d_n < 2n$. By constructing a family of metabelian extensions (which can be identified with subfields of Hilbert class fields of cyclotomic fields) he was able to show that $d_n < (\log n)^2$; he also showed that abelian extensions of $\mathbb{Q}$ satisfied $d_n \geq c\frac{n\log\log n}{\log n}$ for some constant $c > 0$.

Let us be a bit more precise; write $n = r + 2s$ and consider the set $\mathcal{K}$ of number fields K of degree divisible by n such that $r_K/r = s_K/s$, where $(K : \mathbb{Q}) = r_K + 2s_K$. Then we define $\alpha(r, s) = \liminf d_n^{1/n}$, where the lim inf is over all fields in $\mathcal{K}$. The results of Odlyzko show that

$$\begin{array}{lll} \alpha(r,s) & \geq & (22.3)^{2s/n}(60.8)^{r/n} \qquad \text{unconditionally, and} \\ \alpha(r,s) & \geq & (44.7)^{2s/n}(215.3)^{r/n} \qquad \text{assuming the truth of GRH.} \end{array}$$

Martinet [556] showed that the field $K = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1}, \sqrt{-46}\,)$ has an infinite 2-class field tower. This shows that $d_n \leq 92.3$ for all $n = 5 \cdot 2^m$, $m \geq 1$. Incidentally, we don't know an answer to the following

Question 1. *Is d_p bounded as $p \longmapsto \infty$, where p is prime?*

1.9.4 Galois groups of Class Field Towers

Let k denote a quadratic number field, and let $d = d_1 \ldots d_t$ be the factorization of $d = \mathrm{disc}\, k$ into prime discriminants; let $k^{(1,2)} = k^+_{\mathrm{gen}}$ denote the genus class field of k in the strict sense, and define $k^{(2,2)}$ to be the central class field of $k^{(1,2)}/\mathbb{Q}$. For prime discriminants d_j, write $d = d'd_j^\nu$ ($\nu \in \{0, 1\}$) and define the symbol $[d, d_j]$ by

$$(-1)^{[d,d_j]} = \Big(\frac{d'}{p}\Big),$$

where p is the unique prime dividing d_j.

For 2-groups Γ, define $\Gamma^{(1,2)} = \Gamma^2\Gamma'$, $\Gamma^{(2,2)} = \Gamma'^2[\Gamma, \Gamma']$ etc. Fröhlich (see [286] for a modern presentation of the original proof) showed

Theorem 1.9.25. *Let k be a quadratic number field, and let $d = d_1 \cdots d_n$ be the factorization of $d = \mathrm{disc}\, k$ into prime discriminants. Let Γ denote the Galois group of $k^\infty_{(2)}$ ($k^\infty_{(2)}$ being the union of all fields in the 2-class field tower of k). Then there is an exact sequence*

$$1 \longrightarrow R \longrightarrow F \longrightarrow \Gamma \longrightarrow 1,$$

where F/R is the pro-2-group with generators $s_1, \ldots, s_{n-1}$, and defining relations

$$\prod_{1\le j\le n, j\neq i}^{n} (s_1^2 s_j^2 [s_i, s_j])^{[q_1,q_j]} \in \Gamma^{(2,2)}.$$

As a corollary of Fröhlich's result, Koch [147] obtained

Theorem 1.9.26. *Let $K = k^{(2,2)}$; then the Galois group $\Gamma = \mathrm{Gal}\,(K/k)$ is generated by $t-1$ automorphisms $\sigma_1, \ldots, \sigma_{t-1}$ subject to the following relations:*

i) $\Gamma^{(2,2)} = 1$;

ii) $\prod_{\nu=1}^{t-1} (\sigma_\nu^2 [\sigma_\nu, \sigma_\mu])^{[d_\nu, d_\mu]} = \sigma_\mu^{2[d,d_\mu]}$ *for* $\mu = 1, 2, \ldots, t-1$;

iii) $\prod_{\nu=1}^{t-1} \sigma_\nu^{2[d_\nu, d_t]} = 1$.

From this theorem Koch derived the following corollary:

Proposition 1.9.27. *Let k be a quadratic number field such that $\mathrm{Cl}_2^+(k) \supseteq (4,4)$; then there exists an extension K/k of degree 32 which is unramified outside ∞ and with Galois group $\mathrm{Gal}\,(K/k) \simeq D_4 \curlywedge (4,4)$.*

An analogous result for p-class fields (p odd) was found by Nomura [101]:

Proposition 1.9.28. *Let k be a quadratic number field or a quadratic extension of an imaginary quadratic number field. Moreover, let p be an odd prime, and assume that $k \neq \mathbb{Q}(\sqrt{-3}\,)$ if $p = 3$. If $\mathrm{rank}\,\mathrm{Cl}_p(k) \ge 2$, then there exists an unramified normal extension K/k with Galois group $\mathrm{Gal}\,(K/k) \simeq H(p^3)$, where*

$$H(p^3) = \langle x, y : [x,y] = z, x^p = y^p = z^p = 1, [x,z] = [y,z] = 1 \rangle.$$

Nomura also proved a similar theorem for cyclic cubic ground fields:

Proposition 1.9.29. *Let k be as above, assume that p is an odd prime $\equiv -1 \bmod 3$, and let K/k be a cyclic cubic extension. If $p \mid h(K)$, then there exists an unramifed normal extension M/K with $\mathrm{Gal}\,(M/K) \simeq H(p^3)$.*

The corresponding result for $p = 2$ was proved by Bachoc and Kwon [527] and Couture and Derhem [460]:

Proposition 1.9.30. *Let k be a cyclic cubic number field, and suppose that $\mathrm{Cl}_2(k) \simeq (2,2)$. Then there exists a normal extension K/k with $\mathrm{Gal}\,(K/k) \simeq H_8$ which is unramified outside ∞.*

In 1993, Nomura [190] found the following generalization:

Proposition 1.9.31. *Let p and ℓ denote distinct odd primes, and let f denote the smallest integer ≥ 1 such that $p^f \equiv 1 \bmod \ell$. If f is even, and if K/k is a finite ℓ-extension of number fields such that $p \mid h(K)$, then p divides the class number of the Hilbert p-class field of K.*

The Galois groups of terminating 2-class field towers of quadratic number fields have been studied a lot in recent years (see [429], [460], [189], [463], [193], [215], [214], [202]). Some of the results obtained for imaginary quadratic base fields are collected in Theorem 1.9.32 and Table 1.

Theorem 1.9.32. *Let G be a 2-group such that G' is cyclic. Then G occurs as $\mathrm{Gal}\,(k^2/k)$ for an imaginary quadratic number field k only if G is one of the groups listed in Table 1.5. More exactly, $\mathrm{Gal}\,(k^2/k) \simeq G$ for these G if and only if $\mathrm{disc}\,k$ (and possibly some unit) satisfy the conditions $(*)$ in Table 1. As usual, p, p' denote primes $\equiv 1 \bmod 4$, q, q', q'' are primes $\equiv 3 \bmod 4$, ε_d denotes the fundamental unit of $\mathbb{Q}(\sqrt{d}\,)$, and $h_2(d)$ its 2-class number. In all cases we have $k^2 = k^3$.*

Table 1.5:

disc k	conditions	G	
d	$d<0$ prime	1	
dd'	$d<0$, $d'>0$ prime,	(2^m)	$2^m = h_2(k)$
$dd'd''$	$d,d',d''<0$ prime	$(2,2^m)$	$2^m = h_2(k)/2$
$-rpp'$	$(p/p')=(r/p)=(r/p')=-1$	H_8	
$-rpp'$	$(p/p')=1,(r/p)=(r/p')=-1$ $N\varepsilon_{pp'}=+1$	D_m, $m\geq 4$	$m = 2h_2(pp')$
$-rpp'$	$(p/p')=1,(r/p)=(r/p')=-1$, $N\varepsilon_{pp'}=-1$	H_m, $m\geq 16$	$m = 4h_2(pp')$
$-rpp'$	$(r/p)=+1$, $(p/p')=(r/p')=-1$		$m = 4h_2(-rp)$
$-4pp'$	$p\equiv 1$, $p'\equiv 5 \bmod 8$, $(p/p')=-1$	SD_m	$m = 4h_2(-4p)$
$-4pp'$	$p\equiv p'\equiv 5 \bmod 8, (p/p')=-1$	M_{4m}	$m = h_2(k)/2$
$-4pp'$	$p\equiv p'\equiv 5 \bmod 8, (p/p')=+1$ $N\varepsilon_{pp'}=-1$	MC_m^-	$2^m = h_2(pp')$
$-4pp'$	$p\equiv p'\equiv 5 \bmod 8, (p/p')=+1$, $N\varepsilon_{pp'}=+1$	$\mathrm{MC}_{m,t}^+$	$2^m = h_2(k)/2$ $2^t = h_2(pp')$
$-4pp'$	$p\equiv 1, p'\equiv 5 \bmod 8$, $(p/p')=+1, (p/p')_4(p'/p)_4=-1$	$\Gamma_{m,t}^1$	$2^m = h_2(k)/2$ $2^t = h_2(-4p)$
$-rpp'$	$(p/p')=(r/p)=1$, $(r/p')=(p/p')_4(p'/p)_4=-1$	$\Gamma_{m,t}^2$	$2^m = h_2(k)/2$ $2^t = h_2(-rp)$

Table 1.6:

group	presentation	order	$\#\mathfrak{M}(G)$
D_m	$\langle a,b : a^m=b^2=1,\ [a,b]=a^{-2}\rangle$	2m	2
H_{4m}	$\langle a,b : a^m=b^2=-1,\ [a,b]=a^{-2}\rangle$	4m	1
SD_{4m}	$\langle a,b : a^{2m}=b^2=1,\ [a,b]=a^{m-2}\rangle$	4m	1
M_{4m}	$\langle a,b : a^m=b^2=-1,\ [a,b]=-1\rangle$	4m	1
MC_m^-	$\langle a,b : b^{2^{m+1}}=1, a^4=b^{2^m},\ a^{-1}ba=b^{-1}\rangle$	2^{m+3}	1
$\mathrm{MC}_{m,t}^+$	$\langle a,b : a^{2^{t+1}}=b^{2^m}=1,\ b^{-1}ab=a^{-1}\rangle$	2^{m+t+1}	2
$\Gamma_{m,t}^1$	$\langle a,b : a^4=b^{2^m}=1,\ c=[a,b],$ $a^2=c^{2^{t-1}},\ [a,c]=c^2,\ [ab,c]=1\rangle$	2^{m+t+1}	2
$\Gamma_{m,t}^2$	$\langle a,b : a^4=b^{2^{m+1}}=1,\ c=[a,b],$ $a^2=b^{2^m}=c^{2^{t-1}},\ [a,c]=c^2,\ [ab,c]=1\rangle$	2^{m+t+1}	2

Table 1.7:

disc k	factors	$\mathrm{Cl}_2(k)$	disc k	factors	$\mathrm{Cl}_2(k)$
-1015	$-7\cdot 5\cdot 29$	$(2,8)$	-1780	$-4\cdot 5\cdot 89$	$(2,4)$
-1240	$-31\cdot 8\cdot 5$	$(2,4)$	-2035	$-11\cdot 5\cdot 37$	$(2,4)$
-1443	$-3\cdot 13\cdot 37$	$(2,4)$	-2067	$-3\cdot 13\cdot 53$	$(2,4)$
-1595	$-11\cdot 5\cdot 29$	$(2,8)$	-2072	$-7\cdot 8\cdot 37$	$(2,8)$
-1615	$-19\cdot 5\cdot 17$	$(2,4)$	-2296	$-7\cdot 8\cdot 41$	$(8,2)$
-1624	$-7\cdot 8\cdot 29$	$(2,8)$	-2379	$-3\cdot 13\cdot 61$	$(4,4)$

Table 1.8:

G	disc k	$\#G$	G	disc k	$\#G$
$(2,2)$	-84	4	M_{128}	-7076	128
$(2,4)$	-264	8	MC_2^-	-580	32
$(2,8)$	-399	16	$MC_{3,1}^+$	-1220	32
$(2,16)$	-1239	32	$MC_{2,2}^+$	-2020	32
$(2,32)$	-5271	64	$MC_{4,1}^+$	-2180	64
D_4	-408	8	$\Gamma_{2,2}^1$	-4820	32
D_8	-1515	16	$\Gamma_{2,3}^1$	-820	64
H_8	-120	8	$\Gamma_{3,2}^1$	-884	64
H_{16}	-195	16	$\Gamma_{3,3}^1$	-6068	128
H_{32}	-2712	32	$\Gamma_{4,2}^1$	-8980	128
H_{64}	-6915	64	$\Gamma_{2,2}^2$	-952	32
SD_{16}	-340	16	$\Gamma_{2,3}^2$	-915	64
SD_{32}	-2132	32	$\Gamma_{3,2}^2$	-663	64
SD_{64}	-5140	64	$\Gamma_{2,4}^2$	-4715	128
M_{16}	-260	16	$\Gamma_{3,3}^2$	-2296	128
M_{32}	-740	32	$\Gamma_{4,2}^2$	-5784	128

Table 1.9:

M_{16}	16.011	$\Gamma_2\, d$
M_{32}	32.022	$\Gamma_2\, k$
MC_2^-	32.032	$\Gamma_3\, f$
$MC_{3,1}^+$	32.021	$\Gamma_2\, j_2$
$MC_{2,2}^+$	32.029	$\Gamma_3\, d_1$
$MC_{4,1}^+$	64.041	$\Gamma_2\, w_2$

$\Gamma_{2,2}^1$	32.028	$\Gamma_3\, c_2$
$\Gamma_{3,2}^1$	64.063	$\Gamma_3\, n_2$
$\Gamma_{2,3}^1$	64.139	$\Gamma_8\, c_2$
$\Gamma_{2,2}^2$	32.031	$\Gamma_3\, e$
$\Gamma_{2,3}^2$	64.066	$\Gamma_8\, e$
$\Gamma_{3,2}^2$	64.142	$\Gamma_3\, p$

In Table 1.5, the symbols D, H, SD and M denote dihedral, quaternion, semidihedral and modular groups; presentations for the groups can be found in Table 1.6.

In Table 1.8 we give the smallest examples of imaginary quadratic fields and given group $\mathrm{Gal}\,(k^2/k)$; among the fields with $|\mathrm{disc}\, k| \le 2379$, Table 1.7 gives those which have noncyclic $\mathrm{Cl}_2(k^1)$.

The discriminants $2379 < |\mathrm{disc}\, k| < 8000$ such that $\mathrm{Cl}_2(k^1)$ is noncyclic are
-2392, -2715, -2755, -2788, -2840, -2847, -2915, -2968, -3160, -3335, -3435, -3560, -3604, -3783, -3939, -4251, -4495, -4823, -4895, -4964, -5015, -5135, -5235, -5335, -5336, -5555, -5576, -5795, -6040, -6052, -6104, -6123, -6215, -6307, -6328, -6355, -6392, -6596, -6747, -6771, -6935, -7059, -7208, -7503, -7511, -7512, -7527, -7535, -7544, -7579, -7640, -7672, -7684, -7960.

Finally, Table 1.9 gives isomorphisms between our groups and those in the tables of Senior and Hall.

1.9.5 Reflection Theorems

In this section we will deal with relations between the p-rank of ideal classes in certain number fields. The first result in this direction (which is a strengthening of Kummer's classical observation that $\ell \mid h^+$ implies $\ell \mid h^-$) is due to Hecke [304]:

Proposition 1.9.33. *Let ℓ be an odd prime, $k = \mathbb{Q}(\zeta_\ell)$, and let $\mathrm{Cl}_\ell^+(k)$ and $\mathrm{Cl}_\ell^-(k)$ denote the plus and the minus part of $\mathrm{Cl}_\ell(k)$. Then $\mathrm{rank}\,\mathrm{Cl}_\ell^+(k) \le \mathrm{rank}\,\mathrm{Cl}_\ell^-(k)$.*

Next Scholz [307] and Reichardt [310] discovered a connection between the 3-ranks of class groups of certain quadratic number fields:

Proposition 1.9.34. *Let $k^+ = \mathbb{Q}(\sqrt{m})$ be a real quadratic number field, and put $k^- = \mathbb{Q}(\sqrt{-3m})$. Then the 3-ranks r_3^+ and r_3^- of $\mathrm{Cl}(k^+)$ and $\mathrm{Cl}(k^-)$ satisfy the inequalities $r_3^+ \le r_3^- \le r_3^+ + 1$.*

Lepoldt later generalized this to p-ranks and called his result the "Spiegelungssatz", whence the title of this section.

Top [365] gave a lower bound for $r_3^+ + r_3^-$ in terms of the rank of a certain elliptic curve; Brinkhuis [357, 367] discovered connections between normal integral bases in cubic Hilbert class fields and the difference $r_3^+ - r_3^-$. A completely different proof of Prop. 1.9.34 using connections between 3-class groups of quadratic number fields and Selmer groups of elliptic curves based on ideas of Frey [330] was given by Nekovar [361]; see also Schaefer [371].

The fact that something analogous to Prop. 1.9.34 holds for the 4-rank of the ideal class groups of $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{-m})$ was not noticed until 1970, when Damey and Payan [317] proved

Proposition 1.9.35. *Let $k^+ = \mathbb{Q}(\sqrt{m})$ be a real quadratic number field, and put $k^- = \mathbb{Q}(\sqrt{-m})$. Then the 4-ranks r_4^+ and r_4^- of $\mathrm{Cl}^+(k^+)$ and $\mathrm{Cl}^+(k^-)$ (ideal class groups in the strict sense) satisfy the inequalities $r_4^+ \le r_4^- \le r_4^+ + 1$.*

Other proofs are due to Halter-Koch [353], Gras [323] and Uehara [360]; for a generalization, see Oriat [344].

Let k be a quadratic number field with discriminant d, and let r denote the 3-rank of its ideal class group. As we have already noted above, Hasse [10] used class field theory to show that there are exactly $\frac{1}{2}(3^r - 1)$ non-conjugate cubic number fields K with discriminant d, and that the extensions Kk/k give all the cubic subfields of the Hilbert class field k^1 of k. Callahan [325] discovered that the 3-ranks of k and K are related:

Proposition 1.9.36. *Let k be a quadratic number field with discriminant d, and suppose that its class number is divisible by 3. Let K be one of the cubic extensions of $\mathbb{Q}$ with discriminant d, and let r_2 and r_3 denote the 3-ranks of $\mathrm{Cl}(k)$ and $\mathrm{Cl}(K)$, respectively. Then $r_3 = r_2 - 1$.*

Callahan could only prove that $r_2 - 2 \le r_3 \le r_2 - 1$, but conjectured that in fact $r_3 = r_2 - 1$. This was verified later by G. Gras and Gerth [336]. Another proof is due to Bölling [352], who later [356] generalized this result to dihedral extensions of prime degree ℓ:

Proposition 1.9.37. *Let k be a quadratic number field with discriminant d, and suppose that its class number is divisible by an odd prime ℓ. Each unramified cyclic extension of degree ℓ over k is a dihedral extension of $\mathbb{Q}$; let K be one of its subfields, and let r_2 and r_ℓ denote the ℓ-ranks of $\mathrm{Cl}(k)$ and $\mathrm{Cl}(K)$, respectively. Then $r_2 - 1 \le r_\ell \le (r_2 - 1)\frac{\ell - 1}{2}$.*

A similar situation occurs for the 2-class groups of cyclic cubic fields k (Heilbronn [319]):

Proposition 1.9.38. *Let k be a cyclic cubic field with discriminant d, and let r denote the 2-rank of $\mathrm{Cl}(k)$; then $r \equiv 0 \bmod 2$ (cf. Inaba [232] or Gras [323]), and there exist exactly $\frac{1}{3}(2^r - 1)$ quartic fields K with discriminant d, and the extensions Kk/k give all unramified V_4-extensions which are normal over $\mathbb{Q}$. The normal closure N of $K/\mathbb{Q}$ has Galois group $\mathrm{Gal}\,(N/\mathbb{Q}) \simeq A_4$, the alternating group of order 12.*

The following pretty result on 3-ranks of certain pure cubic fields and their normal closure is due to Kobayashi [324] (see also Gerth [331]):

Proposition 1.9.39. *Let m be a cubefree integer not divisible by any prime $p \equiv 1 \bmod 3$, and put $k = \mathbb{Q}(\sqrt[3]{m})$ and $K = k(\sqrt{-3})$. Then $\mathrm{rank}\,\mathrm{Cl}_3(K) = 2 \cdot \mathrm{rank}\,\mathrm{Cl}_3(k)$.*

It was generalized subsequently by G. Gras [326] to

Proposition 1.9.40. *Let K be a normal extension of $\mathbb{Q}$ with $\mathrm{Gal}\,(K/\mathbb{Q}) \simeq S_3$, and let k denote its quadratic subfield. If no prime $p \in \mathrm{Spl}(k/\mathbb{Q})$ ramifies in K/k, and if $3 \nmid h(k)$, then $\mathrm{rank}\,\mathrm{Cl}_3(K) = 2 \cdot \mathrm{rank}\,\mathrm{Cl}_3(k)$.*

Two more elementary reflection theorems are

Proposition 1.9.41. *Let k be a totally real number field with odd class number. Let K/k and L/k be totally complex quadratic extensions, and assume that K/k is unramified outside ∞. Then* $\operatorname{rank}\mathrm{Cl}_2(K) \leq \operatorname{rank}\mathrm{Cl}_2(L)$.

Proof. Let H be the maximal unramified elementary abelian 2-extension of K; then $\operatorname{rank}\mathrm{Cl}_2(K) = (H : k)$. We claim that H/k is also an elementary abelian 2-extension. In order to see this, let E/K be a quadratic subfield of H/k; we have to show that $\mathrm{Gal}\,(E/k) \simeq (2,2)$. First we notice that E/k is normal: if not, let σ denote the non-trivial automorphism of K/k; then EE^σ is the normal closure of E/k, and we have $\mathrm{Gal}\,(EE^\sigma/k) \simeq D_4$, the dihedral group of order 8. Let K' be the quadratic subfield of EE^σ/k over which EE^σ is cyclic. Then K' must be totally complex (if not, there would be an infinite prime completely ramifying in EE^σ/K'), hence the third quadratic subfield K'' in EE^σ/k is totally real. Moreover, K'/k and K''/k are unramified at the finite primes (because EE^σ/k is), hence K''/k is a quadratic extension which is unramified everywhere. This contradicts the fact that the class number of k is odd.

Since there are only two groups of order 4, it is sufficient to show that E/k cannot be cyclic. But this is clear, because its quadratic subextension K/k is CM. □

Proposition 1.9.42. *Let k be a totally real number field with odd class number. Let K/k and L/k be totally complex quadratic extensions, and assume that there is exactly one prime ideal ramified in K/k. If there is at least one prime ideal ramified in L/k, then* $\operatorname{rank}\mathrm{Cl}_2(K) \leq \operatorname{rank}\mathrm{Cl}_2(L)$.

1.10 Unsolved Problems

Conjecture 2. *For every $n \geq 2$, there exist infinitely many primes $p \equiv 1 \bmod 4$ such that $\mathrm{Cl}_2(k) \simeq \mathbb{Z}/2^n\mathbb{Z}$, where $k = \mathbb{Q}(\sqrt{-p})$ is an imaginary quadratic number field with discriminant $-4p$.*

This can be proved for $n = 2$ and $n = 3$; moreover, the existence of governing fields in these cases shows that the primes $p \equiv 1 \bmod 4$ such that $h(-4p) \equiv 2^n \bmod 2^{n+1}$ have Dirichlet density 2^{-n-2}. Computational data suggest that this continues to hold for $n = 4, 5, \ldots$, but a proof seems out of reach.

I only recently noticed that the following 'conjecture' has already been proved by Bölling; nevertheless, the questions for general base fields are still open:

Conjecture 3. *Let k be a quadratic number field, and suppose that p is an odd prime such that $p \mid h(k)$. The unramified cyclic p-extensions L/k are normal with Galois group $\mathrm{Gal}\,(L/\mathbb{Q}) \simeq D_p$, the dihedral group of order $2p$. Let K be one of its subfields of degree p, and let r_2 and r_p denote the p-rank of $\mathrm{Cl}(k)$ and $\mathrm{Cl}(K)$, respectively. Then*

$$r_2 - 1 \leq r_p \leq \frac{p-1}{2}(r_2 - 1).$$

The proof of the upper bound is rather elementary, but the lower bound seems to be quite difficult to prove. Actually, the upper bound continues to hold if we replace $\mathbb{Q}$ by a field F with class number prime to p; the conjecture for the lower bound has to be replaced by $r_2 - 1 - e$, where e denotes the p-rank of $E_F/N_{K/F}E_K$, E_F and E_K being the unit groups of F and K, respectively. Of course we have $e = 0$ if the unit rank of F is 0, i.e. if $F = \mathbb{Q}$ or F is imaginary quadratic; this blends in nicely with the results of Nomura [101].

Question 2. *Given $n \in \mathbb{N}$ and a prime p, is there a quadratic number field whose p-class field tower terminates after exactly n steps?*

For $p = 2, 3$ there exist examples with $n \leq 2$.

Question 3. *Suppose that K/k is a nontrivial unramified p-extension such that $k \subseteq K \subsetneq k^1_{(p)} \subsetneq k^2_{(p)}$. Does $K^1_{(p)} = k^2_{(p)}$ imply that $k^2_{(p)} = k^3_{(p)} = \ldots = k^\infty_{(p)}$? Assume in addition that $(K : k) = p$; is it true that $K^1_{(p)} = k^2_{(p)}$ implies that $h_p(L) = h_p(k)$ for all $L \subset k^1_{(p)}$ with $K \neq L$ and $(L : k) = p$?*

Question 4. *Let k be a number field and assume that $k \subseteq K \subsetneq L \subset k_{(p)}^{\infty}$ (i.e. $K \subsetneq L$ are subextensions of the p-class field tower of k. Then is it true that $K_{(p)}^1 = L_{(p)}^1$ implies that $K_{(p)}^1 = k_{(p)}^{\infty}$?*

Herbrand's Theorem gives all elementary abelian unramified ℓ-extensions of $\mathbb{Q}(\zeta_\ell)$ in a very explicit way if $\ell \nmid h^+(\ell)$.

Question 5. *Is it possible to give a similar explicit description of the capitulation in these extensions? If it is, does Ribet's construction yield similar answers?*

The following conjecture is due to Martinet [166, 558]:

Conjecture 4. *If k is an imaginary quadratic field such that $\operatorname{rank} \mathrm{Cl}_2(k) \geq 4$ then k has infinite 2-class field tower.*

In a similar vein we ask

Question 6. *Do there exist imaginary quadratic number fields k with $\mathrm{Cl}_2(k) \simeq (4,4), (2,2,4)$ or $(2,4,4)$ and finite 2-class field tower?*

Question 7. *Let k be a number field with p-class field tower $k_{(p)}^1 \subseteq k_{(p)}^2 \subseteq \ldots$, and suppose that $\operatorname{rank} \mathrm{Cl}_p(k_{(p)}^n) \geq \operatorname{rank} \mathrm{Cl}_p(k_{(p)}^{n+1})$. Does this imply that the p-class field tower of k terminates?*

Question 8. *Let K/k be a finite extension of number fields. Are there any simple and nontrivial criteria for the inequality $\operatorname{rank} \mathrm{Cl}_p(K/k) \leq \operatorname{rank} \mathrm{Cl}_p(K)$ to be sharp?*

Question 9. *If k is a number field with odd class number, then the ambiguous class number formula gives the rank of $\mathrm{Cl}_2(K)$ for quadratic extensions K/k. What can be said if $h(k)$ is even? If, e.g., $\mathrm{Cl}_2(k) \simeq \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Am}(K/k) \simeq \mathbb{Z}/2\mathbb{Z}$, and if K/k is ramified, then it can be shown that*

$$\mathrm{Cl}_2(K) \simeq \begin{cases} \mathbb{Z}/2^n\mathbb{Z}\ (n \neq 2) & \text{or } (2,2) \text{ if } \kappa = 1; \\ \mathbb{Z}/2^n\mathbb{Z}\ (n \geq 1) & \text{if } \kappa \neq 1. \end{cases}$$

More general results would be welcome.

Kobayashi's result 1.9.39 begs the question what's happening for split primes. Numerical experiments with pure cubic fields suggest the following conjecture:

Conjecture 5. *Let $p \equiv 1 \bmod 3$ be a prime, and let $K = \mathbb{Q}(\sqrt[3]{p})$. Then $\mathrm{Cl}_3(K)$ is cyclic, and if it contains a cyclic subgroup of order 9 then $p \equiv 1 \bmod 9$.*

Let $L = K(\sqrt{-3})$ be the normal closure of K. If $p \equiv 4, 7 \bmod 9$, then

$$\mathrm{Cl}_3(L) \simeq \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{if} \quad (3/p)_3 \neq 1 \\ (\mathbb{Z}/3\mathbb{Z})^2 & \text{if} \quad (3/p)_3 = 1 \end{cases}$$

If $p \equiv 1 \bmod 9$, then $\operatorname{rank} \mathrm{Cl}_3(L) \in \{1, 2\}$, whether $(3/p)_3 = 1$ or not.

Question 10. *What can be said about the covering tree of $(2, 2^n)$?*

Chapter 2

The Construction of Hilbert ℓ-Class Fields

In this chapter we will refine and extend ideas of G. Gras [31, 37] concerning the construction of Hilbert class fields. We will also show how to derive special cases of Leopoldt's Spiegelungssatz from our results, and present connections with the structure of the ℓ-class group of $\mathbb{Q}(\zeta_\ell)$. Apart from [37], Oriat's papers [629] and [337] have been very helpful.

2.1 Decomposition into Eigenspaces

2.1.1 Idempotents

Although much of what follows actually holds in more general situations, we will assume in this section that k/F is an abelian extension such that the exponent of $G = \mathrm{Gal}\,(k/F)$ divides $\ell - 1$. This will allow us to view $\mathbb{F}_\ell$-characters of G as homomorphisms: in fact, let $\widehat{G} = \mathrm{Hom}\,(G, \mathbb{F}_\ell^\times)$; since $\exp G \mid \ell - 1$, we have $\widehat{G} \simeq G$. For every $\phi \in \widehat{G}$ define

$$e_\phi = \frac{1}{n} \sum_{\sigma \in G} \phi(\sigma^{-1})\sigma,$$

where $n = \#G$. We claim that the elements $e_\phi \in \mathbb{F}_\ell[G]$ form a complete set of central idempotents in the group ring $\mathbb{F}_\ell[G]$:

Proposition 2.1.1. *The elements e_ϕ have the following properties:*

$$1.\ \sum_{\phi \in \widehat{G}} e_\phi = 1; \qquad 2.\ e_\phi e_\psi = \begin{cases} 0 \text{ if } \phi \neq \psi; \\ e_\phi \text{ if } \phi = \psi; \end{cases} \qquad 3.\ \sigma e_\phi = \phi(\sigma) e_\phi.$$

Proof. This is proved by straightforward verification:

1. $$\sum_{\phi \in \widehat{G}} e_\phi = \frac{1}{n} \sum_{\phi \in \widehat{G}} \sum_{\sigma \in G} \phi(\sigma^{-1})\sigma = \frac{1}{n} \sum_{\sigma \in G} \sigma \sum_{\phi \in \widehat{G}} \phi(\sigma^{-1}) = 1,$$

   where we have used the well known property $\sum_{\phi \in \widehat{G}} \phi(\sigma^{-1}) = \begin{cases} n, \text{ if } \sigma = 1, \\ 0, \text{ if } \sigma \neq 1. \end{cases}$.

2. $$e_\phi e_\psi = \Big(\frac{1}{n} \sum_{\sigma \in G} \phi(\sigma^{-1})\sigma\Big)\Big(\frac{1}{n} \sum_{\tau \in G} \psi(\tau^{-1})\tau\Big).$$

Reorganizing the sum and substituting $\sigma = \rho\tau^{-1}$ yields

$$e_\phi e_\psi = \frac{1}{n^2}\sum_\rho \phi(\rho^{-1})\rho\sum_\tau(\psi^{-1}\phi)(\tau) = \frac{1}{n}e_\phi\sum_\tau(\psi^{-1}\phi)(\tau).$$

This last sum, however, vanishes whenever $\phi \neq \psi$, and equals n if $\phi = \psi$. This proves our claim.

3.
$$\sigma e_\phi = \frac{1}{n}\sum_\tau \phi(\tau^{-1})\sigma\tau = \phi(\sigma)\frac{1}{n}\sum_\tau \phi((\sigma\tau)^{-1})\sigma\tau = \phi(\sigma)e_\phi.$$

□

This implies that every $\mathbb{F}_\ell[G]$-module A can be written as a direct sum of submodules $A(\phi) = A^{e_\phi}$: in fact, the relation $A = A^{\sum e_\phi}$ shows that the $A(\phi)$ generate A, and the orthogonality of the idempotents implies at once that the sum

$$A = \bigoplus_{\phi\in\widehat{G}} A(\phi)$$

is direct. Since $\sigma e_\phi = \phi(\sigma)e_\phi$, we conclude that $A(\phi) = \{a \in A : \sigma(a) = a^{\phi(\sigma)} \text{ for all } \sigma \in G\}$. If we put $A(\phi)^\perp = \bigoplus_{\psi\neq\phi} A(\psi)$, then clearly $a \in A(\phi)^\perp \iff a^{e_\phi} = 1$.

If G is cyclic, then all $\phi \in \widehat{G}$ are powers of the character ϕ_1 defined by mapping a generator of G to a primitive n^{th} root mod ℓ (recall that $n \mid \ell - 1$), which we will denote by r. In this case we often write $A_i = A(\phi_1^i)$.

2.1.2 Contribution of Subspaces

Next we will study the base change, i.e. we replace F by some extension L contained in k/F. To this end, let U be the subgroup of G which corresponds to L by Galois theory, and let $\pi : G \longrightarrow G/U$ denote the canonical projection (our groups are abelian). If ψ is a character of G/U, then $\phi = \psi \circ \pi$ is a character of G such that $G_\phi \supseteq U$. It is easy to see that in this way we get a bijection between the characters of G/U and the characters of G whose kernels contain U. Extending this map linearly we get a map $\pi : \mathbb{F}_\ell[G] \longrightarrow \mathbb{F}_\ell[G/U]$. It is easily verfied that $\pi(e_\phi) = e_{\pi(\phi)}$.

Now put $A = \mathcal{E}_k = E(k)/E(k)^\ell$, and assume that $\phi \in \widehat{G}$ has kernel G_ϕ; let L be the fixed field of G_ϕ. Then the subset of all elements of $A(\phi)$ which are invariant under $U = \mathrm{Gal}\,(k/L)$ form a submodule which can be identified with $E_L(\psi)$, where $E_L = E(L)/E(L)^\ell$ and where $\psi \circ \pi = \phi$.

In our applications, A will often be a subgroup of $k^\times$. Of course we want to know whether a certain part $A(\phi)$ of A can be computed from the arithmetic of a subextension of k/F. To this end put $G_\phi = \ker\phi = \{\sigma \in G : \phi(\sigma) = 1\}$ and let k_ϕ be the subfield of k fixed by G_ϕ. We can define a 'relative norm' on A by $N_\phi : A \longrightarrow A : a \longmapsto \prod_{\sigma\in G_\phi} a^\sigma$. Clearly N_ϕ induces an isomorphism on $A(\phi)$. If, for example, we take $A = E(k)$ (the unit group of k), then $E(\phi)$ is generated by units of k_ϕ (which is a nontrivial observation only if $G_\phi \neq 1$). Similarly, let $A = C(k)$, the group of ideal classes of k whose order divides ℓ: then $C(\phi)$ is generated by ideal classes of k_ϕ (Observe that we may identify $\mathrm{Cl}_\ell(k_\phi)$ with its image in $\mathrm{Cl}_\ell(k)$ since the relative degree $(k : F)$ is not divisible by ℓ).

2.1.3 Hilbert's Satz 90

We will also need 'Hilbert's Satz 90':

Proposition 2.1.2. *Let A be an $\mathbb{F}_\ell[G]$-module and suppose that $G = \langle\sigma\rangle$ is cyclic of order $n \mid \ell - 1$. Then $a^{e_j} = 1$ if and only if $a = b^{\sigma - r^j}$ for some $b \in A$.*

Proof. Put $F_i(X) = \frac{1}{n}\sum_{\nu=0}^{n-1} r^{-\nu i}X^\nu \in \mathbb{F}_\ell[X]$; then clearly $F_i(\sigma) = e_i$. Since

$$F_i(r^j) = \frac{1}{n}\sum_{\nu=0}^{n-1} r^{-\nu i}r^{\nu j} = \frac{1}{n}\sum_{\nu=0}^{n-1} r^{\nu(j-i)} = \delta_{ij},$$

we conclude that $F_i(X)$ is a constant times the product over all $(X - r^j)$ for $j \neq i$; evaluating the coefficient of the highest term yields in fact that

$$F_i(X) = \frac{1}{n} r^i \prod_{j \neq i} (X - r^j),$$

though this will not be needed in the sequel.

Now assume that $a^{e_i} = 1$; then $a = \prod_{i \neq j} a^{e_j}$. Since the $e_j = F_j(\sigma)$ have a common factor $\sigma - r^i$, we can write $e_j = (\sigma - r^i) f_j$, and we find

$$a = \prod_{i \neq j} a^{e_j} = \Big(\prod_{i \neq j} a^{f_j} \Big)^{\sigma - r^i}.$$

The other direction is trivial, hence our claim follows. □

Observe that e_0 is essentially the norm, and that Prop. 2.1.2 shows that the norm of a is trivial iff $a = b^{\sigma - 1}$. In fact, even E. Noether's generalization of Hilbert 90 holds:

Theorem 2.1.3. *Let $\delta : G \longrightarrow A$ be a map of a finite group G into a $\mathbb{Z}_\ell[G]$-module A. Suppose that $\ell \nmid n$, where $n = \#G$ denotes the order of G, and assume that δ satisfies the Noether equations $\delta(\sigma\tau) = \delta(\sigma)^\tau \delta(\tau)^{\phi(\sigma)}$ for all $\sigma, \tau \in G$. Then there exists an $a \in A$ such that $\delta(\sigma) = a^{\sigma - \phi(\sigma)}$.*

Proof. Define $b = \prod_{\sigma \in G} \delta(\sigma)^{-\phi(\sigma)^{-1}}$. Then

$$\begin{aligned} b^\tau &= \prod_{\sigma \in G} \big(\delta(\sigma)^\tau\big)^{-\phi(\sigma)^{-1}} = \prod_{\sigma \in G} \big(\delta(\sigma\tau)\delta(\tau)^{-\phi(\sigma)}\big)^{-\phi(\sigma)^{-1}} \\ &= \delta(\tau)^n \Big(\prod_{\sigma \in G} \delta(\sigma\tau)^{-\phi(\sigma\tau)^{-1}} \Big)^{\phi(\tau)} = \delta(\tau)^n b^{\phi(\tau)}. \end{aligned}$$

Let f be the multiplicative inverse of n in $\mathbb{Z}_\ell$; then $a = b^f$ has the desired properties. □

Hilbert's Satz 90 is of course contained as a special case in Thm. 2.1.3: in fact, every $\mathbb{F}_\ell[G]$-module is a $\mathbb{Z}_\ell[G]$-module via the canonical projection $\mathbb{Z}_\ell \longrightarrow \mathbb{Z}_\ell / \ell\mathbb{Z}_\ell \simeq \mathbb{F}_\ell$. Now assume that $a \in A_\phi^\perp$ and define a map $\delta : G \longrightarrow A$ by $\delta(1) = 1$ and

$$\delta(\sigma^{i+1}) = a^{S(i)} \text{ for } i \geq 0, \text{ where } S(i) = \sum_{j=0}^{i} \sigma^{i-j} \phi(\sigma)^j.$$

This is well defined because $\delta(\sigma^n)$ is an element of $A_\phi^\perp$ (since a is) which is killed by $\sigma - \phi(\sigma)$, i.e. $\delta(\sigma^n) \in A_\phi^\perp \cap A_\phi = 1$. Moreover δ satisfies the Noether equations $\delta(\sigma\tau) = \delta(\sigma)^\tau \delta(\tau)^{\phi(\sigma)}$, hence Thm. 2.1.3 shows that there exists an element $b \in A$ such that $a = \delta(\sigma) = b^{\sigma - \phi(\sigma)}$.

2.2 Kummer Theory

2.2.1 The Kummer Pairing

We start by reviewing Kummer Theory. Let $K/k/F$ be a tower of extensions with the following properties:

1. k/F is normal with finite Galois group $G = \mathrm{Gal}\,(k/F)$;
2. K/k is abelian of exponent m;
3. k contains a primitive m^{th} root of unity ζ.

In this situation, Kummer theory gives a bijection between normal extensions K/k of exponent m and subgroups $W = W_K = \{\alpha \in k^\times : \alpha^{1/m} \in K\}$. We can make $\mathrm{Gal}\,(K/k)$ act on the elements $\omega = \alpha k^{\times m} \in W/k^{\times m}$ by putting $\beta = \alpha^{1/m}$ and observing that, for any $\tau \in \mathrm{Gal}\,(K/k)$, we have $\tau(\beta)^m = \tau(\alpha) = \alpha = \beta^m$; this implies that $\beta^{\tau-1} \in \mu_m$, where $\mu_m = \langle\zeta\rangle$ is the group of m^{th} roots of unity, and we end up with a (well defined(!)) map $W/k^{\times m} \times \mathrm{Gal}\,(K/k) \longrightarrow \mu_m : \ \langle\omega, \tau\rangle \longmapsto \beta^{\tau-1}$. We claim that this is a pairing, i.e. that the map is $\mathbb{Z}$-bilinear. In fact, we find

$$\begin{aligned} \langle\omega^a, \tau\rangle &= (\beta^a)^{\tau-1} = (\beta^{\tau-1})^a \quad \text{and} \\ \langle\omega, \tau^a\rangle &= \beta^{\tau^a-1} = (\beta^{\tau-1})^{1+\tau+\ldots+\tau^{a-1}} = (\beta^{\tau-1})^a. \end{aligned}$$

Moreover, this pairing is perfect, i.e. the left and right kernels are trivial.

Next we observe that $G = \mathrm{Gal}\,(k/F)$ acts on μ_m; it also acts naturally on $W/k^{\times m}$ but we have to make sure that $\langle\omega^\sigma, \tau\rangle$ still makes sense: this is done by putting $\langle\omega^\sigma, \tau\rangle = (\beta^s)^{\tau-1}$, where s is an extension of σ to K/F. Since different choices of s will change β^s by at most a root of unity (which is killed by $\tau - 1$), this is indeed well defined. If we make $\mathrm{Gal}\,(K/k)$ into a G-module by defining $\tau^\sigma = s^{-1}\tau s$ (check that this is well defined), then the actions on the three groups in our pairing are compatible:

$$\langle\omega^\sigma, \tau^\sigma\rangle = (\beta^s)^{\tau^\sigma - 1} = (\beta^s)^{s^{-1}\tau s}/\beta^s = \beta^{\tau s}/\beta^s = (\beta^{\tau-1})^\sigma = \langle\omega, \tau\rangle^\sigma.$$

Clearly K/F is normal if and only if G acts on $W/k^{\times m}$. In the special case where $W/k^{\times m} = \langle\omega\rangle$ is cyclic we see that K/F is normal if and only if $\omega^\sigma = \omega^{\phi(\sigma)}$ for some $\phi(\sigma) \in (\mathbb{Z}/m\mathbb{Z})^\times$. The map $\phi : G \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ is easily seen to be a homomorphism, i.e. an element of $\widehat{G}$. There is a second character $G \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ connected with the action of G on k/F, namely the cyclotomic character χ defined by $\zeta^\sigma = \zeta^{\chi(\sigma)}$.

Now assume that $K = k(\sqrt[m]{\omega})$ is normal over F; we want to compute $\sigma^{-1}\tau\sigma$ (note that this actually stands for $s^{-1}\tau s$, where s is any extension of σ to $\mathrm{Gal}\,(K/F)$). We find

$$\langle\omega^\sigma, \tau^\sigma\rangle = (\beta^{\tau-1})^{\chi(\sigma)} = \langle\omega^{\chi(\sigma)}, \tau\rangle = \langle\omega, \tau\rangle^{\chi(\sigma)}, \quad \text{as well as } \ \langle\omega^\sigma, \tau^\sigma\rangle = \langle\omega^{\phi(\sigma)}, \tau^\sigma\rangle = \langle\omega, \tau^\sigma\rangle^{\phi(\sigma)}.$$

Therefore

$$\langle\omega, \tau^\sigma\rangle = \langle\omega, \tau\rangle^{\chi(\sigma)\phi(\sigma)^{-1}} = \langle\omega, \tau^{\chi(\sigma)\phi(\sigma)^{-1}}\rangle,$$

from which we conclude that $\sigma^{-1}\tau\sigma = \tau^{\chi(\sigma)\phi(\sigma)^{-1}}$. We have proved

Proposition 2.2.1. *Let k/F be a normal extension such that k contains the m^{th} roots of unity, and let $K = k(\sqrt[m]{\alpha})$ be an extension of degree m. Then K/F is normal if and only if there exists a character $\phi : \mathrm{Gal}\,(k/F) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ such that $\omega^\sigma = \omega^{\phi(\sigma)}$ for every $\omega = \alpha k^{\times m}$. In this case, we have $\sigma^{-1}\tau\sigma = \tau^{\chi(\sigma)\phi(\sigma)^{-1}}$ for all $\sigma \in \mathrm{Gal}\,(k/F)$ and all $\tau \in \mathrm{Gal}\,(K/k)$, where χ is the cyclotomic character. Thus $K/k/F$ is central if and only if $\phi = \chi$. If, in particular, k/F is cyclic, then K/F is abelian if and only if $r = 1$ (i.e. $k = F$) or $\phi = \chi$.*

2.2.2 Eigenspaces of the Kummer Radical

Now suppose that K/F is normal, i.e. that G acts on $W/k^{\times m}$. If we pick any $\omega \in W$ then $k(\sqrt[m]{\omega})/F$ need not be normal. The problem we want to discuss is the following: can we choose some $\omega_j \in W$ in such a way that

a) the ω_j are independent in $W/k^{\times m}$;

b) K is the compositum of the $k_j = k(\sqrt[m]{\omega_j})$;

c) each k_j is normal over F.

We will see that the answer is yes and that we can even compute the Galois groups of the extensions k_j/F.

Decomposing the G-module $W/k^{\times m}$ into eigenspaces yields

$$W/k^{\times m} = \bigoplus_{\phi \in \widehat{G}} W(\phi)/k^{\times m}.$$

Then $\omega \in W(\phi)/k^{\times m}$ satisfies $\omega^\sigma = \omega^{\phi(\sigma)}$. By Prop. 2.2.1 this implies that $k(\sqrt[m]{\omega})/F$ is normal. Moreover, we get

$$\sigma^{-1}\tau\sigma = \tau^{\chi(\sigma)\phi(\sigma)^{-1}}.$$

Since any extension $1 \longrightarrow N \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$ of finite groups splits if $\#N$ and $\#G = (\Gamma : N)$ are coprime, we can choose extensions of the $\sigma \in G$ so that they form a subgroup of Γ isomorphic to G. This proves

Proposition 2.2.2. *Suppose that $G = S_1 \times \ldots \times S_q$ is a direct product of cyclic groups $S_i = \langle\sigma_i\rangle$, and assume that $n_i = \#S_i \mid \ell - 1$. Then, for any $\omega \in W(\phi)/k^{\times m}$, the extension $L = k(\sqrt[m]{\omega})$ is normal over F with Galois group*

$$\Gamma \simeq \langle\sigma_1, \ldots, \sigma_q, \tau : \sigma_i^{n_i} = \tau^m = 1, [\sigma_i, \sigma_j] = 1, \sigma_i^{-1}\tau\sigma_i = \tau^a \quad \text{for } a = \chi(\sigma_i)\phi(\sigma_i)^{-1}\rangle.$$

In particular, Γ is abelian if and only if $\chi = \phi$.

This shows that the submodule $W(\chi)$ of W is the interesting one when it comes to constructing class fields, for example. Therefore we would like to have a nice interpretation of $W(\chi)$; our next result shows that $W(\chi)$ does not come from the contributions of the subextensions of k/F if $k = F' = F(\zeta_\ell)$. This means essentially that the information needed for the construction of class fields is not contained in the subextensions of k/F.

In fact, let A be a G-module, and define $A(F'/L)$ for every subextension L of F'/F as the kernel of the norm map $N_{F'/L} : A \longrightarrow A : a \longmapsto \prod \sigma(a)$, where the product is over all $\sigma \in G$ fixing L elementwise.

Proposition 2.2.3. *Using the notation we have just introduced we have*

$$A_1 \subseteq \bigcap_{F \subseteq L \subsetneq F'} A_\ell(F'/L).$$

Proof. Let r be a primitive n^{th} root mod p and let σ denote the generating automorphism $\zeta_p \longrightarrow \zeta_p^r$ of F'/F. We know that $A_1 = \{a \in A_\ell : a^\sigma = a^r\}$. Let L be a subfield of F'/F and put $f = (L : F)$, $g = (F' : L)$. Then L is the fixed field of σ_r^f. Put $t \equiv r^f \bmod \ell$; then $N_{F'/L}a = a^S$ for $S = 1 + t + t^2 + \ldots + t^{g-1}$, and from $tS \equiv S \bmod \ell$ we deduce that $\ell \mid S$ (since $t = 1$ would imply $L = F'$). This gives $N_{F'/L}a = 1$, i.e. $a \in A_\ell(F'/L)$. □

2.3 Construction of ℓ-Class Fields

Let F be a number field which does not contain the ℓ^{th} roots of unity. In order to construct the ℓ-class field of F by Kummer theory we first adjoin ζ_ℓ, i.e. we put $F' = F(\zeta_\ell)$. As in Chap. 1 we choose a basis $\eta_0 = \zeta_\ell, \eta_1, \ldots, \eta_\lambda$ of $E_{F'}/E_{F'}^\ell$, then find generators $\mathfrak{b}_1, \ldots, \mathfrak{b}_f$ of ${}_\ell\mathrm{Cl}(F')$ and set $\mathfrak{b}_j^\ell = \beta_j\mathcal{O}_{F'}$. Finally we form the group

$$\mathfrak{E} = \langle\eta_0, \ldots, \eta_\lambda, \beta_1, \ldots, \beta_f\rangle F'^\ell \subseteq F'^\times/F'^{\times\ell}.$$

We know that the unramified cyclic extensions $L' = F'(\sqrt[\ell]{\omega})$ of F' are generated by the primary elements $\omega \in \mathfrak{E}$. Nevertheless just searching for primary elements in $\mathfrak{E}$ is a bad idea for several reasons: first of all, because there is a better method, and second, because we eventually want to apply our method to the construction of ray class fields, where we may *want* ramification at ℓ.

So we would like to make the group $\mathfrak{E}$ as small as possible before searching for primary numbers in it; one way to do this is to exclude some $\omega \in \mathfrak{E}$ which cannot give abelian extensions over F. For example, it is clear that any $\omega \in \mathfrak{E} \cap F^\times/F'^{\times\ell}$ satisfies $\omega^\sigma = \omega$, and therefore $F'(\sqrt[\ell]{\omega})/F$ is not abelian (cf. Prop. 2.2.1). Our aim is therefore to try to eliminate the subgroup of $\mathfrak{E}$ "coming from F". This is of course achieved by decomposing $\mathfrak{E}$ into eigenspaces. Since F'/F is cyclic, we use the notation $A_j = A(\phi^j)$, where ϕ is some fixed generator of $\widehat{G}$.

First we consider the unit group $E(F')$ or, more exactly, its image $\mathcal{E}$ in the factor group $F'^\times/F'^{\times\ell}$. Note that $\mathcal{E} = E(F')F'^{\times\ell}/F'^{\times\ell} \simeq E(F')/E(F')^\ell$. This yields

$$\mathcal{E} = \bigoplus_{i=0}^{n-1}\mathcal{E}_i \;\simeq\; E(F)/E(F')^\ell \oplus \bigoplus_{i=1}^{n-1}\mathcal{E}_i \quad \text{and} \quad \mathcal{E}(F'/F) = \bigoplus_{i=1}^{n-1}\mathcal{E}_i.$$

Next we decompose the subgroup $C = {}_\ell\mathrm{Cl}(F')$ of ideal classes of order dividing ℓ; clearly we have $C = \bigoplus C_i$ (with $C_i = C^{e_i}$). Now $ne_0 = \sum_a \sigma_a^{-1} = \sum_a \sigma_a$ is the algebraic norm; since $((F' : F), \ell) = 1$, the norm $N_{F'/F} : \mathrm{Cl}_\ell(F') \longrightarrow \mathrm{Cl}_\ell(F)$ is surjective and the conorm $j : \mathrm{Cl}_\ell(F) \longrightarrow \mathrm{Cl}_\ell(F')$ is injective on the ℓ-class group, hence we can identify C_0 and ${}_\ell\mathrm{Cl}(F)$. This means that we have

$$C = {}_\ell\mathrm{Cl}(F') \simeq {}_\ell\mathrm{Cl}(F) \oplus \bigoplus_{i=1}^{n-1} C_i \quad \text{and} \quad {}_\ell\mathrm{Cl}(F'/F) \simeq \bigoplus_{i=1}^{n-1} C_i.$$

Now we can give the "correct" definition of $\mathfrak{E} \subseteq {F'}^\times/{F'}^{\times\ell}$: for an ideal class $c \in C_i$, choose an integral ideal $\mathfrak{a}$ prime to ℓ such that $c = [\mathfrak{a}]$. Then $\mathfrak{a}^\ell = (\alpha)$ for some $\alpha \in \mathcal{O}_{F'}$, and $\mathfrak{a}^\sigma = \xi\mathfrak{a}^{r^i}$ for some $\xi \in F'$. This implies that $(\alpha)^\sigma = (\alpha)^r\xi^\ell$, hence there exists a unit $\varepsilon \in E(F')$ such that $\alpha^{\sigma - r^i} = \varepsilon\xi^\ell$ (note that we do not need to know $E(F')$ here). Applying e_i to this equation we get $\varepsilon^{e_i} \in E(F')^\ell$, and Hilbert 90 gives us a unit $\eta \in E(F')$ such that $\varepsilon \in \eta^{\sigma - r^i}E(F')^\ell$. Therefore that $\beta = \alpha\eta^{-1}$ generates the ideal $\mathfrak{a}^\ell$ and satisfies $\beta^{\sigma - r^i} \in {F'}^{\times\ell}$.

This shows the following: suppose we have an ideal class $c = [\mathfrak{a}] \in C_i$. Then we may choose a generator β of $\mathfrak{a}^\ell$ in such a way that $\beta \in F_i'$. If we do this for a set of ideal classes generating $C = \bigoplus C_i$ then we get a subgroup $\mathcal{C} = \bigoplus \mathcal{C}_i$ of ${F'}^\times/{F'}^{\times\ell}$, with the additional property that $C_i \simeq \mathcal{C}_i$. Put $\mathfrak{E} = \mathcal{E} \oplus \mathcal{C}$; then $\mathfrak{E}$ is also an $\mathbb{F}_\ell[G]$-module, hence

$$\mathfrak{E} = \bigoplus_{i=0}^{n-1} \mathfrak{E}_i,$$

and it is clear that an extension $F'(\sqrt[\ell]{\omega})$ is abelian over F if and only if $\omega \in \mathfrak{E}_1$ (again see Prop. 2.2.1). From what we have just proved we deduce that $\operatorname{rank}\mathfrak{E}_i = \operatorname{rank}\mathcal{E}_i + \operatorname{rank}\mathcal{C}_i$; in fact we have $\mathfrak{E}_i \simeq \mathcal{E}_i \oplus \mathcal{C}_i$ for every $0 \leq i \leq n-1$.

We therefore propose the following algorithm for constructing the Hilbert ℓ-class field of a number field k:

1. adjoin the ℓ^{th} roots of unity to form $k' = k(\zeta_\ell)$;
2. compute the subgroup $E(\chi)$ of an ℓ-maximal unit group;
3. compute the subgroup $C(\chi)$ of the ℓ-class group of k';
4. form $\mathfrak{E}(\chi)$ and compute $\widetilde{\mathfrak{E}}(\chi)$;
5. use the formulas given by Gras [31] and Odai [89] to compute generating polynomials for the unramified cyclic ℓ-extensions of k.

Remark 2. *For the construction of a unit η such that $\varepsilon = \eta^{\sigma - r^i}$ we do not need to know $E(F')$.*

Remark 3. *For an efficient method to compute $\widetilde{\mathfrak{E}}_i$ from $\mathfrak{E}_i$, see [29].*

Remark 4. *It is possible to compute $\mathcal{C}_1$ without having to compute the whole class group of F': let $\mathfrak{P}$ be a prime ideal in F' such that $c = [\mathfrak{P}] \in C_1$. Then the prime ideal $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$ below $\mathfrak{P}$ splits completely in F'/F (otherwise c would be in the oldclass group (i.e. the one coming from the decomposition field)). Moreover, the order of $\mathfrak{P}$ in $\mathrm{Cl}_\ell(F')$ is ℓ, and $\mathfrak{P}^{\sigma - r} \sim 1$ in $\mathrm{Cl}_\ell(F')$. Thus, $\mathcal{C}_1$ is generated by all prime ideals $\mathfrak{P}$ whose norm is below, say, the Minkowski bounds and who enjoy the properties listed above.*

Remark 5. *One should examine the current algorithms for computing units of algebraic number fields and try to modify them in such a way that they give $E(\chi)$ without having to compute all of $E = E(K)/E(K)^\ell$.*

Example 2.3.1. *Suppose that K is a cubic number field with class number divisible by $\ell = 3$. If K is totally real, then $E_1 = \langle\zeta_\ell\rangle$, since here K is the maximal real subfield of K', and we know that Hasse's unit index $q(K) = (E_{K'} : W_{K'}E_K)$ divides 2, i.e. $W_{K'}E_K$ is a 3-maximal subgroup of the unit group of K' (this shows incidentally that the construction of the cubic unramified extension is more difficult for complex cubic fields).*

In the special case where $C_1 = \mathrm{Cl}_3(K'/K)$ is trivial we can conclude that the Hilbert 3-class field of K' must be $K'(\sqrt[3]{\zeta_3})$, and therefore that the Hilbert 3-class field of K is simply KL, where L is the cubic field of discriminant 81 (i.e. the cubic subfield of $\mathbb{Q}(\zeta_9)$).

In [119], the authors compute the Hilbert class field for all 267 real cubic fields with discriminant < 100.000 and class number 3 and write that for 49 of these fields it is sufficient to consider Kummer extensions generated by units of K'. This shows that for these fields the Hilbert class field coincides with the genus class field. A search for real cubic fields with discriminant < 100.000 and nontrivial genus class field revealed that there are at least 195 such fields (I didn't check conductors > 127); except for six fields with class number 6, all of them have class number 3. In particular, for 189 of the 267 fields examined in [119] the Hilbert class field coincides with the genus class field.

Checking whether a cubic field K possesses a nontrivial genus class field is easy:

Proposition 2.3.1. *Let K be a cubic number field with discriminant $d = \operatorname{disc} K$ and assume that $f \equiv 1 \bmod 3$ is prime. Then the compositum of K and the cyclic cubic field k_f of conductor f is unramified over K if and only if $f^2 \mid d$.*

Proof. Assume that $f^2 \mid \operatorname{disc} K$. Then f ramifies completely in $K/\mathbb{Q}$. This in turn implies that f ramifies in $K(\sqrt{d})/\mathbb{Q}(\sqrt{d})$, and since this extension is cyclic (in fact, $N = K(\sqrt{d})$ is the normal closure of $K/\mathbb{Q}$), it ramifies completely. If the prime ideals above f would ramify in $k_f N/N$, they would be ramified completely in $k_f N/\mathbb{Q}(\sqrt{d})$. But this extension is bicyclic of degree 9, and only prime ideals above 3 can ramify completely in such extensions (this is due to the fact that the factor group V_0/V_1 of the ramification subgroups is cyclic). Therefore, $k_f N/N$ is unramified, and since $k_f N/K$ is abelian (it is cyclic of degree 6), $k_f K/K$ must be unramified as well.

On the other hand, if $k_f K/K$ is unramified, then applying the formula for the discriminants of towers to $k_f K/K/\mathbb{Q}$ yields $\operatorname{disc} k_f K = d^3$; applying it to $k_f K/k_f/\mathbb{Q}$ we find that $f^6 \mid \operatorname{disc} k_f K$ (recall that $\operatorname{disc} k_f = f^2$), and this shows that $f^2 \mid d$. □

Thus the compositum of K with the cyclic cubic field of prime conductor f is unramified over K if and only if $f^2 \mid \operatorname{disc} K$; only the cyclic cubic field of conductor 9 needs special attention (we have simply computed the discriminant of the compositum for all fields such that $\operatorname{disc} K$ is exactly divisible by 81, although working locally at 3 would have been faster).

2.4 ℓ-Class Fields of Quadratic Extensions

In this section we will have a closer look at ℓ-class fields of quadratic extensions k/F, and we will use this additional information (i.e. the fact that k/F is normal) to simplify our construction. We will need the following special case of what we proved in the first section (Prop. 2.2.1):

Proposition 2.4.1. *Let k/F be a quadratic extension, τ the nontrivial automorphism of k/F, ℓ an odd prime, and suppose that k contains the ℓ^{th} roots of unity. Then $K = k(\sqrt[\ell]{\omega})$ is normal over F if and only if $\omega^\tau = \omega^a \xi^\ell$ for some $\xi \in k$ and $a \in \{-1, +1\}$; moreover,*

$$\begin{aligned} \mathrm{Gal}\,(K/F) \simeq \mathbb{Z}/2\ell\mathbb{Z} \quad &\Longleftrightarrow \quad \begin{cases} a = +1 & \text{and} \quad \zeta \in F, \\ a = -1 & \text{and} \quad \zeta \in k \setminus F \end{cases} \\ \mathrm{Gal}\,(K/F) \simeq D_\ell \quad &\Longleftrightarrow \quad \begin{cases} a = -1 & \text{and} \quad \zeta \in F, \\ a = +1 & \text{and} \quad \zeta \in k \setminus F \end{cases} \end{aligned}$$

Now let k/F be a quadratic extension of number fields, and assume that $\ell \mid h(k)$ (note that this notation differs from the one we have used so far: k is not assumed to contain the ℓ^{th} roots of unity). Assume moreover that k is not contained in $F' = F(\zeta_\ell)$ and that $\ell \nmid h(F')$. Then $G = \mathrm{Gal}\,(k'/F) \simeq C_2 \times C_n$ for some divisor $n = \#G$ of $\ell - 1$.

Let $\tau \in G$ denote the automorphism of order 2 fixing F'. $\mathrm{Gal}\,(k'/k)$ is generated by some automorphism $\sigma_r \in G$ mapping ζ to ζ^r. Let $\widetilde{k}$ be the fixed field of $\langle \sigma_{-1}\tau \rangle$. We know that the ℓ-class fields of k are contained in the Kummer extensions corresponding to $\mathfrak{E}_1$, and more exactly to its subgroup $\widetilde{\mathfrak{E}}_1$ of

ℓ-primary elements. Now $\mathrm{Gal}\,(k'/F')$ acts on $\widetilde{\mathfrak{E}}_1$; using the idempotents $e^+ = \frac{1}{2}(1+\tau)$ and $e^- = \frac{1}{2}(1-\tau)$ we can define $\widetilde{\mathfrak{E}}_1^+ = \widetilde{\mathfrak{E}}_1^{e^+}$, $\widetilde{\mathfrak{E}}_1^- = \widetilde{\mathfrak{E}}_1^{e^-}$, and we get $\widetilde{\mathfrak{E}}_1 = \widetilde{\mathfrak{E}}_1^+ \oplus \widetilde{\mathfrak{E}}_1^-$.

By Prop. 2.4.1 we know that every $\omega \in \widetilde{\mathfrak{E}}_1^+$ gives rise to an unramified extension K/k' such that $\mathrm{Gal}\,(K/F') \simeq C_2 \times C_\ell$. Since $\ell \nmid h(F')$, there are no such extensions, hence all the unramified cyclic ℓ-extensions of K which are abelian over k must come from $\widetilde{\mathfrak{E}}_1^-$.

Now we claim that $\mathfrak{E}_1^-$ is generated by elements of the field $\widetilde{k}$. But since both τ and σ_{-1} act as -1 on $\mathfrak{E}_1^-$, their product $\tau\sigma_{-1}$ acts trivially. In particular, the relative norm $N_{k'/\widetilde{k}} = 1 + \tau\sigma_{-1}$ induces an isomorphism on $\mathfrak{E}_1^-$. This shows that all elements of $\mathfrak{E}_1^-$ (and, a fortiori, of $\widetilde{\mathfrak{E}}_1$) are generated by elements of $\widetilde{k}$:

Proposition 2.4.2. *Let k be a quadratic extension of number field F, and let ℓ be an odd prime. Assume that k is not contained in $k' = k(\zeta_\ell)$, and let $\tau \in G = \mathrm{Gal}\,(k'/F)$ be the automorphism fixing $F' = F(\zeta_\ell)$. Let $\widetilde{k}$ be the fixed field of $\sigma_{-1}\tau$, where σ_{-1} is the automorphism mapping $\zeta_\ell \longrightarrow \zeta_\ell^{-1}$. Then a cyclic ℓ-extension L/k' with $\mathrm{Gal}\,(L/F') \simeq D_\ell$ is abelian over k if and only if L has the form $L = k'(\sqrt[\ell]{\widetilde{\omega}})$ for some $\widetilde{\omega} \in \widetilde{k}/\widetilde{k}^{\times\ell}$ such that $\sigma_r(\widetilde{\omega}) = \widetilde{\omega}^r$. In particular, L contains an unramified cyclic extension of degree ℓ over k if and only if $\widetilde{\omega} \in \mathfrak{E}_1^-$.*

We see that instead of having to compute a subgroup of $\mathrm{Cl}(k')$ it suffices to know the generators of the class group of a smaller field.

Example 2.4.1. *Let us illustrate the construction procedure by examining $K = \mathbb{Q}(\sqrt{79})$. K has class number 3, and its ideal class group is generated by the prime ideal $5_1 = (5, 21 + 2\sqrt{79})$ of norm 5; moreover, $5_1^3 = (\omega_1)$ for $\omega_1 = 21 + 2\sqrt{79}$. The fundamental unit of K is $\varepsilon = 80 + 9\sqrt{79}$, but we have seen that we do not need it for the construction of the class field of K.*

Now let us take a look at $K' = \mathbb{Q}(\sqrt{79}, \sqrt{-3})$. The class number formula for bicyclic biquadratic number fields gives $h(K') = 18$. One factor 3 is accounted for by the subgroup generated by 5_1, the other comes from the 3-class group $\langle[13_1]\rangle$ of the subfield $F = \mathbb{Q}(\sqrt{-3 \cdot 79})$, where $13_1 = (13, 8 + 3\sqrt{-3 \cdot 79})$ is a prime ideal in $\mathcal{O}_F$ above 13. We find $13_1^3 = (\omega_2)$ for $\omega_2 = 8 + 3\sqrt{-3 \cdot 79}$.

We find $\mathfrak{E} = \langle\zeta_3, \varepsilon, \omega_1, \omega_2\rangle$. Decomposing $\mathfrak{E}$ yields $\mathfrak{E}_0 = \langle\varepsilon, \omega_1\rangle$ and $\mathfrak{E}_1 = \langle\zeta_3, \omega_2\rangle$. For the construction of the Hilbert class field of K we just have to examine $\mathfrak{E}_1$. In fact, since $\mathfrak{E}_1^+ = \langle\zeta_3\rangle$, it is sufficient to consider $\mathfrak{E}_1^- = \langle\omega_2\rangle$: since $h(K) = 3$, we conclude that ω_2 must be *primary. Therefore, the extension $K'(\sqrt[3]{\omega_2})$ contains the Hilbert class field of K: in fact, it is generated by a root $\mu = \sqrt[3]{\omega_2} + \sqrt[3]{\omega_2'}$ of the polynomial $x^3 - 39x - 16 \in \mathbb{Z}[x]$ (in general, $\mu = \sqrt[3]{\omega} + \sqrt[3]{\omega'}$, where $N\omega = n^3$ and $T\omega = t$, satisfies the equation $x^3 - 3nx - t = 0$ because of $\mu^3 = \omega + \omega' + 3\mu(\sqrt[3]{\omega\omega'}) = t + 3n\mu$).*

Just as easily we can give the Hilbert class field F^1 of F (note that $F' = K'$): the ideal class group of F is cyclic of order 6, with $[13_1]$ generating the subgroup of order 3. The Kummer extension containing F^1 is generated by an element of $\mathfrak{E}_0 = \langle\varepsilon, \omega_1\rangle$. Since ε is primary, we find $F^1 = F(\theta)$, where $\theta = \sqrt[3]{\varepsilon} + \sqrt[3]{\varepsilon'}$ is a root of the polynomial $x^3 - 3x - 160$.

The 2-class field of F is just its genus field $F(\sqrt{-1})$. Summarizing our results we get the class field $F'^1 = F(\sqrt{-1}, \mu, \theta)$ of F'. If we prefer real generators, we can replace $\sqrt{-1}$ by $\sqrt{3 \cdot 79}$.

Example 2.4.2. *Next we look at an example taken from [123], the bicyclic field $K = \mathbb{Q}(\sqrt{33}, \sqrt{-23})$. Here $\mathrm{Cl}(K) \simeq (4, 3, 3)$, and the 2-class field of K is easily computed by noting that K is an unramified quadratic extension of $k = \mathbb{Q}(\sqrt{-759})$ and that $\mathrm{Cl}(k) \simeq (2, 4, 3)$: now Rédei-Reichardt applies, and solving $x^2 + 11y^2 = 33z^2$ we find that $L = K\big(\sqrt{-5 + 2\sqrt{-11}}\,\big)$ is the 2-class field of K. Alternatively, L is generated by a root of $x^4 + 10x^2 + 69$.*

Since the 3-class group of a bicyclic number field is the direct product of the 3-class groups of its quadratic subfields, it suffices to compute the 3-class fields of $F = \mathbb{Q}(\sqrt{-23})$ and of k. Since $\mathbb{Q}(\sqrt{69})$ has class number 1, we only need its unit group, and from $\varepsilon = \frac{1}{2}(25 + 3\sqrt{69})$ we read off that the roots of $x^3 - 3x - 25$ generate the 3-class field of F. Finally we look at $\mathbb{Q}(\sqrt{253})$; here $\varepsilon = \frac{1}{2}(1861 + 117\sqrt{253})$ is the fundamental unit, giving the polynomial $x^3 - 3x - 1861$.

Collecting everything we see that the roots of

$$x^4 + 10x^2 + 69, \quad x^3 - 3x - 25, \quad \textit{and} \quad x^3 - 3x - 1861$$

generate the Hilbert class field of K.

Remark 6. *Although the coefficients of the polynomials in the last example are fairly small, we can already see that their size might become quite large if the fundamental units have large coefficients. In fact, if $\mathcal{C}_1 = 1$ and if $\mathcal{E}_1^-$ has rank 1, then the size of the constant term of the resulting polynomial only depends on the unit $\varepsilon \in \mathcal{E}_1^-$. In such a case it would be desirable to find some $\alpha \in \mathcal{O}_{\tilde{k}}$ such that $\alpha^3\varepsilon$ has small coefficients. In our example $d = 253$, where $\varepsilon = \frac{1}{2}(1861 + 117\sqrt{253})$, such an element is $\alpha = 16 - \sqrt{253}$: clearly $\alpha^3\varepsilon = \frac{1}{2}(19 + \sqrt{253})$ has smaller coefficients than ε. The resulting polynomial is $x^3 - 9x - 19$.*

Example 2.4.3. *Let us see what we can say about the class field of $K = \mathbb{Q}(\sqrt{-47})$. K has class number 5, so we put $K' = K(\zeta_5)$ and define σ to be a generator of $\mathrm{Gal}\,(K/K)$. Since K' has class number 5 we conclude that $C_1 = 1$ (only $\mathrm{Cl}_5(K)$ contributes to $\mathrm{Cl}_5(K')$). Let $\varepsilon = \frac{1}{2}(1 + \sqrt{5})$ be the fundamental unit of $\mathbb{Q}(\sqrt{5})$; we can find a unit $\eta \in K'^+$ in such a way that $\eta^{1+\sigma^2} = \pm 1$. Then Hasse has shown that $E = \langle \zeta, \varepsilon, \eta, \eta^\sigma \rangle$ form a 5-maximal subgroup of the unit group of K'. Now we get $\eta^{2+\sigma} \in \mathcal{E}_1$: in fact, $(\eta^{2+\sigma})^\sigma = \pm\eta^{2\sigma-1} \overset{5}{=} (\eta^{2+\sigma})^2$. Moreover, we have $\eta^{3+\sigma} \in \mathcal{E}_3$ and $\varepsilon \in \mathcal{E}_2$, and this shows that $\mathcal{E} = \mathcal{E}_0 \oplus \mathcal{E}_1 \oplus \mathcal{E}_2 \oplus \mathcal{E}_3$, where $\mathcal{E}_0 = E^\ell$, $\mathcal{E}_1 = \langle \zeta_5, \eta^{2+\sigma} \rangle E^\ell$, $\mathcal{E}_2 = \langle \varepsilon \rangle E^\ell$, and $\mathcal{E}_3 = \langle \eta^{3+\sigma} \rangle E^\ell$. Anyway, if $K'(\sqrt[5]{\mu})$ is an abelian extension of K then we must have $\mu \in \mathcal{E}_1$. Since $\mathcal{E}_1^- = \langle \eta^{2+\sigma} \rangle E^\ell$, we conclude that $\eta^{2+\sigma}$ is 5-primary, hence the class field we are looking for is $K'(\sqrt[5]{\eta^{2+\sigma}})$.*

The actual computation of the unit η yields

$$\eta = \frac{1}{2}\Big(\frac{47 - 5\sqrt{5}}{2} - \frac{5 - \sqrt{5}}{2}\sqrt{47\frac{5 + \sqrt{5}}{2}}\Big).$$

This is Hasse's [26] result. By the way, the relative class number $h^* = \#\mathrm{Cl}(K'/K'^+) = 2 \cdot 5$ given there is incorrect: K has odd class number, $(K' : K) = 4$ is a 2-power, and exactly one prime ramifies in K'/K: the ambiguous class number formula implies that K' has odd class number.

The problem of how to compute a generating polynomial for the cyclic unramified extension of K from the Kummer generator $\omega \in K'$ has been dealt with by Gras [31] and Odai [89].

It is easy to derive bounds for the ranks of the groups $\mathcal{E}_i$ from the unit theorems of Minkowski and Herbrand; see Leopoldt [313] or Oriat and Satgé [350].

2.5 Leopoldt's Spiegelungssatz

It is an interesting observation that the results of the preceding sections enable us to prove nontrivial relations between the ranks of class groups. In fact, since the unramified cyclic extensions of degree ℓ over K are generated by ℓ^{th} roots of elements of $\mathfrak{E}_1$ when lifted to K', we find immediately that $\mathrm{rank}\mathrm{Cl}_\ell(K) \leq \mathrm{rank}_\ell\mathfrak{E}_1 = \mathrm{rank}_\ell\mathcal{E}_1 + \mathrm{rank}_\ell C_1 \leq \mathrm{rank}_\ell E(K'/K)/E(K')^\ell + \mathrm{rank}_\ell\mathrm{Cl}(K'/K)$. Of course, these last bounds are rather crude; this section is devoted to refining them.

What we want is to find relations between the submodules $\mathcal{C}_i$ of the ℓ-class group and the submodules $\widetilde{\mathfrak{E}}_j$ of the Kummer radical of an extension k'/k. This is accomplished by the fact that the Artin isomorphism is actually a $\mathrm{Gal}\,(k/F)$-isomorphism. We claim

Theorem 2.5.1. *Let k/F be a finite abelian extension with Galois group G. Then the following assertions are equivalent:*

i) $C(\phi) \neq 1$;

ii) there exists an unramified extension K/k of degree ℓ with $\mathrm{Gal}\,(K/k) = \langle \tau \rangle$ which is normal over k such that $\tau^\sigma = \tau^{\phi(\sigma)}$;

Moreover, if k contains the ℓ^{th} roots of unity and if $\#G \mid \ell - 1$, then i) and ii) are also equivalent to

iii) $\widetilde{\mathfrak{E}}(\chi\phi^{-1}) \neq 1$.

Proof. Assume that $C(\phi) \neq 1$. Let I and H denote the group of fractional and principal fractional ideals of k. To every ideal group D such that $H \leq D \leq I$ there corresponds an unramified abelian extension K/k of degree $(D : H)$. Let K be the class field corresponding to a subgroup D of order ℓ in $C(\phi)$, and let c be an ideal class generating D. Then K/k is an unramified abelian extension of degree ℓ, and since G acts on D, K/F is normal. Moreover, the Artin isomorphism shows that $\tau = \left(\frac{K/k}{c}\right)$ generates $\mathrm{Gal}\,(K/k)$, and the functoriality of the Artin symbol gives

$$\tau^\sigma = \Big(\frac{K/k}{c^\sigma}\Big) = \Big(\frac{K/k}{c}\Big)^{\phi(\sigma)} = \tau^{\phi(\sigma)}.$$

This proves i) $\Longrightarrow$ ii).

For a proof of the other direction, assume that K satisfies the conditions ii). By Artin's reciprocity theorem, there is an ideal class $c \in \mathrm{Cl}_\ell(k)$ such that $\tau = \left(\frac{K/k}{c}\right)$, and we find $c^{\sigma-\phi(\sigma)} \in C = N_{K/k}\mathrm{Cl}_\ell(K)$. Now C is a $\mathbb{Z}_\ell[G]$-module, and the map $\delta : G \longrightarrow C : \sigma \longmapsto c^{\sigma-\phi(\sigma)}$ satisfies the Noether equations of Thm. 2.1.3. Therefore there exists an ideal class $d \in C$ such that $\delta(\sigma) = d^{\sigma-\phi(\sigma)}$. But now $c' = cd^{-1}$ is an ideal class with $\tau = \left(\frac{K/k}{c'}\right)$ (in particular, $c' \neq 1$) and $c'^{\sigma-\phi(\sigma)} = 1$, and this shows that $c' \in C(\phi)$.

Now assume that ii) holds and write K in the form $K = k'(\sqrt[\ell]{\omega})$ for some $\omega \in \widetilde{\mathfrak{E}}$. By Prop. 2.2.1 we know that $\tau^\sigma = \tau^{\phi(\sigma)}$ if and only if $\omega^\sigma = \omega^{\chi(\sigma)\phi(\sigma)^{-1}}$. This actually shows that ii) $\iff$ iii). $\square$

The character $\overline{\phi} = \chi\phi^{-1}$ is called the reflection of ϕ; note that $\overline{\overline{\phi}} = \chi\chi^{-1}\phi = \phi$, thus reflection is an involution on $\mathrm{Aut}(\widehat{G})$.

Proposition 2.5.2. *Let k be as above; then* $\mathrm{rank}\mathcal{C}(\phi) \leq \mathrm{rank}\widetilde{\mathcal{E}}(\overline{\phi}) + \mathrm{rank}\mathcal{C}(\overline{\phi})$.

Let us apply Prop. 2.5.2 to the simplest case $\ell = 3$. Let k be a number field and put $k' = k(\zeta_3)$. Then $\mathcal{C}_0 = {}_3\mathrm{Cl}(k)$ and $\mathcal{C}_1 = {}_3\mathrm{Cl}(k'/k)$. Let δ_0 and δ_1 denote the number of independent 3-primary units in $E(k)$ and $E(k'/k)$, respectively; then

$$\begin{aligned} \mathrm{rank}\mathrm{Cl}_3(k) &= \mathrm{rank}\mathcal{C}_0 \leq \widetilde{\mathcal{E}}_1 + \mathrm{rank}\mathcal{C}_1 = \delta_1 + \mathrm{rank}\mathrm{Cl}_3(k'/k), \\ \mathrm{rank}\mathrm{Cl}_3(k'/k) &= \mathrm{rank}\mathcal{C}_1 \leq \widetilde{\mathcal{E}}_0 + \mathrm{rank}\mathcal{C}_0 = \delta_0 + \mathrm{rank}\mathrm{Cl}_3(k). \end{aligned}$$

Taken together this gives

$$2\mathrm{rank}\ \mathrm{Cl}_3(k) \leq \delta(K'/K) + \mathrm{rank}\ \mathrm{Cl}_3(k') \leq 2\mathrm{rank}\ \mathrm{Cl}_3(k) + \delta(K').$$

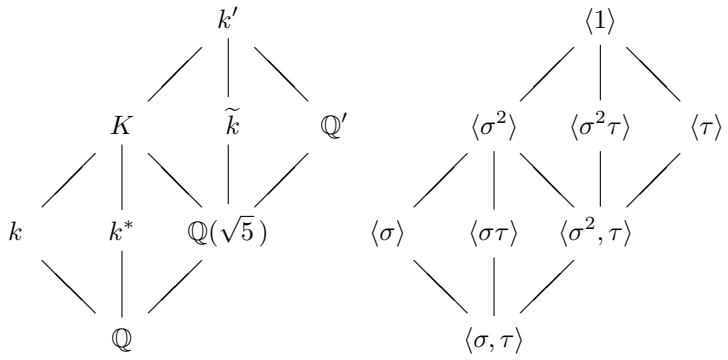
Proposition 2.5.3. *Let K be a number field; let $\delta(K)$ and $\delta(K')$ denote the number of independent 3-primary units of $E(K)$ and $E(K')$, respectively, and put $\delta(K'/K) = \delta(K') - \delta(K)$. Then*

$$2\mathrm{rank}\ \mathrm{Cl}_3(K) \leq \delta(K'/K) + \mathrm{rank}\ \mathrm{Cl}_3(K') \leq 2\mathrm{rank}\ \mathrm{Cl}_3(K) + \delta(K').$$

For quadratic number fields K, Prop. 2.5.3 is just Scholz's reflection theorem which says that the 3-ranks of $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{-3m})$ differ at most by 1.

If K is a totally real cubic field then $\delta(K'/K) = 1$ if and only if ζ_3 is 3-primary, and $\delta(K'/K) = 0$ otherwise. In particular, we have $1 \leq r_3' \leq 4$; the reason why there are no examples with $r_3' = 1$ in [119] is that r_3' was not computed for the fields with $\delta(K'/K) = 1$. It is however easy to find examples (e.g. the cyclic cubic fields of conductor $9 \cdot 7$). Moreover, there were also no examples with $r_3' = 4$; this is probably due to the fact that only fields with discriminants < 100.000 were tested.

Next we'll look more closely at the case $\ell = 5$ for quadratic number fields k. Our results will contain those of Parry [54, 59] on the Hilbert 5-class fields of the quadratic number fields $k = \mathbb{Q}(\sqrt{m})$ and $k^* = \mathbb{Q}(\sqrt{5m})$ as a special case. To this end, let $m \in \mathbb{Z}$ be squarefree (not necessarily positive). The quadratic subfields of $k' = k(\zeta_5)$ are k, k^* and $\mathbb{Q}(\sqrt{5})$. The Galois group $G = \mathrm{Gal}\,(k'/\mathbb{Q})$ is generated by the automorphisms $\sigma : \zeta \longrightarrow \zeta^2$, $\sqrt{m} \longrightarrow \sqrt{m}$ and $\tau : \sqrt{m} \longrightarrow -\sqrt{m}$, $\zeta \longrightarrow \zeta$. The following Hasse diagrams display all the fields and groups involved:



In order to construct the 5-class field of k we decompose the group $\mathfrak{E}$ as before by using the idempotents e_j of the group algebra $\mathbb{Z}[\mathrm{Gal}\,(k'/\mathbb{Q})]$ and get $\mathfrak{E} = \mathfrak{E}_0 \oplus \mathfrak{E}_1 \oplus \mathfrak{E}_2 \oplus \mathfrak{E}_3$. We know that $k'(\sqrt[5]{\omega})$ (for $\omega \in \mathfrak{E}$) is abelian over k if and only if $\omega \in \mathfrak{E}_1$.

Decomposing the G-modules $\mathfrak{E}_j$ with regard to the action of τ gives $\mathfrak{E}_j = \mathfrak{E}_j^+ \oplus \mathfrak{E}_j^-$. Replacing the base field k by k^* gives us $\mathfrak{E}^* = \mathfrak{E}_0^* \oplus \mathfrak{E}_1^* \oplus \mathfrak{E}_2^* \oplus \mathfrak{E}_3^*$; observe that this decomposition corresponds to the action of $\sigma^* = \sigma\tau$. Since τ acts as $-1 \equiv r^2 \bmod 4$ on the submodules $\mathfrak{E}_j^-$, we find that $\mathfrak{E}_j^+ = \mathfrak{E}_j^{*+}$ and $\mathfrak{E}_j^- = \mathfrak{E}_{j+2}^{*-}$, where the index $j+2$ is to be read mod 4. It is also easy to see that $\mathcal{C}_0 = {}_5\mathrm{Cl}(k)$, $\mathcal{C}_2 = {}_5\mathrm{Cl}(k^*)$, and $\mathcal{C}_1 \oplus \mathcal{C}_3 = {}_5\mathrm{Cl}(\widetilde{k})$. Since $\mathbb{Q}'$ has class number 1, we have $\mathcal{C}^+ = 1$.

The unit groups are slightly harder to compute. Let K/k be a finite extension of number fields. A unit $\varepsilon \in E_K$ is called a *relative unit* if $N_{K/k}\varepsilon = 1$; the relative units of K/k form a group $E_{K/k}$. For cyclic quartic extensions $K/\mathbb{Q}$ with real quadratic subfield k Hasse showed that the group $E_k E_{K/k}$ has index ≤ 2 in the full group of units E_K; in particular, $E_k E_{K/k}$ is 5-maximal.

Assume now that $m > 0$; then k, k^* and K are totally real, hence $\widetilde{k}$ is totally complex, and, in particular, there are no nontrivial relative units in $\widetilde{k}/\mathbb{Q}(\sqrt{5})$. If, on the other hand, k is imaginary quadratic, then k^* and K are CM-fields, hence $\widetilde{k}$ is totally real. In each case, k' has unit rank 3, and

$$E = \langle\zeta, \varepsilon_5, \varepsilon, \varepsilon^\sigma\rangle \text{ if } m < 0, \quad E = \langle\zeta, \varepsilon_5, \varepsilon_m, \varepsilon_{5m}\rangle \text{ if } m > 0,$$

is a 5-maximal subgroup of $E(k')$ (here ε_d denotes the fundamental unit of $\mathbb{Q}(\sqrt{d})$, and ε (in the case $m < 0$) is a relative unit, i.e. it satisfies $\varepsilon^{1+\sigma^2} = \pm 1$). Now we find that $(\varepsilon^{2+\sigma})^\sigma = \pm\varepsilon^{2\sigma-1} \overset{5}{=} (\varepsilon^{2+\sigma})^2$, i.e. $\varepsilon^{2+\sigma} \in E_1$. The 5-maximality of E implies that $\varepsilon^{2+\sigma}$ is not trivial in E_1; doing similar computations for the other groups E_j and counting ranks (the equality $E_1 = \langle\varepsilon^{2+\sigma}\rangle$ comes from observing that the ranks of the constructed subgroups add up to the 5-rank of $E(k')/E(k')^5$) gives the following table (the case $m < 0$ is handled similarly):

$m > 0$		$m < 0$	
$\mathcal{E}_0^+ = 1$	$\mathcal{E}_0^- = \langle\varepsilon_m\rangle$	$\mathcal{E}_0^+ = 1$	$\mathcal{E}_0^- = 1$
$\mathcal{E}_1^+ = \langle\zeta\rangle$	$\mathcal{E}_1^- = 1$	$\mathcal{E}_1^+ = \langle\zeta\rangle$	$\mathcal{E}_1^- = \langle\varepsilon^{2+\sigma}\rangle$
$\mathcal{E}_2^+ = \langle\varepsilon_5\rangle$	$\mathcal{E}_2^- = \langle\varepsilon_{5m}\rangle$	$\mathcal{E}_2^+ = \langle\varepsilon_5\rangle$	$\mathcal{E}_2^- = 1$
$\mathcal{E}_3^+ = 1$	$\mathcal{E}_3^- = 1$	$\mathcal{E}_3^+ = 1$	$\mathcal{E}_3^- = \langle\varepsilon^{3+\sigma}\rangle$

Next we examine which extensions $K = k'(\sqrt[5]{\omega})$ are abelian over certain subfields of k'. Let H be the subgroup of $G = \langle\sigma,\tau\rangle$ fixing L; then k'/L is abelian if and only if H commutes with ϕ. From Prop. 2.2.1 we get

$$K \text{ is abelian over } \left\{\begin{array}{c} k \\ k^* \\ K \\ \widetilde{k} \end{array}\right\} \text{ if and only if } \omega \in \left\{\begin{array}{c} \mathfrak{E}_1 \\ \mathfrak{E}_1^+ \oplus \mathfrak{E}_3^- \\ \mathfrak{E}_1 \oplus \mathfrak{E}_3 \\ \mathfrak{E}_0^- \oplus \mathfrak{E}_1^+ \oplus \mathfrak{E}_2^- \oplus \mathfrak{E}_3^+ \end{array}\right\}$$

Now $k'(\sqrt[5]{\omega})$ (for $\omega \in \mathfrak{E}$) is abelian over k^* if and only if $\omega \in \mathfrak{E}_1^* = \mathfrak{E}_1^+ \oplus \mathfrak{E}_3^-$. Next $\mathcal{C}^+ = 1$ implies $\mathfrak{E}_1^+ = \mathcal{E}_1^+ = \langle\zeta\rangle E(k')^\ell$. On the other hand we know that unramified extensions $k'(\sqrt[5]{\omega})$ which are abelian

over k or k^* come from $\widetilde{\mathfrak{E}}_1^-$ or $(\widetilde{\mathfrak{E}}_1^*)^-$, respectively. But $\mathfrak{E}^- \subseteq \widetilde{\mathcal{E}}_1^- \oplus \mathcal{C}_1^-$, and $\mathcal{E}_1^-$ is generated by the relative units of $\widetilde{k}/\mathbb{Q}(\sqrt{5}\,)$.

Letting δ denote the number of independent 5-primary units in $\mathcal{E}_1^-$ (i.e. $\delta(\widetilde{k}) = 0$ if $\widetilde{k}$ is CM or if $\widetilde{k}$ is totally real and the unique (up to a factor of ± 1) relative unit in $\mathcal{E}_1^-$ is not 5-primary) we get $\mathrm{rank}\mathcal{C}_0 \le \delta + \mathrm{rank}\mathcal{C}_1$. Replacing k by k^* we get in a similar way $\mathrm{rank}\mathrm{Cl}_5(k^*) = \mathrm{rank}\mathcal{C}_2 \le \delta^* + \mathrm{rank}\mathcal{C}_3$.

Theorem 2.5.4. *Let $k = \mathbb{Q}(\sqrt{m}\,)$ be a quadratic number field, and let k^* and $\widetilde{k}$ be defined as above. Put*

$$\delta = \begin{cases} 1 & \text{if } \varepsilon_m \text{ is 5-primary,} \\ 0 & \text{otherwise,} \end{cases} \qquad \delta^* = \begin{cases} 1 & \text{if } \varepsilon_{5m} \text{ is 5-primary,} \\ 0 & \text{otherwise,} \end{cases}$$

if $m > 0$ and

$$\delta = \begin{cases} 1 & \text{if } \varepsilon^{2+\sigma} \text{ is 5-primary,} \\ 0 & \text{otherwise,} \end{cases} \qquad \delta^* = \begin{cases} 1 & \text{if } \varepsilon^{3+\sigma} \text{ is 5-primary,} \\ 0 & \text{otherwise,} \end{cases}$$

if $m < 0$, where ε denotes the relative unit of $\widetilde{k}$ as defined above. Using the idempotents of $\mathbb{Z}[\mathrm{Gal}\,(k'/k)]$, we factorize $C = {}_5\mathrm{Cl}(k') = C_0 \oplus C_1 \oplus C_2 \oplus C_3$; then $C_0 \simeq {}_5\mathrm{Cl}(k)$, $C_2 \simeq {}_5\mathrm{Cl}(k^*)$, and $C_1 \oplus C_3 \simeq {}_5\mathrm{Cl}(\widetilde{k})$. Let $r_5(F)$ denote the 5-rank of the ideal class group of F:

$$\left.\begin{array}{ccccc} r_5(k) & \le & \mathrm{rank}C_1 & \le & r_5(k) + \delta \\ r_5(k^*) & \le & \mathrm{rank}C_3 & \le & r_5(k^*) + \delta^* \\ r_5(k) + r_5(k^*) & \le & r_5(\widetilde{k}) & \le & r_5(k) + r_5(k^*) + \delta + \delta^* \end{array}\right\} \quad \text{if } m > 0,$$

$$\left.\begin{array}{ccccc} r_5(k) - \delta & \le & \mathrm{rank}C_1 & \le & r_5(k) \\ r_5(k^*) - \delta^* & \le & \mathrm{rank}C_3 & \le & r_5(k^*) \\ r_5(k) + r_5(k^*) - \delta - \delta^* & \le & r_5(\widetilde{k}) & \le & r_5(k) + r_5(k^*) \end{array}\right\} \quad \text{if } m < 0.$$

The following table was computed using PARI:

m	$r_5(k)$	$r_5(k^*)$	$r_5(\widetilde{k})$	δ	δ^*	$\mathrm{rank}C_1$	$\mathrm{rank}C_3$	$\mathrm{Cl}(\widetilde{k})$
-571	1	1	1					
-347	1	0	1			1	0	
-47	1	0	0	1	0	0	0	
401	1	0	1	0	0	1	0	$(20, 4)$
1996	1	0	2	0	1	1	1	$(20, 10, 2)$
4504	1	1	2	0	1	1	1	$(30, 30)$

2.6 ℓ-Class Fields of Cyclotomic Fields

The ℓ-class field of $\mathbb{Q}(\zeta_\ell)$ has been studied extensively because of the connections with Fermat's Last Theorem. Pollaczek was the first to prove an essential part of what today is called "Herbrand's Theorem". In order to state it, let us introduce some notation. Let $K = \mathbb{Q}(\zeta_\ell)$, and put $G = \mathrm{Gal}\,(K/\mathbb{Q})$. Then $K^+ = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$ is the maximal real subfield of K; its class number is denoted by h_ℓ^+. The minus class group $\mathrm{Cl}^-(K)$ of K is defined to be the kernel of the norm map $N_{K/K^+}\mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(K^+)$. If h_ℓ^- denotes its order, we have the formula $h(K) = h_\ell^- h_\ell^+$.

We will also need the cyclotomic units η_ν, $\nu = 2, 4, \ldots, \ell - 3$ (where g denotes a primitive root modulo ℓ)

$$\eta_\nu = \prod_{a=1}^{\ell-1} \left(\zeta^{\frac{1-g}{2}} \, \frac{1-\zeta^g}{1-\zeta} \right)^{a^\nu \sigma_a^{-1}}.$$

A little computation shows easily that $\eta_\nu^{\sigma_r} = \eta_\nu^{r^\nu} \varepsilon^\ell$ for some unit $\varepsilon \in E_K$; this shows that $\eta_\nu \in E_\nu$, where $E = E_K/E_K^\ell$ and $E = E_0 \oplus E_1 \oplus \ldots \oplus E_{\ell-1}$ is the decomposition of the $\mathbb{F}_\ell[G]$-module E into submodules.

Let B_n be the n^{th} Bernoulli number; Pollaczek [8] and Herbrand [11] proved

Theorem 2.6.1. *For the $\mathbb{F}_\ell[G]$-module $C = {}_\ell\mathrm{Cl}(K)$, the following is true:*

a) $C_1 = 0$*;*

b) if $\nu < \ell$ *is odd and* $\ell \nmid B_{\ell-\nu}$ *then* $C_\nu = 0$*.*

On the other hand, if $\ell \mid B_{\ell-\nu}$ *then* η_ν *is* ℓ*-primary, i.e.* $\eta_\nu \equiv \xi^\ell \bmod (1-\zeta)^\ell$ *for some* $\xi \in K$*. If the class number* h^+ *of the maximal real subfield* $K^+ = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$ *is not divisible by* ℓ*, then* η_ν *is not an* ℓ^{th} *power, and* $K_\nu = K(\sqrt[\ell]{\eta_\nu})$ *is an unramified cyclic extension of degree* ℓ *over* K*.*

The fact that these class fields are generated by ℓ-th roots of units was predicted by Takagi [306]:

Proposition 2.6.2. *Let* $K = k(\zeta_\ell)$ *be a quadratic extension, and suppose that the class number of* k *is not divisible by* ℓ*. Then every unramified cyclic extension of degree* ℓ *over* K *has the form* $K(\sqrt[\ell]{\varepsilon})$*, where* ε *is a unit in* E_K*. In particular,* $\mathrm{rankCl}_\ell(K) \leq \frac{\ell-3}{2}$ *if* $K = \mathbb{Q}(\zeta_\ell)$ *and* $\ell \nmid h^+(K)$*.*

Proof. We have $\widetilde{\mathfrak{E}} = \widetilde{\mathfrak{E}}_0 + \widetilde{\mathfrak{E}}_1$; moreover $\mathrm{rank}_\ell \widetilde{\mathfrak{E}}_1 = \mathrm{rankCl}_\ell(k) = 0$. Therefore the class fields of K have the form $K(\sqrt[\ell]{\omega})$ for $\omega \in \widetilde{\mathfrak{E}}_0$. Since $\ell \nmid h(k)$ we have $C_0 = 1$, which shows that $\omega \in \widetilde{E}_0$.

If $K = \mathbb{Q}(\zeta_\ell)$, then $K(\sqrt[\ell]{\zeta_\ell})$ is ramified; hence there are at most $\dim(E_K/E_K^\ell) - 1$ independent units giving rise to unramified ℓ-extensions. Whence the claim. □

If $\ell \nmid h_\ell^+$, then the class field K_ν constructed by Herbrand does not only show that one of the C_i is non-trivial: actually it implies that $C_\nu \neq 1$.

Corollary 2.6.3. *Assume that* $\ell \mid B_{\ell-\nu}$ *and* $\ell \nmid h^+$*; then* $C_\nu \neq 1$*.*

This is an immediate consequence of Thm. 2.5.1. In fact, the assumptions imply that $K(\sqrt[\ell]{\eta_\nu})$ is a cyclic unramified extension of degree ℓ; since $\eta_\nu \in \widetilde{\mathfrak{E}}_\nu$, Thm. 2.5.1 implies that $C_{1-\nu} = C_{\ell-\nu}$ is not trivial.

It was not clear what happened for primes ℓ such that $\ell \mid h^+(\mathbb{Q}(\zeta_\ell))$ (Vandiver's conjecture says that there aren't any) until Ribet [49] used the theory of modular forms to prove

Theorem 2.6.4. *If* $\ell \mid B_{\ell-\nu}$ *for some odd* $\nu \leq \ell - 2$*, then* $C_\nu \neq 0$*.*

Together with Theorem 2.6.1 this shows that $p \mid B_{\ell-\nu}$ if and only if C_ν is not trivial.

We have seen that $\ell \mid B_{\ell-\nu}$ implies that $C_\nu \neq 1$, and in particular, that ℓ divides the class number of $K = \mathbb{Q}(\zeta_\ell)$. In fact we can even determine whether ℓ divides the class number of some subfield (Vandiver [305]):

Proposition 2.6.5. *Suppose that* $\ell \nmid h_\ell^+$*,* $\ell \mid B_{\ell-\nu}$ *for some odd* $\nu \leq \ell - 2$*, and put* $m = (\nu, \ell - 1)$*. Then* ℓ *divides the class number of the unique subfield of degree* $\frac{\ell-1}{m}$ *of* $\mathbb{Q}(\zeta_\ell)$*.*

Proof. Let $L = K(\sqrt[\ell]{\eta_\nu})$ be the class field constructed above. We know that $L/\mathbb{Q}$ is normal with Galois group $\Gamma = \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau | \sigma^{\ell-1} = \tau^\ell = 1, \sigma^{-1}\tau\sigma = \tau^a \rangle$

□

Proposition 2.6.6. *Let* $C = \bigoplus C_\nu$ *be the decomposition introduced above. If* ν *is an even integer* $\leq \ell - 3$ *then*

$$\mathrm{rank}C_\nu \;\leq\; \mathrm{rank}C_{\ell-\nu} \;\leq\; \mathrm{rank}C_\nu + 1.$$

Chapter 3

Separants

In 1971, L. Goldstein introduced generalized prime discriminants for fields F with class number 1; it turned out that every discriminant of a quadratic extensions of F could be written as a product of prime discriminants if and only if F is totally real with class number 1 in the strict sense. In this chapter we define a group which measures the extent to which such factorizations are non-unique.

3.1 Introduction

The simplest invariant of a quadratic number field $k = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ squarefree, is its *discriminant* $\operatorname{disc} k$, which is given by

$$\operatorname{disc} k = \begin{array}{ll} m, & \text{if } m \equiv 1 \bmod 4 \\ 4m, & \text{if } m \equiv 2, 3 \bmod 4 \end{array}.$$

In contrast to fields of higher degree, a quadratic number field k is defined uniquely by its discriminant $\operatorname{disc} k$. Gauss has shown (cum grano salis) that the 2-rank of the ideal class group can be computed by factorizing $\operatorname{disc} k$ into *prime discriminants*; these are discriminants which are prime powers, i.e.,

$$\operatorname{disc} k \in \{-4, \pm 8, -q \ (q \equiv 3 \bmod 4 \text{ prime}), \ p \ (p \equiv 1 \bmod 4 \text{ prime})\}.$$

It is easy to see that every discriminant of a quadratic number field can be written uniquely (up to permutation) as a product of prime discriminants; the 2-rank of the ideal class group of k in the strict sense then equals $t - 1$, where t is number of factors of $\operatorname{disc} k$.

Now suppose that F is a number field with class number 1; then the ring of integers $\mathcal{O}_k$ of every quadratic extension k/F has an $\mathcal{O}_F$-basis $\{1, \alpha\}$, i.e., $\mathcal{O}_k = \mathcal{O}_F \oplus \alpha\mathcal{O}_F$. The *generalized discriminant* of k/F defined by $\operatorname{disc}(k/F) = \operatorname{disc} \alpha = (\alpha - \alpha')^2$ is unique up to squares of units in $\mathcal{O}_F$; we will call a generalized discriminant *prime* if it is a prime power. Then it is natural to ask if every generalized discriminant can be factorized into prime discriminants, and if this factorization (if it exists) is unique (up to permutation or multiplication by squares of units). This question was answered partially by Goldstein [249] who showed that such a factorization exists if F is a totally real number field which has class number $h^+(F) = 1$ in the strict sense, i.e., if F has class number 1 and units with independent signatures. He also showed that all factorizations into prime discriminants are equivalent if and only if $(k_{\text{gen}} : k) = 2^{t-1}$, where t is the number of "factors" of d; however he failed to notice that this always holds if F is totally real and $h^+(F) = 1$, and his Theorem 5.1, which treats unique factorization into prime discriminants over real quadratic F, is even false. Sunley [251] settled unique factorization for real quadratic number fields with strict class number 1, and finally Davis [264] found that the totally real fields F with $h^+(F) = 1$ are the only number fields in which factorization into prime discriminants exists, and that these factorizations are necessarily unique.

In fact it is easily seen that the discriminants of some quadratic extensions of $F = \mathbb{Q}(i)$, $i^2 = -1$,

cannot be factorized into prime discriminants: if $\mu \in \mathbb{Z}[i]$ is squarefree, then

$$\operatorname{disc}(k/F) = \begin{array}{ll} \pm\mu, & \text{if } \mu \equiv \pm 1 \bmod 4 \\ \pm 2i\mu, & \text{if } \mu \equiv \pm 1 + 2i \bmod 4 \\ \pm 4\mu, & \text{if } \mu \equiv \pm i \bmod 2 \text{ or } \mu \equiv 0 \bmod 1+i \end{array} .$$

In particular, the discriminant $\pm(1+2i)2i$ of $\mathbb{Q}\left(\sqrt{1+2i}\right)$ is neither prime nor a product of prime discriminants, because the only prime discriminants above $1+i$ are $d = \pm 4i$ for $\mathbb{Q}\left(\sqrt{i}\right)$ and $d = \pm 4 \pm 4i$ for $\mathbb{Q}\left(\sqrt{1 \pm i}\right)$.

An even simpler example is provided by quadratic fields, if we take the infinite primes into account: the factorization of $\operatorname{disc} k$ into prime discriminants corresponds to the maximal abelian extension k^+_{gen} of $\mathbb{Q}$ which is unramified at the finite primes. Suppose we are only interested in extensions which are also unramified at ∞; then only factorizations into "positive" discriminants correspond to subfields of k_{gen}.

Example 3.1.1. *Let $k = \mathbb{Q}(\sqrt{1155})$; then $d = \operatorname{disc} k = 1155 = 4 \cdot 3 \cdot 5 \cdot 7 \cdot 11$, and its factorization into prime discriminants is $d = (-4) \cdot (-3) \cdot 5 \cdot (-7) \cdot (-11)$. This shows that $\mathrm{Cl}^+(k)$ has 2-rank 4, and that $k^+_{gen} = \mathbb{Q}(\sqrt{-1}, \sqrt{-3}, \sqrt{5}, \sqrt{-7}, \sqrt{-11})$ is the genus field of k in the strict sense. On the other hand, $\mathrm{Cl}(k)$ has 2-rank 3, and the genus field of k in the usual sense is $k_{gen} = \mathbb{Q}(\sqrt{5}, \sqrt{3}, \sqrt{7}, \sqrt{11})$, which does not correspond (directly) to a factorization of d into positive prime discriminants, but rather is associated to the factorizations $d = 5 \cdot 12 \cdot 77 = 5 \cdot 28 \cdot 33 = 5 \cdot 44 \cdot 21$ of d into relatively prime and positive discriminants.*

In order to restore unique factorization into prime discriminants, we have to follow Kummer's idea of introducing "ideal elements"; for $F = \mathbb{Q}(\sqrt{-1})$, such an ideal discriminant would be the set

$$\{2i\mu \mid \mu \equiv \pm 1 + 2i \bmod 4 \text{ squarefree}\}$$

of all discriminants which are exactly divisible by $2i$. Similarly, $\{-3, -4, -7, -8, -11, \ldots\}$ would be an ideal discriminant at ∞ in the real quadratic case.

We will show how to make these ideal elements into a group containing the generalized discriminants as a subgroup, and we will compute the order of their factor group. It turns out that this factor group is trivial if and only if F is totally real and $h^+(F) = 1$, hence our results contain those of Goldstein, Sunley and Davis described above as a special case.

The results of this chapter, which elaborates ideas sketched in the authors dissertation [115], will be used in Chap. 4, where theorems of Koch, Rédei and Reichardt, and Scholz on the 2-class field tower of quadratic number fields will be generalized. I have meanwhile discovered that the idea of introducing "ideal discriminants" has been anticipated by Brandt [234, 235] for quadratic extensions of $\mathbb{Q}(\sqrt{-1})$.

One more remark: we will give a completely different definition of separants in the next section; this will simplify the introduction of a group structure on the set of separants considerably.

3.2 Norm Residue Characters

Proposition 3.2.1. *Let $k_j/F, j = 1, 2$, be quadratic extensions of F, and put $d_j = \operatorname{sep}(k_j/F)$. Then $L = k_1 k_2$ is a V_4-extension of F with subfields k_1, k_2, k_3, and the following assertions are equivalent:*

i) $d_1 \cdot d_2 = d_1 * d_2$;

ii) $(d_1, d_2) \mid \infty$;

iii) L/k_3 *is unramified outside* ∞.

3.3 The Separant Class Group $\mathrm{SCl}(F)$

3.4 Fields with $\mathrm{SCl}(F) = 1$

An important property of fields with trivial separant class group is

Proposition 3.4.1. *Let F be a number field with $\mathrm{SCl}(F) = 1$; then for every prime $\mathfrak{p} \mid 2\mathcal{O}_F$ there exists a unit $\varepsilon \in E_F$ such that $\mathfrak{p}$ is the only finite prime ramified in $F(\sqrt{\varepsilon}\,)/F$. Moreover, if $\mathfrak{p}$ is ramified in $F(\sqrt{\alpha}\,)$ for some $\alpha \not\equiv 0 \bmod b$, then $\mathfrak{p}$ does not ramify in $k = F(\sqrt{\alpha\varepsilon}\,)/F$.*

Chapter 4

The Construction of 2-Class Fields

In this Chapter we deal with the 2-class field tower of an algebraic number field; in particular we are interested in simple ciriteria which guarantee the existence of certain "small" unramified non-abelian 2-extensions. Then we correct and extend results of Koch on the 2-class field tower of quadratic number fields, and we show how to generalize Scholz's reciprocity law to fields of higher degree.

4.1 Introduction

The first result on 2-class groups of quadratic number fields k that was not contained in the genus theory of Gauss and Dirichlet is the criterion of Rédei and Reichardt [15], which links the existence of quartic cyclic unramified extensions of k to certain factorizations of the discriminant $\operatorname{disc} k$ into prime discriminants. Koch showed how a theorem of Fröhlich could be used to generalize this correspondence to other unramified extensions of class 2. Our aim is to generalize these results from quadratic extensions of $\mathbb{Q}$ to quadratic extensions of number fields F with odd class number in the strict sense. To this end we replace Goldstein's generalized prime discriminants by prime separants (see Cahp. 3 for the necessary background) and show that the theory of Rédei, Reichardt and Scholz (cf. [12, 15, 535]) is valid over such fields. In particular, we will find a reciprocity theorem which contains Scholz's reciprocity law as a very special case. Moreover we will show how to construct parts of the 2-class field tower of certain number fields k beyond the Hilbert 2-class field k^1; in particular, we will study unramified dihedral and quaternionic extensions.

4.2 Cyclic extensions

We start with the proof of a criterion which in case $F = \mathbb{Q}$ is due to Rédei and Reichardt. To this end, we need some notations: let L/F be a D_4-extension, i.e., a normal extension such that $\operatorname{Gal}(L/F) \simeq D_4 = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ (thus D_4 is the dihedral group of order 8). Then diagram 1 gives the subfields of L/F and the subgroups of D_4 corresponding to these subfields by Galois theory.

We call an extension K/k *unramified* if no *finite* prime ramifies in K/k; accordingly, two separants d_1, d_2 are said to be *relatively prime* if $(d_1, d_2) \mid \infty$.

Theorem 4.2.1. *Let F be a number field with odd class number, k/F a quadratic extension, and L/k an unramified C_4-extension. Then*

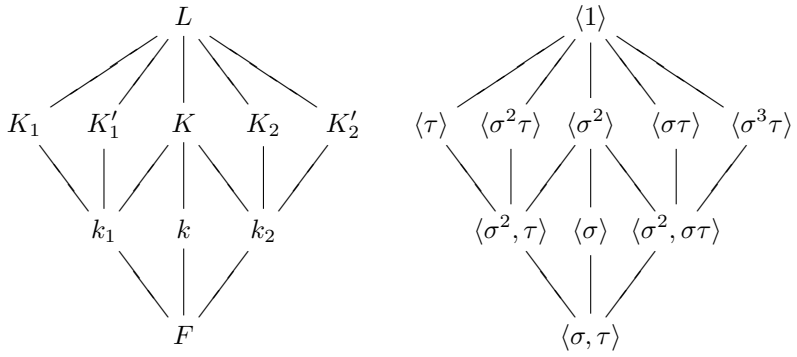
i) L/F is normal with Galois group $\operatorname{Gal}(L/F) \simeq D_4$, and L/k is the cyclic quartic extension in L/F;

ii) there exists a "C_4-factorization" $d = \operatorname{sep}(k/F) = d_1 \cdot d_2$ of d into separants d_1, d_2 such that

a) $(d_1, d_2) = 1$;

b) $(d_1/\mathfrak{p}_2) = (d_2/\mathfrak{p}_1) = +1$ for all prime ideals $\mathfrak{p}_1 \mid d_1$ and $\mathfrak{p}_2 \mid d_2$.

Diagram 1



On the other hand, if $d = d_1 \cdot d_2$ is a C_4-factorization, let δ_j be a representative of d_j, $j = 1, 2$; then the diophantine equation

$$X^2 - \delta_1 Y^2 - \delta_2 Z^2 = 0 \tag{4.1}$$

is solvable in $\mathcal{O}_F$. For any solution $(x, y, z) \in \mathcal{O}_F^3$ of (4.1), put $\mu = x + y\sqrt{\delta_1}$ and $\nu = 2(x - z\sqrt{\delta_2})$; then $L = k(\sqrt{d_1}, \sqrt{\mu}\,) = k(\sqrt{d_2}, \sqrt{\nu}\,)$ is a cyclic quartic extension of k, which is unramified outside 2∞; moreover, L/F is normal and $\mathrm{Gal}\,(L/F) \simeq D_4$.

If $\mathrm{SCl}(F) = 1$ (that is, if F is totally real and has odd class number in the strict sense, cf. Ch. 3), we can choose the solutions to (4.1) in such a way that L/k becomes unramified at all finite primes.

This implies the criterion of Rédei-Reichardt as a

Corollary 4.2.2. *Suppose that $\mathrm{SCl}(F) = 1$ and let k/F be a quadratic extension with separant d; then the following assertions are equivalent:*

a) there exists a C_4-factorization $d = d_1 \cdot d_2$;

b) there exists an unramified C_4-extension of k.

The question whether these extensions are ramified at the infinite primes will be answered in Sect. 4.3

Proof of Theor. 4.2.1. The fact that L/F is normal follows from [507]; a direct proof runs as follows: $\mathrm{Gal}\,(L/k)$ is cyclic of order 4, and corresponds via Artin's reciprocity law to a subgroup H of index 4 in $\mathrm{Cl}(k)$ which is defined by $H = \ker\left\{\left(\frac{L/k}{\cdot}\right) : \mathrm{Cl}(k) \longrightarrow \mathrm{Gal}\,(L/k)\right\}$. Moreover, $\left(\frac{L/k}{c}\right) = \left(\frac{L/k}{\mathfrak{p}}\right)$, where $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_k$ generating the ideal class $c \in \mathrm{Cl}(k)$. If c generates $Cl(k)/H$, then $\mathrm{Gal}\,(L/k)$ is generated by the Artin symbol $\sigma = \left(\frac{L/k}{c}\right)$. Let τ denote the non-trivial automorphism of k/F, and let $\tilde{\tau}$ be an extension of τ to some normal closure of L/F; then L/F is normal if and only if $\tilde{\tau}^{-1}\sigma\tilde{\tau}$ is a power of σ. Letting automorphisms act on the right, we find $\tilde{\tau}^{-1}\sigma\tilde{\tau} = \left(\frac{L/k}{c^\tau}\right) = \sigma^{-1}$: to see this, observe that the ideal class $c^{1+\tau}$ is generated by an ideal from $\mathcal{O}_F$ and hence has odd order; since $Cl(k)/H \simeq \mathbb{Z}/4\mathbb{Z}$, we must have $c^{1+\tau} \in H$. But H is the kernel of the Artin symbol, and this shows that $\left(\frac{L/k}{c^{1+\tau}}\right) = 1$.

So far we know that L/F is Galois, and that $\mathrm{Gal}\,(L/F) = \langle\sigma, \tilde{\tau}\rangle$. We also know that σ has order 4, and that $[\sigma, \tilde{\tau}] = \sigma^2$. It remains to show that $\tilde{\tau}$ has order 2. To this end we observe that $\tau = \left(\frac{k/F}{\mathfrak{p}}\right)$ for some prime ideal $\mathfrak{p}$ which is inert in k/F (exactly the split primes are in the kernel of the Artin symbol). Write $\tilde{\tau} = \left(\frac{L/F}{\mathfrak{P}}\right)$ for some extension $\mathfrak{P}$ of $\mathfrak{p}$ to $\mathcal{O}_L$. Then by well known properties of the Artin symbol (for example, see [627], II, V', p. 9) we find $\tilde{\tau}^2 = \left(\frac{L/k}{\mathfrak{p}}\right)$, and this automorphism is trivial because the ideal class generated by $\mathfrak{p}$ has odd order, hence lies in H.

We have seen that $\mathrm{Gal}\,(L/F) \simeq D_4$; therefore L/F contains three quadratic extensions; one of them is, of course, k/F, and the other two will be denoted k_1 and k_2. Since k_1k/k and k_2k/k are unramified at the finite primes, Prop. 3.3.2.1 shows that $d = \mathrm{sep}(k/F)$ is the product of two separants $d_1 = \mathrm{sep}(k_1/F)$ and $d_2 = \mathrm{sep}(k_2/F)$, and that $(d_1, d_2) \mid \infty$.

If $\mathfrak{p}$ were an infinite prime dividing both d_1 and d_2, then $\mathfrak{p}$ would ramify in k_1 and k_2, hence in K/k. But L/k is cyclic of order 4, and primes ramifying in K/k have inertia field k in L, so $\mathfrak{p}$ must also ramify in L/K: this is obviously nonsense for infinite primes, and we see that $(d_1, d_2) = 1$.

In order to show that $(d_1/\mathfrak{p}_2) = +1$ for all prime ideals $\mathfrak{p}_2$ dividing d_2, we have to study the decomposition groups $Z = Z_{\mathfrak{P}}(L/F)$ of the prime ideals $\mathfrak{P}$ above $\mathfrak{p}$ in L/F. Suppose that $\mathfrak{p}_2 \mid d_2$; then $\mathfrak{p}_2$ ramifies in k_2/F, and the inertia subgroup $T = T_{\mathfrak{P}}(L/F)$ has the following properties:

1. T has order 2: this is clear, because $\mathfrak{p}$ has ramification index 2 in L/F (recall that L/k is unramified);
2. $T \subseteq U = \langle \sigma\tau, \sigma^2 \rangle$: observe that $T \subseteq U$ if and only if $\mathfrak{p}$ does not ramify in the fixed field of U, which is k_1:
3. $T \cap \mathrm{Gal}\,(L/k) = \{1\}$: this is equivalent to $\mathfrak{p}$ being unramified in L/k.

The only subgroups of D_4 with these properties are $T = \langle \sigma\tau \rangle$ and $T = \langle \sigma^3\tau \rangle$. The fact that $T \lhd Z$ is normal in Z shows that Z must be a subgroup of the normalizer $\langle \sigma\tau, \sigma^2 \rangle$ of T in D_4. But $Z \subseteq \langle \sigma\tau, \sigma^2 \rangle$ implies that the fixed field k_1 of $\langle \sigma\tau, \sigma^2 \rangle$ is contained in the decomposition field of $\mathfrak{p}$ in L/F, i.e., that $\mathfrak{p}$ splits in k_1. By symmetry, we also have $(d_2/\mathfrak{p}_1) = +1$, and this proves the first part of Theor. 4.2.1. □

The proof of the second part of Theor. 4.2.1 consists of several steps:

Solvability of (4.1)

We have to show that (4.1) has local solutions, i.e., that (4.1) is solvable mod $\mathfrak{p}^\nu$ for every $\nu \in \mathbb{N}$ and every prime place $\mathfrak{p}$. For places $\mathfrak{p} \nmid d$ this is easily done (recall that the conductor of δ_j divides d), and for infinite places it can be deduced from the fact that δ_1 and δ_2 cannot both be negative at a given infinite prime $\mathfrak{p}$. Hence we may assume that $\mathfrak{p} \mid d$; making use of the norm residue symbol of Hasse, we have to show that $\left(\frac{\delta_1, \delta_2}{\mathfrak{p}}\right) = 1$. Using the formulae in [627], II, (4.) on p. 54, (14.) on p. 55, we find

$$\left(\frac{\delta_1, \delta_2}{\mathfrak{p}}\right) = \left(\frac{d_2}{\mathfrak{p}}\right)^a, \quad \text{if } \mathfrak{p}^a \parallel d_1, \text{ and}$$
$$\left(\frac{\delta_2, \delta_1}{\mathfrak{p}}\right) = \left(\frac{d_1}{\mathfrak{p}}\right)^a, \quad \text{if } \mathfrak{p}^a \parallel d_2.$$

Now the fact that $d = d_1 \cdot d_2$ is a C_4-factorization shows that the quadratic residue symbols $(d_j/\mathfrak{p}) = 1$, hence (4.1) has indeed non-trivial solutions.

Remark 7. *If $\mathfrak{p}^a \parallel d$ for some even $a = a(\mathfrak{p})$, we only used that $(d_1, d_2) = 1$; hence (4.1) is solvable under the weakened condition that $(d_1/\mathfrak{p}_2) = (d_2/\mathfrak{p}_1) = +1$ for all prime ideals $\mathfrak{p}_j$ such that $a(\mathfrak{p}_j)$ is odd. We will need the stronger property $(d_1/\mathfrak{p}_2) = 1$ for removing these $\mathfrak{p}_2 \mid 2$ from the list of ramified primes.*

$\mathrm{Gal}\,(L/F) \simeq D_4$

For computing the Galois group of L/F, we use Lemma 1.1.1.6. The relation

$$\frac{\mu}{\nu} = \frac{2(x + y\sqrt{\delta_1}\,)}{x^2 - \delta_2 y^2} = \left(\frac{x + y\sqrt{\delta_1} + z\sqrt{\delta_2}}{y\sqrt{\delta_1}}\right)^2$$

shows that indeed $k(\sqrt{d_1}, \sqrt{\mu}\,) = k(\sqrt{d_2}, \sqrt{\nu}\,)$ as claimed. We define automorphisms of L/k

$$\sigma : \sqrt{\delta_1} \longmapsto -\sqrt{\delta_1}, \qquad \sqrt{\delta_2} \longmapsto -\sqrt{\delta_2},$$
$$\tau : \sqrt{\delta_1} \longmapsto +\sqrt{\delta_1}, \qquad \sqrt{\delta_2} \longmapsto -\sqrt{\delta_2}.$$

and find $\alpha_\sigma = \mu/(z\sqrt{\delta_2}\,)$, $\varepsilon_\sigma = -1$, $\alpha_\tau = \varepsilon_\tau = 1$ and $\alpha_{\sigma\tau} = \alpha_\sigma$, $\varepsilon_{\sigma\tau} = 1$. This shows that $\mathrm{Gal}\,(L/F) \simeq D_4$.

Ramification outside 2∞

Because the class number h of F is odd, L can also be generated by the square root of μ^h. If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_F$ such that $\mathfrak{p} \mid \mu$, then $\mathfrak{p}^h \mid \mu^h$. Since $\mathfrak{p}^h = (\pi)$ is principal, and because changing μ^h by a factor in $F^\times$ does not change the Galois group of L/F, we can divide μ^h by all $\mathfrak{p}^h = (\pi)$ such that $\mathfrak{p} \mid \mu$ and arrive at a $\mu_1 \in K^\times$ which is not divisible by any prime ideal $\mathfrak{p} \lhd \mathcal{O}_F$. In particular, L/k is unramified outside 2∞ for $L = K(\sqrt{\mu_1})$, and it is obvious that μ_1 corresponds to a solution of (4.1), hence we may assume without loss of generality that $\mu = \mu_1$.

Ramification above 2 if $\mathrm{SCl}(F) = 1$

Before we start removing the ramification above 2, we recall the part of the decomposition law for relative quadratic extensions which we will need:

(†) Let $k = F(\sqrt{\mu})$ be a quadratic extension of a number field F; let $\mathfrak{p} \mid 2$ be a prime ideal in $\mathcal{O}_F$, and suppose that $\mathfrak{p} \nmid \mu$ and $\mathfrak{p}^m \parallel 2$. Then

- $\mathfrak{p}$ splits if $\mu \equiv \xi^2 \bmod \mathfrak{p}^{2m+1}$ for some $\xi \in \mathcal{O}_F$;
- $\mathfrak{p}$ does not ramify if $\mu \equiv \xi^2 \bmod \mathfrak{p}^{2m}$ for some $\xi \in \mathcal{O}_F$;
- $\mathfrak{p}$ ramifies if $\mu \equiv \xi^2 \bmod \mathfrak{p}^{2m}$ is not solvable in $\mathcal{O}_F$.

We are now in the following situation: we have found a solution to (4.1) corresponding to a $\mu \in \mathcal{O}_F$ which has no prime ideal divisors from $\mathcal{O}_F$. We want to show that there is a unit $\varepsilon \in E_F$ such that $L' = K(\sqrt{\mu\varepsilon})$ is a C_4-extension of k unramified outside ∞. The Galois group of $K(\sqrt{\mu})/F$ does not change when we multiply μ with an $r \in F^\times$, and neither does ramification outside 2∞ if $r \in E_F$, hence we only need to take care of the ramification above 2.

We will begin with the prime ideals $\mathfrak{p} \mid d$ above 2 and will assume without loss of generality that $\mathfrak{p} \mid d_2$; since $d = d_1 \cdot d_2$ is a C_4-factorization, $\mathfrak{p} = \mathfrak{P}\mathfrak{P}'$ splits in k_1. Moreover, $\mathfrak{P}$ and $\mathfrak{P}'$ ramify in K/k_1, and L/K is unramified at $\mathfrak{P}$ if and only if $\mathfrak{P}$ does not ramify in one of K_1/k_1 or K_1'/k_1. Suppose it does; then $\mathfrak{p} \nmid \mu$ shows that $\mathfrak{P} \nmid \mu$ or $\mathfrak{P}' \nmid \mu$; changing the roles of μ and μ' if necessary we may assume that $\mathfrak{P} \nmid \mu$. $\mathfrak{P}$ has inertia degree 1 over F, hence for every $m \in \mathbb{N}$ there exists an $\alpha \in \mathcal{O}_F$ such that $\mu \equiv \alpha \bmod \mathfrak{P}^{2m}$. Choose $m \in \mathbb{N}$ as in (†) above; then Prop. 3.3.4.1 guarantees the existence of a unit $\varepsilon \in E_F$ such that

a) $\alpha\varepsilon \equiv \xi^2 \bmod \mathfrak{p}^{2m}$, and

b) $\mathfrak{p}$ is the only prime ideal ramifying in $F(\sqrt{\varepsilon})/F$.

This implies that $\mu\varepsilon \equiv \alpha\varepsilon \equiv \xi^2 \bmod \mathfrak{P}^{2m}$, so $\mathfrak{P}$ does not ramify in the quadratic extension $k_1(\sqrt{\mu\varepsilon})/k_1$. This procedure does not change the ramification outside $\mathfrak{p}\infty$ and may be applied repeatedly to all $\mathfrak{p}$ dividing both 2 and d.

Next assume that $\mathfrak{p} \mid 2$ does not ramify in K; if $\mathfrak{p}$ splits in k_1/F or k_2/F, then the same procedure as above reduces possible ramification at $\mathfrak{p}$ without damaging ramification at other finite places. Hence we are left to consider the case when $\mathfrak{p}$ is inert in k_1/F and k_2/F. Since $\mathfrak{p}$ does not ramify in k_2, the congruence $\delta_2 \equiv \xi^2 \bmod \mathfrak{p}^{2m}$ is solvable, hence so is $N_1\mu = \mu\mu' = x^2 - \delta_1 y^2 = \delta_2 z^2 \equiv \xi^2 \bmod \mathfrak{p}^{2m}$. Now we need

Lemma 4.2.3. *Suppose that* $\mathrm{SCl}(F) = 1$*, let* $\mathfrak{p} \mid 2$ *be a prime ideal in* $\mathcal{O}_F$*, and suppose that* $\mathfrak{p}$ *is inert in a quadratic extension* K/F*; moreover, assume that* $\mathfrak{p} \nmid \alpha \in \mathcal{O}_K$*, and put* $L = K(\sqrt{\alpha\alpha'})$*. If the congruence* $N_{K/F}\alpha \equiv \xi^2 \bmod \mathfrak{p}^{2m}$ *is solvable, then there exist* $a \in \mathcal{O}_F$ *and* $\beta \in \mathcal{O}_L$ *such that* $\alpha \equiv a\beta^2 \bmod \mathfrak{p}^{2m}$*.*

Lemma 4.2.3 implies that $\mu \equiv a\beta^2 \bmod \mathfrak{p}^{2m}$ for some $a \in \mathcal{O}_F$; Prop. 3.3.4.1 shows the existence of a unit $\varepsilon \in E_F$ such that $a\varepsilon$ is a square mod $\mathfrak{p}^{2m}$ without changing the ramification outside $\mathfrak{p}\infty$. Replacing μ by $\mu\varepsilon$, we have removed the ramification at $\mathfrak{p}$.

Proof of Lemma 4.2.3. We first find a $\gamma \in \mathcal{O}_K \setminus \mathfrak{p}$ such that $\mathfrak{p} \nmid Tr_{K/F}(\alpha\gamma^2)$. If $\mathfrak{p} \nmid (\alpha + \alpha')$, then $\gamma = 1$ does the trick. Hence assume that $\mathfrak{p} \mid Tr_{K/F}(\alpha)$ and recall that $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_F/\mathfrak{p}$ are finite fields. The trace map $Tr : \mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_F/\mathfrak{p}$ is onto, hence here is a $\gamma \in \mathcal{O}_K \setminus \mathfrak{p}$ such that $Tr(\gamma) \equiv 1 \bmod \mathfrak{p}$. Now

$\mathfrak{p} \mid (\alpha+\alpha')$ and $\mathfrak{p} \mid 2$ imply that $\alpha\gamma^2 + \alpha'\gamma'^2 \equiv \alpha(\gamma+\gamma')^2 \equiv \alpha \bmod \mathfrak{p}$. Replacing α by $\alpha\gamma^2$ if necessary, we may assume that $\mathfrak{p} \nmid (\alpha+\alpha')$.

Now we see that $\mathfrak{p} \nmid \alpha(\alpha+\alpha'+2\alpha\alpha')$; the assumption $\alpha\alpha' \equiv \xi^2 \bmod \mathfrak{p}^{2m}$ implies that $\sqrt{\alpha\alpha'} \equiv \xi \bmod \mathfrak{p}^m$, hence $\mathfrak{p}^m \mid 2$ shows that $2\sqrt{\alpha\alpha'} \equiv 2\xi \bmod \mathfrak{p}^{2m}$, and we see that $\alpha+\alpha'+2\sqrt{\alpha\alpha'} \equiv a \bmod \mathfrak{p}^{2m}$ for some $a \in \mathcal{O}_F$. The claimed congruence now follows from the identity $\alpha(\alpha+\alpha'+2\sqrt{\alpha\alpha'}) = (\alpha+\sqrt{\alpha\alpha'})^2$. □

Remark 8. *The conditions in Theor. 4.3.3 cannot be weakened; in particular, its assertions do not hold if* $\mathrm{SCl}(F) \neq 1$ *or if* $d = d_1 \cdot d_2$ *is not a* C_4*-factorization:*

1. *Let* $F = \mathbb{Q}(i)$, $i^2 = -1$*; we have shown in Ch. 3 that* $\mathrm{SCl}(F) \simeq \mathbb{Z}/2\mathbb{Z}$*. Put* $\pi = 1+4i$, $\rho = 5+4i$*: then* $d = \pi \cdot \rho$ *is a* C_4*-factorization and* $L = F(i, \sqrt{\pi}, \sqrt{\rho}, \sqrt{2+\sqrt{\rho}})$ *is a dihedral extension of* F*, unramified outside* 2∞*, but there does not exist an unramified* C_4*-extension of* $k = F(\sqrt{d})$ *because* $h(k) = 2$*.*

2. *Let* $F = \mathbb{Q}$ *and* $k = \mathbb{Q}(\sqrt{-5})$*; then* $\mathrm{SCl}(F) = 1$*, but* $d = -20 = -4 \cdot 5$ *is no* C_4*-factorization (because* $(\frac{5}{2}) = -1$*). Although* $L = \mathbb{Q}(i, \sqrt{5}, \sqrt{1+2i})$ *is a dihedral extension of* $\mathbb{Q}$ *such that* L/k *is unramified outside* 2∞*, there is no unramified* C_4*-extension of* k *because* $h(k) = 2$*.*

   The existence of the C_4*-extension* L/k *could have been predicted by Remark 7, because* $2^m \parallel d_1 = -4$*, where* $m = 2$ *is even.*

Halter-Koch [353] has shown that the criterion of Rédei and Reichardt implies an inequality due to Damey and Payan [317] on the 4-ranks of the ideal class groups of $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{-m})$; the results proved in this section allow us to generalize Halter-Koch's proof to all base fields F such that $\mathrm{SCl}(F) = 1$. We will not give any details, however, because Oriat [344] was able to generalize these inequalities to arbitrary number fields F (this seems to indicate that there may be an extension of the theory of separants to arbitrary number fields F).

For examples of unramified C_4-extensions of quadratic extensions of $F = \mathbb{Q}$ we refer the reader to Fueter [5] or Herz [24]; we will, however, give a few less trivial examples:

$F = \mathbb{Q}(\sqrt{2})$

d	d_1	d_2	α
$85+36\sqrt{2}$	$7+2\sqrt{2}$	$11+2\sqrt{2}$	$-11-6\sqrt{2}+(2+2\sqrt{2})\sqrt{11+2\sqrt{2}} \ll 0$
113	$11+2\sqrt{2}$	$11-2\sqrt{2}$	$10+5\sqrt{2}+\sqrt{11+2\sqrt{2}} \gg 0$
$253+120\sqrt{2}$	$13+4\sqrt{2}$	$17+4\sqrt{2}$	$25-14\sqrt{2}+(8-6\sqrt{2})\sqrt{13+4\sqrt{2}} \gg 0$

$F = \mathbb{Q}(\sqrt{5})$

d	d_1	d_2	α
-19	$-1+2\sqrt{5}$	$-1-2\sqrt{5}$	$\sqrt{5}+(1-\sqrt{5})\sqrt{-1+2\sqrt{5}}$
$97+36\sqrt{5}$	$7+2\sqrt{5}$	$11+2\sqrt{5}$	$-12-17\sqrt{5}+(1+\sqrt{5})\sqrt{11+2\sqrt{5}} \ll 0$

Remark 9. *Rédei and Reichardt also showed how to construct unramified cyclic extensions of* 2*-power degree* ≥ 8*; their ideas can be extended to fields* F *such that* $\mathrm{SCl}(F) = 1$ *(see [115]), and the construction is feasible for* $F = \mathbb{Q}$ *and* $n = 8$*.*

4.3 Scholz's reciprocity law

Now we will study the question whether the unramified cyclic extensions constructed in Sect. 4.2 are ramified at the infinite primes. In the special case $F = \mathbb{Q}$, this has been done by Scholz [535], and as a byproduct he found the reciprocity law that today bears his name. It turns out that something similar can be achieved over fields with $\mathrm{SCl}(F) = 1$.

Let k/F be a quadratic extension, E_k the unit group of $\mathcal{O}_k$, $(\cdot/\cdot)$ and $[\cdot/\cdot]$ the quadratic residue symbol in F and k, respectively. If $\alpha \in F^\times$ and if $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_F$ such that $\mathfrak{p}\mathcal{O}_k = \mathfrak{P}\mathfrak{P}'$ then it is easy to see that $[\alpha/\mathfrak{P}] = (\alpha/\mathfrak{p})$. For a prime ideal $\mathfrak{p}$ such that

a) $(\varepsilon/\mathfrak{p}) = +1$ for every unit $\varepsilon \in E_F$;

b) $\mathfrak{p} = \mathfrak{P}\mathfrak{P}'$ splits in k/F;

we define a symbol $(E_k/\mathfrak{p})$ by

$$(E_k/\mathfrak{p}) = \begin{cases} +1 & \text{if } [\eta/\mathfrak{P}] = +1 \text{ for all } \eta \in E_k, \\ -1 & \text{if } [\eta/\mathfrak{P}] = -1 \text{ for some } \eta \in E_k. \end{cases}$$

This symbol $(E_k/\mathfrak{p})$ does not depend on the choice of $\mathfrak{P}$ because

$$[\eta/\mathfrak{P}][\eta/\mathfrak{P}'] = [\eta\eta'/\mathfrak{P}] = (N_{k/F}\eta/\mathfrak{p}) = +1.$$

Now we can state

Proposition 4.3.1. *Let F be a number field with $\mathrm{SCl}(F) = 1$, $d \gg 0$ a separant such that $(2, d) = 1$, $k = F(\sqrt{d})$, $d = d_1 \cdot d_2$ a C_4-factorization of d into totally positive prime separants d_1, d_2, and let L/k be the corresponding cyclic quartic extension of k which is unramified outside ∞. Moreover, let $\mathfrak{p}_i$, $i = 1, 2$, denote the prime ideal in $\mathcal{O}_F$ such that $\mathfrak{p}_i \mid d_i$, and let E_i be the unit group of $k_i = F(\sqrt{d_i})$. Then $(\varepsilon/\mathfrak{p}) = 1$ for all units $\varepsilon \in E_F$ and all $\mathfrak{p} \mid d$, and the following assertions are equivalent:*

i) L is totally real, i.e., L/k is unramified at ∞;

ii) the ray class number of $\mathcal{O}_1 \bmod \mathfrak{P}_2$ is even, where $\mathfrak{P}_2$ is a prime ideal above $\mathfrak{p}_2$ in $\mathcal{O}_1 = \mathcal{O}_{k_1}$;

iii) $(E_1/\mathfrak{p}_2) = +1$, i.e., every unit in E_1 is a quadratic residue $\bmod \mathfrak{P}_2$.

Prop. 4.3.1 enables us to deduce a weak reciprocity law as a

Corollary 4.3.2. *Under the assumptions of Prop. 4.3.1 we have $(E_1/\mathfrak{p}_2) = (E_2/\mathfrak{p}_1)$.*

Proof. Proof of Prop. 4.3.1 We want to prove that $(\varepsilon/\mathfrak{p}) = 1$ for all units $\varepsilon \in E_F$; to this end, assume that $\mathfrak{p} \mid d_1$. Our assumption $(d, 2) = 1$ guarantees that $\mathfrak{p}$ does not ramify in $F(\sqrt{\varepsilon})/F$, hence formula (4) in [627], II §11, gives

$$\Big(\frac{\varepsilon}{\mathfrak{p}}\Big) = \Big(\frac{d_1, \varepsilon}{\mathfrak{p}}\Big).$$

Now $\mathfrak{p}$ is the only ramified place in k_1/F, and since units are norm residues at all unramified primes, the product formula of the norm residue symbol shows

$$1 \;=\; \prod_{\mathfrak{q}} \Big(\frac{d_1, \varepsilon}{\mathfrak{q}}\Big) \;=\; \Big(\frac{d_1, \varepsilon}{\mathfrak{p}}\Big) \;=\; \Big(\frac{\varepsilon}{\mathfrak{p}}\Big).$$

i) $\Rightarrow$ ii): The extension L/k_1 has Galois group V_4 and subfields K_1, K_1' and $K = F(\sqrt{d_1}, \sqrt{d_2})$. If L/k is unramified at ∞, then so are K_1/k_1 and K_1'/k_1. In the proof of Theor. 4.2.1 we have seen that exactly one of the prime ideals $\mathfrak{P}$, $\mathfrak{P}'$ above $\mathfrak{p}_2$, say $\mathfrak{P}$, ramifies in K_1/k_1: hence K_1 is contained in the ray class field mod $\mathfrak{P}^f$ of k_1 for some $f \geq 1$. But $(d, 2) = 1$ guarantees tame ramification, hence we have $f = 1$, and this is the claim.

ii) $\Rightarrow$ i): Assume that the ray class number mod $\mathfrak{P}$ in k_1 is even; then there is a quadratic extension K_1/k_1 which is unramified outside $\mathfrak{P}$, and since k_1 has odd class number in the strict sense, $\mathfrak{P}$ is indeed ramified. If K_1/k were normal, then $\mathfrak{P}'$ would also be ramified in K_1/k, thus K_1/k is not normal. The normal closure L of a non-normal quartic field containing a quadratic subfield is necessarily dihedral. L/k is unramified because $\mathrm{diff}\,(L/K)$ divides both $\mathrm{diff}\,(K_1/k_1) = \mathfrak{P}$ and $\mathrm{diff}\,(K_1'/k_1) = \mathfrak{P}'$; the cyclic quartic extension in L/F is L/k: if L/k_2 were cyclic, L/K would ramify above $\mathfrak{p}_1$.

ii) $\iff$ iii): The ray class number $h(\mathfrak{P})$ of $\mathcal{O}_1$ mod $\mathfrak{P} = \mathfrak{P}_2$ is given by the formula

$$h(\mathfrak{P}) = h(F) \cdot \frac{\Phi(\mathfrak{P})}{(E_1 : E_1^{(1)})},$$

where Φ denotes Euler's Phi-function in $\mathcal{O}_1$, and where $E_1^{(1)}$ denotes the subgroup of units in E_1 which are $\equiv 1$ mod $\mathfrak{P}$. We want to show that $h(\mathfrak{P})$ is even if and only if $(E_1/\mathfrak{p}_2) = 1$. To this end we define a homomorphism $\psi : E_1 \longmapsto (\mathcal{O}/\mathfrak{P}\mathcal{O})^\times =: R_\mathfrak{P}$ by $\psi(\varepsilon) = \varepsilon$ mod $\mathfrak{P}$ and note that ψ has kernel $E_1^{(1)} = \{\varepsilon \in E_1 : \varepsilon \equiv 1 \bmod \mathfrak{P}\}$. Since $R_\mathfrak{P}$ is isomorphic to the multiplicative group of a finite field, it is cyclic. Therefore the index $(R_\mathfrak{P} : \psi(E_1))$ is even if and only if $\psi(\varepsilon) \equiv \xi^2$ mod $\mathfrak{P}$ for all units $\varepsilon \in E_1$. This, together with the fact that $R_\mathfrak{P}$ has order $\Phi(\mathfrak{P})$, shows that the ray class number $h(\mathfrak{P})$ is even if and only if $(\varepsilon/\mathfrak{P}) = 1$ for all units $\varepsilon \in E_1$. In fact, the exact sequence

$$1 \longrightarrow E_1^{(1)} \longrightarrow E_1 \longrightarrow R_\mathfrak{P} \longrightarrow R_\mathfrak{P}/\psi(E_1) \longrightarrow 1$$

shows that $(R_\mathfrak{P} : \psi(E_1)) = \Phi(\mathfrak{P})/(E_1 : E_1^{(1)})$.

□

Already the weak reciprocity formula of Cor. 4.3.2 contains Scholz's reciprocity law (for a history on the subject, see the survey of E. Lehmer [635]) as a special case:

Example 4.3.1. *Scholz's Reciprocity Law for $F = \mathbb{Q}$ Let $p \equiv q \equiv 1$ mod 4 be primes such that $(p/q) = 1$, and let ε_p and ε_q denote the fundamental units in $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$, respectively. Then $(p) = \mathfrak{p}\mathfrak{p}'$ in $\mathbb{Q}(\sqrt{q})$ and $(q) = \mathfrak{q}\mathfrak{q}'$ in $\mathbb{Q}(\sqrt{p})$, and we have $[\varepsilon_p/\mathfrak{q}] = [\varepsilon_q/\mathfrak{p}]$.*

It is easily seen that $[\varepsilon_p/\mathfrak{q}]$ does not depend on the choice of ε_p or $\mathfrak{q}$, so we usually write (ε_p/q) instead of $[\varepsilon_p/\mathfrak{q}]$.

Surprisingly, such an explicit form of Scholz reciprocity holds in general: assume that $\mathrm{SCl}(F) = 1$, and let $d_1, d_2 \gg 0$ be prime separants; then a prime ideal $\mathfrak{p}_2 \mid d_2$ splits in $\mathcal{O}_1 = \mathcal{O}_{k_1}$, i.e, $\mathfrak{p}_2\mathcal{O}_1 = \mathfrak{P}_2\mathfrak{P}_2'$. The key observation now is that the quadratic residue character $[\varepsilon_1/\mathfrak{P}_2]$ of a unit $\varepsilon_1 \in E_1$ only depends on $\eta = N_1\varepsilon_1$ (where N_1 denotes the norm of k_1/F). More precisely:

1. $[\varepsilon_1/\mathfrak{P}_2]$ does not depend on the choice of $\mathfrak{P}$: to see this, note that we have, directly from the definition of the quadratic residue symbol, $[\alpha/\mathfrak{P}] = [\alpha'/\mathfrak{P}']$, and this shows that

$$[\varepsilon_1/\mathfrak{P}_2] \cdot [\varepsilon_1/\mathfrak{P}_2'] = [\varepsilon_1/\mathfrak{P}_2] \cdot [\varepsilon_1'/\mathfrak{P}_2] = [N_1\varepsilon_1/\mathfrak{P}_2] = (N_1\varepsilon_1/\mathfrak{p}_2) = 1$$

because of Prop. 4.3.1.

2. Units in E_1 with the same norm have the same quadratic residue character mod $\mathfrak{P}_2$: to prove this it is sufficient to show that $[\varepsilon/\mathfrak{P}_2] = 1$ for all units $\varepsilon \in E_1$ such that $N_1\varepsilon = 1$. Hilbert's Satz 90 says that $N\varepsilon = 1 \iff \varepsilon = \xi^{\sigma-1}$ for some $\xi \in k_1^\times$. This shows that (ξ) is an ambigous ideal of k_1; but the only ramified ideal in k_1/F is $\mathfrak{p}$, hence we must have $(\xi) = \mathfrak{a}$ or $(\xi) = \sqrt{d_1}\mathfrak{a}$ for some fractional ideal $\mathfrak{a}$ in F. Obviously, $\mathfrak{a}$ is principal, and we find that $\varepsilon = \pm\upsilon^{\sigma-1}$ for some unit $\upsilon \in E_1$. But now $[\upsilon/\mathfrak{P}_2] = [\upsilon/\mathfrak{P}_2'] = [\upsilon^\sigma/\mathfrak{P}_2]$ shows that indeed $[\varepsilon/\mathfrak{P}_2] = 1$ as claimed.

This allows us to associate characters X_1, X_2 on E_F to every C_4-factorization $d = d_1d_2$ into a pair of prime separants $d_1, d_2 \gg 0$ as follows: for a unit $\eta \in E_F$, choose a unit $\varepsilon \in E_1$ such that $N_1\varepsilon = \eta$ (this is always possible; see Ch. 3) and define $X_1(\eta) = [\varepsilon/\mathfrak{P}_2]$.

Theorem 4.3.3. *(Scholz's Reciprocity Law) Let F be a number field such that $\mathrm{SCl}(F) = 1$, and suppose that $d = d_1d_2$ is a C_4-factorization of d into prime separants $d_1, d_2 \gg 0$. Then $X_1(\eta) = X_2(\eta)$ for every unit $\eta \in E_F$. Moreover, we have $X_j(\eta) = 1$ if η is the norm of a unit from $k = F(\sqrt{d})$.*

Proof. Assume that $\eta = N_{k/F}\varepsilon$; since K/k is unramified and $Cl_2(k)$ is cyclic, ε is the norm of a unit in E_K, say $\varepsilon = N_{K_k}\upsilon$. Put $\varepsilon_1 = N_{K/k_1}\upsilon$; then $N_1\varepsilon_1 = \eta = N_1\varepsilon$, hence $(\varepsilon/\mathfrak{p}_2) = X_1(\eta) = (\varepsilon_1/\mathfrak{p}_2)$. But

$(\varepsilon_1/\mathfrak{p}_2) = +1$, because ε_1 is norm from K and $\mathfrak{p}$ ramifies in K/k_1. We have shown that $\eta = N_{k/F}\varepsilon \Rightarrow X_1(\eta) = 1$. By symmetry, we also have $X_2(\eta) = 1$.

Our next claim is that $(E_F : N_{k/F}E_k) \leq 2$. To prove this, let $C_{am}^{(2)}$ denote the 2-Sylow subgroup of the group of strongly ambiguous ideal classes of k; it is known that [627]

$$|C_{am}^{(2)}| = \frac{1}{2} \cdot \frac{\prod^{\infty} e(\mathfrak{p})}{(E_F : NE_k)},$$

where $\prod^{\infty}$ indicates that the product runs over all primes including the infinite ones. On the other hand, there are at most $(k_{gen}^{(2)} : k)$ ambiguous ideal classes, where $k_{gen}^{(2)}$ denotes the maximal 2-extension contained in the genus field k_{gen} of k; since $k_{gen}^{(2)} = k(\sqrt{d_1}\,)$, we find that $|C_{am}^{(2)}| \leq 2$. But now $\prod^{\infty} e(\mathfrak{p}) = 4$, because only $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are ramified, hence we have $(E_F : N_{k/F}E_k) \leq 2$ as claimed.

In case we have $(E_F : N_{k/F}E_k) = 1$, there is nothing left to prove, because then every unit is the norm of a unit from E_k; assume therefore that $(E_F : N_{k/F}) = 2$, and let $\eta \in E_F \setminus N_{k/F}E_k$. If Theor. 4.3.3 is false, we must have $X_1(\eta) = -X_2(\eta)$; but if $X_1(\eta) = 1$, then $(E_1/\mathfrak{p}_2) = +1$, whereas $X_2(\eta) = -1$ implies $(E_2/\mathfrak{p}_1) = -1$, and this contradicts Prop. 4.3.1. □

Example 4.3.2. *Let $F = \mathbb{Q}(\sqrt{2}\,)$, $d_1 = 7 + 2\sqrt{2}$, $d_2 = 11 + 2\sqrt{2}$, and $\omega = -1 + \sqrt{2}$. We find $\mathfrak{Q}_1 = (\frac{1}{2}(7 + 2\sqrt{2} + \sqrt{d}\,))$, $\mathfrak{Q}_2 = (\frac{1}{2}(11 + 2\sqrt{2} + \sqrt{d}\,))$, where $\mathfrak{p}\mathcal{O}_k = \mathfrak{Q}_j^2$. Moreover we have the following generators for the prime ideals $\mathfrak{P}_j$ above $\mathfrak{p}_j$ in*

k_1 *:* $\mathfrak{P}_2 = (1 + \sqrt{2} + \sqrt{2}\sqrt{d_1}\,)$, $\sqrt{d_1} \equiv 30 \bmod \mathfrak{P}_2$, $\sqrt{2} \equiv 51 \bmod \mathfrak{P}_2$;

k_2 *:* $\mathfrak{P}_1 = (2 + \sqrt{d_2}\,)$, $\sqrt{d_2} \equiv -2 \bmod \mathfrak{P}_1$, $\sqrt{2} \equiv 17 \bmod \mathfrak{P}_1$.

Now we find

ε	$\frac{1}{2}(1 + \sqrt{2} + \sqrt{d_1}\,)$	$\frac{1}{2}(3 + \sqrt{2} + \sqrt{d_1}\,)$	$(3 + \sqrt{d_2}\,)/\sqrt{2}$	$(2\sqrt{2} + \sqrt{d_2}\,)\omega$
$\eta = N\varepsilon$	-1	ω	$+\omega$	-1
$X_j(\eta)$	$+1$	-1	-1	$+1$

This shows that $X_1(-1) = X_2(-1) = 1$, $X_1(\omega) = X_2(\omega) = -1$. Together with Theor. 4.4.1 below, this explains why the 2-class field constructed in the example at the end of the previous section was totally complex.

4.4 Governing Fields

Almost all of Scholz's results in [535] can similarly be generalized to fields with $\mathrm{SCl}(F) = 1$; in particular this is true for Scholz's construction of the *governing field* (cf. [539]) of $8 \mid h^+(pq)$:

Theorem 4.4.1. *Let F be a field such that $\mathrm{SCl}(F) = 1$, $k = F(\sqrt{d}\,)$, and suppose that $d = d_1d_2$ for prime separants $d_1, d_2 \gg 0$ such that $(d, 2)$. Let $\mathrm{Spl}(K/F)$ denote the set of prime ideals in $\mathcal{O}_F$ which split in K/F. Then*

1. *$(d_1/\mathfrak{p}_2) = -1 \Rightarrow h^+(k) = h(k) \equiv 2 \bmod 4$, and $E_F = NE_k$;*

2. *$(d_1/\mathfrak{p}_2) = +1 \Rightarrow (E_1/\mathfrak{p}_2) = (E_2/\mathfrak{p}_1)$, and we distinguish*

2.1. *$(E_1/\mathfrak{p}_2) = -1$: then $h^+(k) = 2h(k) \equiv 4 \bmod 8$ and $(E_F : NE_k) = 2$;*

2.2. *$(E_1/\mathfrak{p}_2) = +1$: then $(d_1/\mathfrak{p}_2)_4 = (d_2/\mathfrak{p}_1)_4$, and there exist two possibilities:*

a) *$(d_1/\mathfrak{p}_2)_4 = (d_2/\mathfrak{p}_1)_4 = -1$:*

then $h^+(k) = h(k) \equiv 4 \bmod 8$ and $E_F = NE_k$;

b) *$(d_1/\mathfrak{p}_2)_4 = (d_2/\mathfrak{p}_1)_4 = +1$:*

then $h^+(k) \equiv 0 \bmod 8$, *the quartic cyclic unramified extension of* k *is real, and* $E_F = NE_k$ *if and only if the* 2*-class field* k^1 *of* k *is real.*

If we fix d_1, *we have in particular*

$$\begin{array}{lll} 4 \mid h^+(k) & \iff \mathfrak{p}_2 \in \mathrm{Spl}(\Omega_4^+(d_1)/F), & \text{where} \quad \Omega_4^+(d_1) = F(\sqrt{E_F}, \sqrt{d_1}\,); \\ 4 \mid h(k) & \iff \mathfrak{p}_2 \in \mathrm{Spl}(\Omega_4(d_1)/F), & \text{where} \quad \Omega_4(d_1) = F(\sqrt{E_1}, \sqrt{d_1}\,); \\ 8 \mid h^+(k) & \iff \mathfrak{p}_2 \in \mathrm{Spl}(\Omega_8^+(d_1)/F), & \text{where} \quad \Omega_8^+(d_1) = F(\sqrt{E_1}, \sqrt[4]{d_1}\,). \end{array}$$

We note in passing that the material of this section is related to some results of Hilbert [621], Satz 32, 33, on the quadratic reciprocity law in fields with odd class number.

4.5 Unramified Dihedral Extensions

The same methods used to construct unramified cyclic extensions in Sect. 4.2 allow us to prove

Theorem 4.5.1. *Let* F *be a number field with odd class number,* k/F *a quadratic extension, and* L/k *an unramified* D_4*-extension such that* L/F *is normal. Then* $\mathrm{Gal}\,(L/F) \simeq C_2 \times D_4$, *and there exists a "*$D_4$*-factorization"* $d = \mathrm{sep}(k/F) = d_1 d_2 \cdot d_3$ *into separants such that*

(i) $(d_i, d_j) \mid \infty$ *for* $i \neq j$, *and* $(d_1, d_2) = 1$;

(ii) $(d_1/\mathfrak{p}_2) = (d_2/\mathfrak{p}_1) = +1$ *for all prime ideals* $\mathfrak{p}_1 \mid d_1$ *and* $\mathfrak{p}_2 \mid d_2$. *Here*

Moreover, $L/k(\sqrt{d_j}\,)$ *is cyclic for* $j = 3$ *and of type* V_4 *for* $j = 1, 2$.

If, on the other hand, k/F *is a quadratic extension with separant* $d = \mathrm{sep}(k/F)$, *and if* $d = d_1 d_2 \cdot d_3$ *is a* D_4*-factorization, then there is an* $\alpha \in k(\sqrt{d_1}\,)$ *such that* $L = k(\sqrt{d_1}, \sqrt{d_2}, \sqrt{\alpha}\,)$ *is a* D_4*-extension with the following properties:*

1. L/k *is unramified outside* 2∞;
2. $L/k(\sqrt{d_3}\,)$ *is cyclic;*
3. L/F *is normal with Galois group* $C_2 \times D_4$.

If in addition $\mathrm{SCl}(F) = 1$, *then we can find an extension* L/k *which is unramified (outside* ∞*).*

The second part of Theor. 4.5.1 follows directly from our results in Sect. 4.2: in fact, if $d = d_1 d_2 \cdot d_3$ is a D_4-factorization, then $d_1 \cdot d_2$ is a C_4-factorization of $d_1 d_2$; the corresponding unramified C_4-extension L of $F(\sqrt{d_1 d_2}\,)$ lifts to an unramified D_4-extension $M = L(\sqrt{d_3}\,)$ of k.

For the 2-groups occuring below, we will use the notation of [569]; the numbers in [569] coincide with those in [576]. For example, $G = 32.042 = \Gamma_5 a_1 = D_4 \curlyvee D_4$ is the group $\Gamma_5 a_1$ of order 32 in [569], G has number 42 in [569] and [576], and $G = D_4 \curlyvee D_4$ expresses the fact that G can be realized as a push-out of two dihedral groups of order 8.

The assumption that L/F be normal is necessary in Theor. 4.5.1, as our next result shows:

Theorem 4.5.2. *Let* F *be a number field with odd class number,* k/F *a quadratic extension, and* L/k *an unramified* D_4*-extension such that* L/F *is not normal. Let* N *denote the normal closure of* L/F. *Then* $\mathrm{Gal}\,(N/F) \simeq 32.042 = \Gamma_5 a_1 = D_4 \curlyvee D_4$, *and* $\mathrm{Gal}\,(N/k) \simeq 16.06 = \Gamma_2 a_1 = C_2 \times D_4$. *Moreover there exists a factorization* $d = \mathrm{sep}(k/F) = d_1 d_2 d_3 d_4$ *into separants such that*

1. $(d_i, d_j) \mid \infty$ *for all* $i \neq j$;
2. $(d_1/\mathfrak{p}_2) = (d_2/\mathfrak{p}_1) = (d_3/\mathfrak{p}_4) = (d_4/\mathfrak{p}_3) = +1$ *for all* $\mathfrak{p}_i \mid d_i$;
3. $(d_1, d_2) = (d_3, d_4) = 1$.

In this case, L is cyclic over $k(\sqrt{d_1d_2}\,)$ and of type V_4 over $k(\sqrt{d_1d_3}\,)$ and $k(\sqrt{d_1d_4}\,)$.

On the other hand, if $d = d_1d_2d_3d_4$ is a factorization of $d = \mathrm{sep}(k/F)$ with these properties, then the diophantine equations $X_j^2 - d_jY_j^2 - d_{j+1}Z_j^2 = 0$ have non-trivial solutions $(x_j, y_j, z_j) \in F^3$ for $j = 1$ and $j = 3$. These solutions can be chosen in such a way that the square roots of $\alpha = x_1 + y_1\sqrt{d_1}$ and $\beta = x_3 + y_3\sqrt{d_3}$ generate the unramified cyclic quartic extensions of $F(\sqrt{d_1d_2}\,)$ and $F(\sqrt{d_3d_4}\,)$, respectively. Then $M = F(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}, \sqrt{d_4}, \sqrt{\alpha}, \sqrt{\beta})$ is an unramified extension of k with $\mathrm{Gal}\,(M/k) \simeq 32.034 = \Gamma_4a_2 = D_4 \leftthreetimes D_4$ and $\mathrm{Gal}\,(M/F) \simeq D_4 \times D_4$. Its subfield

$$L = F\left(\sqrt{d_1d_2}, \sqrt{d_1d_3}, \sqrt{d_1d_4}, \sqrt{2x_1x_3 + 2y_1y_3\sqrt{d_1d_3} + 2z_1z_3\sqrt{d_2d_4}}\right)$$

is an unramified D_4-extension of k such that $N = L(\sqrt{d_1}\,)$ is the normal closure of L/F. Moreover, $\mathrm{Gal}\,(N/F) \simeq \Gamma_5a_1$.

An explicit example for Theor. 4.5.2 is $d = -3 \cdot 13 \cdot 5 \cdot 29$; here $\mathrm{Cl}(k) \simeq (2, 2, 2, 7)$, and we find $\alpha = \frac{1}{2}(-1 + \sqrt{13}\,)$, $\beta = 7 + 2\sqrt{5}$, and $\mu = -7 + 2\sqrt{65} + 2\sqrt{-87}$.

Remark 10. *The conditions in Theor. 4.5.1 for the Legendre symbols $(d_i/\mathfrak{p}_j)$ coincide with those given in Satz 2 of [147] (after renumbering), whereas those in Theor. 4.5.2 do not. In fact, Koch assumes that the normal extension $\hat{k}/k$ which he is studying is actually normal over $\mathbb{Q}$.*

4.6 Unramified Quaternion Extensions

Theorem 4.6.1. *Let F be a number field with odd class number, k/F a quadratic extension, and L/k an unramified H_8-extension such that L/F is normal. Then*

i) $\mathrm{Gal}\,(L/F) \simeq 16.8 = \Gamma_2b = C_4 \curlyvee H_8$;

ii) there exists a "H_8-factorization" $d = \mathrm{sep}(k/F) = d_1d_2d_3$ into separants such that

  a) L is a quadratic extension of $F(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}\,)$;

  b) $(d_i, d_j) = 1$ for $i \neq j$, and

  c) $(d_1d_2/\mathfrak{p}_3) = (d_2d_3/\mathfrak{p}_1) = (d_3d_1/\mathfrak{p}_2) = +1$ for all prime ideals $\mathfrak{p}_i \mid d_i$.

iii) L is a D_4-extension of $F(\sqrt{d_i}\,)$ for $i = 1, 2, 3$ and a $(C_2 \times C_4)$-extension of $F(\sqrt{d_1d_2}\,)$, $F(\sqrt{d_2d_3}\,)$, and $F(\sqrt{d_3d_1}\,)$.

On the other hand, if k/F is a quadratic extension and $d = \mathrm{sep}(k/F) = d_1d_2d_3$ is a H_8-factorization, then there exists an $a \in \mathcal{O}_F$ such that $(a, 2) = 1$, $a \nmid d_1d_2$, and such that the system of diophantine equations

$$(**) \qquad \begin{aligned} d_1X_1^2 - d_2X_2^2 &= -ad_3X_3^2 \quad (I) \\ Y_1^2 - d_1Y_2^2 &= aY_3^2 \quad (II) \\ Z_1^2 - d_2Z_2^2 &= -aZ_3^2 \quad (III) \end{aligned}$$

has non-trivial solutions in $\mathcal{O}_F$. Let $(x_1, x_2, x_3) \in \mathcal{O}_F^3$ be a solution of (**), let $r \in F^\times$, and put

$$\mu = (x_1\sqrt{d_1} + x_2\sqrt{d_2}\,)(y_1 + y_2\sqrt{d_1}\,)(z_1 + z_2\sqrt{d_2}\,)r;$$

then $L = F(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}, \sqrt{\mu}\,)$ is an H_8-extension of k, such that $\mathrm{Gal}\,(L/F) \simeq 16.8$. Moreover, we can choose μ in such a way that L/k becomes unramified outside 2∞. If in addition $\mathrm{SCl}(F) = 1$, we can make L/k unramified at all finite places.

Proposition 4.6.2. *Let F be a number field with $\mathrm{SCl}(F) = 1$, and let $d = d_1d_2d_3$ be the product of three totally positive prime separants such that $(d_1, d_2) = (d_2, d_3) = (d_3, d_1) = 1$. If $(d_i/\mathfrak{p}_j) = -1$ for all $i \neq j$, then there exists an unramified H_8-extension L of $k = F(\sqrt{d}\,)$ which is normal over F, and the following assertions are equivalent:*

1. *L is totally real;*

2. *the quartic subfield K of L/k has 2-class number $h_2(K) = 2$;*

3. *$(E_k : N_{K/k}E_K) = 1$;*

4. *$(E_{12}/\mathfrak{p}_3) = +1$, where E_{12} denotes the unit group of $F(\sqrt{d_1}, \sqrt{d_2}\,)$.*

Similarly, L is a CM-field $\iff$ $h_2(K) = 1$ $\iff$ $(E_k : N_{K/k}E_K) = 1$ $\iff$ $(E_{12}/\mathfrak{p}_3) = -1$. The symmetry of the d_i implies the reciprocity law

$$\Big(\frac{E_{12}}{\mathfrak{p}_3}\Big) \;=\; \Big(\frac{E_{23}}{\mathfrak{p}_1}\Big) \;=\; \Big(\frac{E_{31}}{\mathfrak{p}_2}\Big).$$

In the special case $F = \mathbb{Q}$, the reciprocity law given in [638] shows that in fact

$$\Big(\frac{E_{12}}{p_3}\Big) \;=\; \Big(\frac{E_{23}}{p_1}\Big) \;=\; \Big(\frac{E_{31}}{p_2}\Big) \;=\; -\Big(\frac{d_1d_2}{p_3}\Big)_4\Big(\frac{d_2d_3}{p_1}\Big)_4\Big(\frac{d_3d_1}{p_2}\Big)_4.$$

If we know beforehand that a quadratic extension k of F admits an unramified H_8-extension, then we can construct it using Theor. 4.6.1 even if $\mathrm{SCl}(F) \neq 1$; the imaginary quadratic number field $\mathbb{Q}(\sqrt{-195}\,)$, for example, posesses an unramified extension L such that $\mathrm{Gal}\,(L/k) \simeq H_{16}$; now let $F = \mathbb{Q}(\sqrt{-3}\,)$ and $k = F(\sqrt{65}\,)$. Then $d = \mathrm{sep}(k/F) = 65 = 5(-1+2\sqrt{-3}\,)(-1-2\sqrt{-3}\,)$ is an H_8-factorization (from this fact alone we are not allowed to conclude that there is an unramified H_8-extension of k, because $\mathrm{SCl}(F) \simeq \mathbb{Z}/2\mathbb{Z}$). Nevertheless we can put $a = -1$, $d_1 = -1+2\sqrt{-3}$, $d_2 = -1-2\sqrt{-3}$, $d_3 = 5$, find that

$$\begin{array}{lll} x_1 = -1+2\sqrt{-3}, & x_2 = 3+\sqrt{-3}, & x_3 = 1, \\ y_1 = 1-\sqrt{-3}, & y_2 = 1, & y_3 = 1, \\ z_1 = 1, & z_2 = 1, & z_3 = 1, \end{array}$$

is a solution of $(**)$, and that a square root of

$$\mu = (x_1\sqrt{d_1} + x_2\sqrt{d_2}\,)(y_1 + y_2\sqrt{d_1}\,) \equiv 1 \bmod 4$$

generates the desired H_8-extension of k.

As in the dihedral case above, we cannot drop the assumption that L/F be normal; a study similar to the one for dihedral extensions shows that if L/k is a H_8-extension such that L/F is not normal, then the normal closure N of L/F has Galois group $\mathrm{Gal}\,(N/F) \simeq 32.043 = \Gamma_5 a_2 = D_4 \curlyvee H_8$. There exists a factorization $d = \mathrm{sep}(k/F) = d_1d_2d_3d_4$ such that $(d_2d_3d_4/\mathfrak{p}_1) = (d_3d_4d_1/\mathfrak{p}_2) = (d_4d_1d_2/\mathfrak{p}_3) = (d_1d_2d_3/\mathfrak{p}_4) = +1$ for all $\mathfrak{p}_i \mid d_i$. The only discriminants $> -12\,000$ of imaginary quadratic number fields with this property are $d = -7\,480 = -11\cdot 5\cdot 8\cdot 17$ and $d = -7\,995 = -3\cdot 13\cdot 5\cdot 41$, and in both cases the corresponding H_8-extension can be constructed explicitly. The construction (even the existence of the field) in the general case is still an open problem.

4.7 Non-abelian 2-groups of order 16

Theorem 4.7.1. *Let F be a number field such that $\mathrm{SCl}(F) = 1$, and let k/F be a quadratic extension; there exists a G-extension K/k which is unramified at the finite places and such that K/F is normal if and only if there is a factorization $d = \mathrm{sep}(k/F) = d_1d_2d_3$ into relatively prime separants such that the conditions (4.1) are satisifed:*

G	$(*)$	$\mathrm{Gal}\,(K/F)$
D_4	$(d_1/\mathfrak{p}_2) = (d_2/\mathfrak{p}_1) = 1$	16.6
H_8	$(d_1d_2/\mathfrak{p}_3) = (d_2d_3/\mathfrak{p}_1) = (d_3d_1/\mathfrak{p}_2) = 1$	16.8
16.9	$(d_1/\mathfrak{p}_2) = (d_1/\mathfrak{p}_3) = (d_2/\mathfrak{p}_1) = (d_3/\mathfrak{p}_1) = 1$	32.033
16.10	$(d_1/\mathfrak{p}_2) = (d_2/\mathfrak{p}_1) = (d_1d_2/\mathfrak{p}_3) = (d_3/\mathfrak{p}_1) = (d_3/\mathfrak{p}_2) = 1$	32.036
$(4,4)$	$(d_i/\mathfrak{p}_j) = 1$ *for all* $i \neq j$	32.034

If $(d_i/\mathfrak{p}_j) = 1$ for all $i \neq j$, there also exists an unramified extension L/k such that $\mathrm{Gal}\,(L/k) \simeq 32.018$ *and* $\mathrm{Gal}\,(L/F) \simeq 64.144$.

Example 4.7.1. *Let k be an imaginary quadratic number field with discriminant d, and suppose that $d = d_1d_2d_3$ is a factorization of d into discriminants; the following table gives unramified G-extensions L/k, where $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}\,)$, for all 2-groups G occuring in Theor. 4.7.1:*

G	d	d_1	d_2	d_3	L
D_4	-195	-3	13	5	$K(\sqrt{-1+2\sqrt{-3}}\,)$
H_8	-120	-3	5	8	$K\big(\sqrt{(2\sqrt{2}+\sqrt{5}\,)(2+\sqrt{5}\,)}\,\big)$
16.09	-663	13	17	-3	$K(\sqrt{-1+2\sqrt{-3}}, \sqrt{-1+2\sqrt{13}}\,)$
16.10	-580	5	29	-4	$K(\sqrt{-1+12\sqrt{-1}}, \sqrt{7+2\sqrt{5}}\,)$
$C_4 \times C_4$	-2379	-3	13	61	$K(\sqrt{-19+12\sqrt{-3}}, \sqrt{5+4\sqrt{13}}\,)$

The unramified 32.018*-extension of $\mathbb{Q}(\sqrt{-2379}\,)$ predicted by Theor. 4.7.1 is obtained by adjoining $\sqrt{-1+2\sqrt{-3}}$ to the $(C_4 \times C_4)$-extension L.*

Remark 11. *The group $G =$ 32.019 $= \Gamma_2 i$ does not occur as $\mathrm{Gal}\,(k^2/k)$ for an imaginary quadratic number field k. This follows at once from Theor. 4.7.1: let k^1 and k^2 be the Hilbert 2-class fields of k and k^1, respectively, and assume that $\mathrm{Gal}\,(k^2/k) \simeq$ 32.019. Then k^1 is an unramified $(C_4 \times C_4)$-extension of k because $G/G' \simeq C_4 \times C_4$. Theor. 4.7.1 implies the existence of an unramified* 32.018*-extension of k, hence Lk^2/k^1 is abelian and unramified, and strictly bigger than k^2: this contradicts the maximality of the Hilbert class field (see 1.9.27). A similar result for q-class fields, q an odd prime, has recently been obtained by Nomura (see Prop. 1.9.28).*

Chapter 5

Tables

5.1 Tables of Class Fields

$\operatorname{disc} k$	$\mathrm{Cl}(k)$	K	$h(K)$
-3	1	$k^1 = k$	1
-4	1	$k^1 = k$	1
-7	1	$k^1 = k$	1
-8	1	$k^1 = k$	1
-11	1	$k^1 = k$	1
-15	2	$k^1 = k(\sqrt{5}\,)$	1
-19	1	$k^1 = k$	1
-20	2	$k^1 = k(\sqrt{5}\,)$	1
-23	3	$k^1 = k(x),\ x^3 - x + 1$	1
-24	2	$k^1 = k(\sqrt{2}\,)$	1
-31	3	$k^1 = k(x),\ x^3 + x + 1$	1
-35	2	$k^1 = k(\sqrt{5}\,)$	1
-39	4	$k^1 = k(\sqrt{-2 + 2\sqrt{13}}\,)$	1
-40	2	$k^1 = k(\sqrt{5}\,)$	1
-43	1	$k^1 = k$	1
-47	5	$k^1 = k(x),\ x^5 - 2x^4 + 2x^3 - x^2 + 1$	1
-51	2	$k^1 = k(\sqrt{17}\,)$	1
-52	2	$k^1 = k(\sqrt{13}\,)$	1
-55	4	$k^1 = k(\sqrt{3 + 2\sqrt{5}}\,)$	1
-56	4	$k^1 = k(\sqrt{-1 + 2\sqrt{2}}\,)$	1
-59	3	$k^1 = k(x),\ x^3 + 2x + 1$	1
-67	1	$k^1 = k$	1
-68	4	$k^1 = k(\sqrt{4 + \sqrt{17}}\,)$	1
-71	7	$k^1 = k(x),\ x^7 - x^6 - x^5 + x^4 - x^3 - x^2 + 2x + 1$	1
-79	5	$k^1 = k(x),\ x^5 - 3x^4 + 2x^3 - x^2 + x - 1$	1
-83	3	$k^1 = k(x),\ x^3 + x^2 + x + 2$	1
-84	$2 \cdot 2$	$k^1 = k(i, \sqrt{-3}\,)$	1
-87	6	$k^1 = k(\sqrt{29}, x),\ x^3 + 2x^2 - x + 1$	1
-88	2	$k^1 = k(\sqrt{2}\,)$	1
-91	2	$k^1 = k(\sqrt{13}\,)$	1
-95	8	$k^1 = k\big(\sqrt{\sqrt{5} + (1 - \sqrt{5})\sqrt{-1 + 2\sqrt{5}}}\big)$	1
-103	5	$k^1 = k(x),\ x^5 - 2x^4 + 3x^3 - 3x^2 + x + 1$	1
-104	6	$k^1 = k(\sqrt{13}, x),\ x^3 - x + 2$	1
-107	3	$k^1 = k(x),\ x^3 - x^2 + 3x - 2$	1
-111	8	$k^1 = k\big(\sqrt{-\frac{1}{2}(9 + \sqrt{37}) + 2\sqrt{11 + 2\sqrt{37}}}\big)$	1
-115	2	$k^1 = k(\sqrt{5}\,)$	3
		$k^2 = k^1(x),\ x^3 - x + 1$	$h^2 = 1$
-116	6	$k^1 = k(\sqrt{29}, x),\ x^3 + x^2 + 2$	1
-119	10	$k^1 = k(\sqrt{17}, x),\ x^5 - 3x^4 + x^3 + x - 1$	1

$\operatorname{disc} k$	$\mathrm{Cl}(k)$	K	$h(K)$
-120	$2\cdot 2$	$k^1 = k(\sqrt{2}, \sqrt{5}\,)$	2
		$k^2 = k^1\big(\sqrt{(2\sqrt{2}+\sqrt{5}\,)(2+\sqrt{5}\,)}\,\big)$	$h^2 = 1$
-123	2	$k^1 = k(\sqrt{41}\,)$	1
-127	5	$k^1 = k(x),\ x^5 - 3x^4 - x^3 + 2x^2 + x - 1$	1
-131	5	$k^1 = k(x),\ x^5 - 5x^4 + 3x^3 + x^2 - x - 1$	1
-132	$2\cdot 2$	$k^1 = k(i, \sqrt{-3}\,)$	1
-136	4	$k^1 = k(\sqrt{6+2\sqrt{17}}\,)$	1
-139	3	$k^1 = k(x),\ x^3 - x^2 + x + 2$	1
-143	10	$k^1 = k(\sqrt{13}, x),\ x^5 - 3x^4 + x^2 + x - 1$	1
-148	2	$k^1 = k(i)$	1
-151	7	$k^1 = k(x),\ x^7 - 3x^6 - x^5 - 3x^4 - x^2 - x - 1$	1
-152	6	$k^1 = k(\sqrt{2}, x),\ x^3 + x^2 - 2x + 2$	1
-155	4	$k^1 = k(\sqrt{-7+4\sqrt{5}}\,)$	3
		$k^2 = k^1(x),\ x^3 + x + 1$	$h^2 = 1$
-159	10	$k^1 = k(\sqrt{-3}, x),\ x^5 - 4x^4 - 2x^3 - x^2 - 2x - 1$	1
-163	1	$k^1 = k$	1
-164	8	$k^1 = k\big(\sqrt{2+2i+\sqrt{5+4i}}\,\big)$	1
-167	11	$k^1 = k(x),\ x^{11} + x^{10} + 5x^9 + 4x^8 + 10x^7 + 6x^6$ $+ 11x^5 + 7x^4 + 9x^3 + 4x^2 + 2x - 1$	1
-168	$2\cdot 2$	$k^1 = k(\sqrt{-2}, \sqrt{-3}\,)$	1
-179	5	$k^1 = k(x),\ x^5 - 6x^4 + x^3 - 5x^2 + 2x - 1$	1
-183	8	$k^1 = k\big(\sqrt{-\frac{5}{2}(5+\sqrt{-3}\,) + 2\sqrt{7+2\sqrt{-3}}}\big)$	1
-184	4	$k^1 = k(\sqrt{-3+4\sqrt{2}}\,)$	3
		$k^2 = k^1(x),\ x^3 - x + 1$	1
-187	2	$k^1 = k(\sqrt{-11}\,)$	1
-191	13	$k^1 = k(x),\ x^{13} - 6x^{12} + 10x^{11} - 16x^{10} + 22x^9 - 19x^8$ $+ 11x^7 - 5x^6 - x^5 + 5x^4 - 4x^3 + 2x - 1$	1
-195	$2\cdot 2$	$k^1 = k(\sqrt{-3}, \sqrt{5}\,)$	4
		$k^2 = k^1(x, y),\ x^2 = -1 + 2\sqrt{-3},\ x'^2 = -1 - 2\sqrt{-3}$ $y^2 = (x^3 + (3+\sqrt{-3}\,)x')(1 - \sqrt{-3} + x')$	1
-199	9	$k^1 = k(x),\ x^9 - 5x^8 + 3x^7 - 3x^6 - 3x^3 - x - 1$ or $k(y, z),\ y^3 + 4y^2 + y + 1, z^3 + yz^2 + (y^2+1)z - y$	1
-203	4	$k^1 = k(\sqrt{-7}, \sqrt{-1+2\sqrt{-7}}\,)$	1
-211	3	$k^1 = k(x),\ x^3 + 3x^2 + x + 2$	
-212	6	$k^1 = k(i, x),\ x^3 + x^2 + 4x + 2$	1
-215	14	$k^1 = k(\sqrt{5}, x), x^7 - 5x^6 + x^5 - 6x^4 + 5x^3 - 3x^2 + 3x - 1$	1
-219	4	$k^1 = k(\sqrt{-3}, \sqrt{5+4\sqrt{-3}}\,)$	1
-223	7	$k^1 = k(x),\ x^7 - 5x^6 + x^4 - 4x^3 - x^2 - 1$	1
-227	5	$k^1 = k(x) = x,\ x^5 - 9x^4 + 9x^3 - 9x^2 + 5x - 1$	1
-228	$2\cdot 2$	$k^1 = k(i, \sqrt{-3}\,)$	1
-231	$2\cdot 6$	$k^1 = k(\sqrt{-3}, \sqrt{-7}, x),\ x^3 - 4x^2 + 5x + 1$	1
-232	2	$k^1 = k(\sqrt{-2}\,)$	1
-235	2	$k^1 = k(\sqrt{5}\,)$	5
		$k^2 = k(x),\ x^5 - x^3 - 2x^2 - x - 1$	1
-239	15	$k^1 = k(x, y),\ x^3 - x + 3 = 0,$ $y^5 - 2y^4 - 5y^3 - 4y^2 - 2y - 1$	1

$\operatorname{disc} k$	$\mathrm{Cl}(k)$	K	$h(K)$
-244	6	$k^1 = k(i,x),\ x^3+2x^2-3x+2$	1
-247	6	$k^1 = k(\sqrt{13},x),\ x^3-3x^2+4x+1$	1
-248	8	$k^1 = k\big(\sqrt{\sqrt{2}+\sqrt{1+4\sqrt{2}}\,(1+\sqrt{2})}\,\big)$	3
		$k^2 = k^1(y),\ y^3+y+1$	1
-251	7	$k^1 = k(x),\ x^7-9x^6-2x^5+4x^4+2x^3-6x^2-5x-1$	1
-255	$2\cdot 6$	$k^1 = k(\sqrt{-3},\sqrt{5},x),\ x^3+x^2+3$	2
		$k^2 = k^1\big(\sqrt{(\sqrt{17}+2\sqrt{5})(4-\sqrt{17})}\,\big)$	1
-259	4	$k^1 = k(\sqrt{3+2\sqrt{-7}}\,)$	1
-260	$2\cdot 4$	$k^1 = k(\sqrt{5},\sqrt{-7+4i}\,)$	2
		$k^2 = k^1(x),\ x^2 = (1-2i)\sqrt{-7+4i}-2i\sqrt{-7+4i}$	1
-263	13	$k^1 = k(x),\ x^{13}-8x^{12}+16x^{11}-27x^{10}+38x^9$ $-36x^8+22x^7-12x^6+13x^5-19x^4$ $+21x^3-15x^2+6x-1$	1
-267	2	$k^1 = k(\sqrt{-3}\,)$	1
-271	11	$k^1 = k(x),\ x^{11}-5x^{10}-6x^9-5x^8+3x^7+$ $+6x^6+3x^5-3x^4-x^3-x^2-1$	1
-276	$2\cdot 4$	$k^1 = k(\sqrt{-23},\sqrt{5+4\sqrt{3}}\,)$	3
		$k^2 = k^1(x),\ x^3-x+1$	1
-280	$2\cdot 2$	$k^1 = k(\sqrt{2},\sqrt{5}\,)$	4
		$k^2 = k^1(y,z),\ y^2 = -1+2\sqrt{2}$	$h^2=1$
-283	3	$k^1 = k(x),\ x^3+4x-1$	$2\cdot 2$
		$k^2 = k^1(y),\ y^4-y-1$	$h^2=2$
		$k^3 = k^2(z),\ z^2 = -3+4y^2-4y^3$	$h^3=1$
-287	14	$k^1 = k(\sqrt{-7},x),$ $x^7-5x^6-6x^5-12x^4-12x^3-10x^2-4x-1$	1
-291	4	$k^1 = k(\sqrt{-7+4\sqrt{-3}}\,)$	1
-292	4	$k^1 = k(\sqrt{-3+8i}\,)$	1
-295	8	$k^1 = k\big(\sqrt{\tfrac{1}{2}(1+3\sqrt{5})+2\sqrt{11+6\sqrt{5}}}\,\big)$	3
		$k^2 = k(z),\ z^3+2z+1=0$	$h^2=1$
-296	10	$k^1 = k(\sqrt{-2},x),\ x^5-29x^4-34x^3-6x^2+5x-1$	1
-299	8	$k^1 = k\big(\sqrt{3-2\sqrt{13}+(6+2\sqrt{13}\,)\sqrt{-43+12\sqrt{13}},}\big)$	1
-303	10	$k^1 = k(\sqrt{-3},x), x^5-10x^4-5x^3+5x^2+x-1$	1
-307	3	$k^1 = k(x),\ x^3-x^2+3x+2$	1
-308	$2\cdot 4$	$k^1 = k(i,\sqrt{11},\sqrt{13+4\sqrt{11}}\,)$	1
-311	19	$k^1 = k(x),\ x^{19}-4x^{18}-16x^{17}-37x^{16}-42x^{15}$ $-38x^{14}-4x^{13}+10x^{12}+25x^{11}$ $+18x^{10}+9x^9+x^8-10x^7-13x^6$ $-14x^5-8x^4-5x^3-2x^2-x-1$	1
-312	$2\cdot 2$	$k^1 = k(\sqrt{2},\sqrt{-3}\,)$	4
		$k^2 = k^1(\sqrt{-1+2\sqrt{-3}}\,,\alpha),\ \alpha = ?$	1
-319	10	$k^1 = k(\sqrt{29},x),\ x^5-6x^4-3x^3+x^2-x-1$	1
-323	4	$k^1 = k(\sqrt{7+2\sqrt{17}}\,)$	1
-327	12	$k^1 = k(\sqrt{-1+6\sqrt{-3}}\,,x),\ x^3-4x^2+3x-1$	1
-328	4	$k^1 = k(\sqrt{-3+4\sqrt{-2}}\,)$	1

$\operatorname{disc} k$	$\mathrm{Cl}(k)$	K	$h(K)$
-331	3	$k^1 = k(x),\ x^3 - 4x^2 + 8x - 9$	$2 \cdot 2$
		$k^2 = k^1(y),\ y^4 - 2y^2 - 3y - 1$	$h^2 = 2$
		$k^3 = k^2(z),\ z^2 + 3 + 4y - 4y^2$	$h^3 = 1$
-335	18	$k^1 = k(\sqrt{5}, x, y),\ x^3 - 2x^2 + 5x - 5,$	
		$y^3 - (2x^2 - x + 7)y^2 - (x^2 - x + 4)$	1
-339	6	$k^1 = k(\sqrt{-3}, x),\ x^3 + 2x^2 + 3$	1
-340	$2 \cdot 2$	$k^1 = k(\sqrt{5}, \sqrt{17}\,)$	4
		$k^2 = k^1(\sqrt{(2 + 2i + \sqrt{1 + 4i})(1 + 2i)}\,)$	$h^2 = 1$
-344	10	$k^1 = k(\sqrt{-2}, x),\ x^5 - 43x^4 + 8x^4 - 19x^2 - 9x - 1$	1
-347	5	$k^1 = k(x),\ x^5 - 13x^4 - 27x^3 - 21x^2 - 7x - 1$	1
-355	4	$k^1 = k(\sqrt{-3 + 16\sqrt{5}}\,)$	7
		$k^2 = k^1(x),\ x^7 - x^6 - x^5 + x^4 - x^3 - x^2 + 2x + 1$	1
-356	12	$k^1 = k(\sqrt{5 + 8i}, x),\ x^3 + 3x^2 - 4x + 2$	1
-359	19	$k^1 = k(x),\ x^{19} - 14x^{18} + 59x^{17} - 113x^{16} + 91x^{15} + 19x^{14}$	
		$- 90x^{13} + 51x^{12} + 2x^{11} - 5x^{10} + 9x^9 - 30x^8 + 22x^7$	
		$+ 7x^6 - 14x^5 + 3x^4 + 2x^3 - 2x^2 + 2x - 1$	1
-367	9	$k^1 = k(x, y),\ x^3 - 2x^2 + 3x - 5,$	
		$y^3 - xy^2 + (x^2 - x)y + x - 2$	1
-371	8	$k^1 = k\big(\sqrt{\tfrac{1}{2}(-13 + \sqrt{53}) + (14 - 2\sqrt{53})\sqrt{29 + 4\sqrt{53}}}\,\big)$	1
-372	$2 \cdot 2$	$k^1 = k(i, \sqrt{-3}\,)$	3
		$k^2 = k^1(x),\ x^3 + x + 1$	1
-376	8	$k^1 = k\big(\sqrt{-3 + (8 - 4\sqrt{2})\sqrt{9 + 8\sqrt{2}}}\,\big)$	5
		$k^2 = k^1(x),\ x^5 - x^3 - 2x^2 - x - 1$	$h^2 = 1$
-379	3	$k^1 = k(x),\ x^3 + x^2 + x + 4$	1
-383	17	$k^1 = k(x),\ x^{17} - 6x^{16} - 24x^{15} - 42x^{14} - 31x^{13} - 23x^{12} - 7x^{11}$	
		$- x^{10} - 4x^9 - 11x^8 - 7x^7 - 13x^6 - x^5 + x^3 + x^2 + x - 1$	1
-388	4	$k^1 = k(\sqrt{9 + 4i})$	1
-391	14	$k^1 = k(\sqrt{17}, x),$	
		$x^7 - 9x^6 + 10x^5 - 14x^4 + 8x^3 - 6x^2 + 2x - 1$	3
		$k^2 = k^1(y),\ y^3 - y + 1$	$h^2 = 1$
-395	8	$k^1 = k\big(\sqrt{-1 + (4 + 2\sqrt{5})\sqrt{1 + 4\sqrt{5}}}\,\big)$	5
		$k^2 = k^1(x),\ x^5 - 3x^4 + 2x^3 - x^2 + x - 1$	1
-399	$2 \cdot 8$	$k^1 = k\big(\sqrt{-7}, \sqrt{-\tfrac{1}{2}(15 + \sqrt{133}) + 2\sqrt{23 + 2\sqrt{133}}}\,\big)$	1
-403	2	$k^1 = k(\sqrt{13}\,)$	3
		$k^2 = k^1(x),\ x^3 + x + 1$	$h^2 = 1$
-404	14	$k^1 = k(i, x),\ P(x) = ?$	1
-407	16	$k^1 = k(x, y), x^2 = \tfrac{1}{2}(11 + \sqrt{37}) + 2\sqrt{7 + 2\sqrt{37}}\,,\ y^2 = ?$	1
-408	$2 \cdot 2$	$k^1 = k(\sqrt{2}, \sqrt{17}\,)$	2
		$k^2 = k^1(\sqrt{-5 + 2\sqrt{2}}\,)$	$h^2 = 1$
-411	6	$k^1 = k(\sqrt{-3}, x),\ x^3 + x^2 + 5x + 2$	1
-415	10	$k^1 = k(\sqrt{5}, x),\ x^5 - 13x^4 + 9x^3 + x - 1$	3
		$k^2 = k^1(y),\ y^3 + y^2 + y + 2$	$h^2 = 1$
-419	9	$k^1 = k(x, y),\ x^3 + 3x^2 - x + 2,\ P(y) = ?$	1
-420	$2 \cdot 2 \cdot 2$	$k^1 = k(i, \sqrt{-3}, \sqrt{5}\,)$	$2 \cdot 2$
		$k^2 = k^1\big(\sqrt{(4i - \sqrt{5})(2 + \sqrt{5})}\,, \sqrt{(2\sqrt{-5} + \sqrt{7})(8 - 3\sqrt{7}\,)}\big)$	1

$\operatorname{disc} k$	$\operatorname{Gal}(k^1/k)$	$\operatorname{Gal}(k^2/k)$	$\operatorname{Gal}(k^3/k)$
-115	C_2	D_3	
-120	$C_2 \times C_2$	H_8	
-155	C_4	H_{12}	
-184	C_4	H_{12}	
-195	$C_2 \times C_2$	H_{16}	
-235	C_2	D_5	
-248	C_8	Λ_{24}	
-255	$C_2 \times C_6$	$C_3 \times H_8$	
-260	$C_2 \times C_4$	M_{16}	
-276	$C_2 \times C_4$	$C_2 \times H_{12}$	
-280	$C_2 \times C_2$	H_{16}	
-283	C_3	A_4	$\widetilde{A}_4$
-295	C_8	Λ_{24}	
-299	C_8	Λ_{24}	
-312	$C_2 \times C_2$	H_{16}	
-331	C_3	A_4	$\widetilde{A}_4$
-340	$C_2 \times C_2$	SD_{16}	
-355	C_4	H_{28}	
-372	$C_2 \times C_2$	$C_2 \times D_3$	
-376	C_8	Λ_{40}	
-391	C_{14}	$C_7 \times D_3$	
-395	C_8	Λ_{40}	
-403	C_2	D_3	
-408	$C_2 \times C_2$	D_4	
-415	C_{10}	$C_5 \times D_3$	
-420	$C_2 \times C_2 \times C_2$	32.040	

The groups involved are:

C_n cyclic group of order n,

D_n dihedral group of order $2n$,

H_n quaternionic group of order n,

SD_n semi-dihedral group of order n,

A_4 alternating group of order 12,

$\widetilde{A}_4$ its covering group of order 24,

$M_{4n} = \langle x, y : x^m = y^2 = -1, yxy^{-1} = -x \rangle$,

$\Lambda_{8n} = \langle x, y : x^{4m} = y^8 = 1, x^m = y^2, yxy^{-1} = x^{2m} - 1 \rangle$,

32.040 the group with this number in some published tables of 2-groups, for example Senior and Hall where -1 denotes a central involution.

5.2 Tables of 2-Groups

In the columns SG(Γ) and FG(Γ) we list the subgroups of index 2 and the factor groups of order #Γ/2, respectively.

1. Groups of order 8

Γ	TW	HS	Γ′	Γ/Γ′	$Z(\Gamma)$	$\Gamma/Z(\Gamma)$	SG(Γ)	FG(Γ)	$\mathfrak{M}(\Gamma)$
(8)	8.001		1	(8)	(8)	1	(4)	(4)	1
(2, 4)	8.002		1	(2, 4)	(2, 4)	1	$(2,2),(4)^2$	$(2,2),(4)^2$	(2)
(2, 2, 2)	8.003		1	(2, 2, 2)	(2, 2, 2)	1	$(2,2)^7$	$(2,2)^7$	(2, 2, 2)
D_4	8.004	$\Gamma_2 a_1$	(2)	(2, 2)	(2)	(2, 2)	$(2,2)^2,(4)$	(2, 2)	(2)
H_8	8.005	$\Gamma_2 a_2$	(2)	(2, 2)	(2)	(2, 2)	$(4)^3$	(2, 2)	1

2. Non-Abelian Groups of order 16

Γ	TW	HS	Γ′	Γ/Γ′	$Z(\Gamma)$	$\Gamma/Z(\Gamma)$
$C_2 \times D_4$	16.006	$\Gamma_2 a_1$	C_2	(2, 2, 2)	(2, 2)	(2, 2)
$C_2 \times H_8$	16.007	$\Gamma_2 a_2$	C_2	(2, 2, 2)	(2, 2)	(2, 2)
$D_4 \curlyvee C_4$	16.008	$\Gamma_2 b$	C_2	(2, 2, 2)	C_4	(2, 2)
$D_4 \curlywedge C_4$	16.009	$\Gamma_2 c_1$	C_2	(2, 4)	(2, 2)	(2, 2)
$H_8 \curlywedge C_4$	16.010	$\Gamma_2 c_2$	C_2	(2, 4)	(2, 2)	(2, 2)
M_{16}	16.011	$\Gamma_2 d$	C_2	(2, 4)	C_4	(2, 2)
D_8	16.012	$\Gamma_3 a_1$	C_4	(2, 2)	C_2	D_4
SD_{16}	16.013	$\Gamma_3 a_2$	C_4	(2, 2)	C_2	D_4
H_{16}	16.014	$\Gamma_3 a_3$	C_4	(2, 2)	C_2	D_4

Γ	SG(Γ)	FG(Γ)	$\mathfrak{M}(\Gamma)$
$C_2 \times D_4$	$(2,2,2)^2,(2,4),D_4^4$	$(2,2,2),D_4^2$	(2, 2, 2)
$C_2 \times H_8$	$(2,4)^3,H_8^4$	$(2,2,2),H_8^2$	(2, 2)
$D_4 \curlyvee C_4$	$(2,4)^3,D_4^3,H_8$	(2, 2, 2)	(2, 2)
$D_4 \curlywedge C_4$	$(2,2,2),(2,4)^2$	$(2,4),D_4^2$	(2, 2)
$H_8 \curlywedge C_4$	$(2,4)^3$	$(2,4),D_4,H_8$	C_2
M_{16}	$(2,4),C_8^2$	(2, 4)	1
D_8	C_8,D_4^2	D_4	C_2
SD_{16}	C_8,D_4,H_8	D_4	1
H_{16}	C_8,H_8^2	D_4	1

Bibliography

I. Construction of Hilbert Class Fields

[1] L. Kronecker, *Die kubischen abelschen Gleichungen des Bereichs* ($\sqrt{-31}$), Werke IV, 125–129

[2] D. Hilbert, *Ausgewählte Kapitel der Zahlentheorie*, Vorlesungsskript Göttingen, Sommersemester 1898 (E. Maus ed.) 1990.

[3] G. Rückle, *Quadratische Reziprozitätsgesetze in algebraischen Zahlkörpern*, Dissertation Göttingen (1901)

[4] L. Sapolsky, *Über die Theorie der relativ-Abelschen cubischen Zahlkörper*, Diss. Göttingen (1902)

[5] R. Fueter, *Der Klassenkörper der quadratischen Körper und die komplexe Multiplikation*, Diss. Göttingen (1903)

[6] R. Fueter, *Die zahlentheoretische Konstruktion des Klassenkörpers*, (1911)

[7] R. Fueter, *Die diophantische Gleichung* $\xi^3 + \eta^3 + \zeta^3 = 0$, Sitzungsber. Heidelberger Akad. Wiss. (1913)

[8] F. Pollaczek, *Über die irregulären Kreiskörper der ℓ-ten und ℓ^n-ten Einheitswurzeln*, Math. Z. **21** (1924), 1–38

[9] R. Fueter, *Über kubische diophantische Gleichungen*, Comment. Math. Helvet. **2** (1930), 69–89

[10] H. Hasse, *Arithmetische Theorie der kubischen Körper auf klassenkörpertheoretischer Grundlage*, Math. Z. **31** (1930), 565–582

[11] J. Herbrand, *Sur les classes des corps circulaires*, J. Math. Pures appl. **11** (1932), 417–441

[12] L. Rédei, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, Math. Naturwiss. Anz. Ungar. Akad. d. Wiss. **49** (1932), 338–363

[13] H. Hasse, *Explizite Konstruktion zyklischer Klassenkörper*, Math. Ann. **109** (1933), 191–195

[14] T. Morishima, *Über die Einheiten und Idealklassen des Galoisschen Zahlkörpers und die Theorie der Kreiskörper der ℓ^ν-ten Einheitswurzeln*, Jap. J. Math. **10** (1933), 83–126

[15] L. Rédei, H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1933), 69–74

[16] H. Reichardt, *Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. **170** (1933), 75–82

[17] D. Mirimanoff, *L'équation* $\xi^3 + \eta^3 + \zeta^3 = 0$ *et la courbe* $x^3 + y^3 = 1$, Comment. Math. Helvet. **6** (1934), 192–198

[18] H. S. Vandiver, *On the composition of the group of ideal classes in a properly irregular cyclotomic field*, Monatsh. f. Math. **182** (1939), 369–380

[19] L. Rédei, *Über den geraden Teil der Ringklassengruppe quadratischer Zahlkörper, die Pellsche Gleichung und die diophantische Gleichung* $rx^2 + sy^2 = z^{2^n}$ *I, II, III*, Math. Naturwiss. Anz. Ungar. Akad. d. Wiss. **62** (1943), 13–34, 35–47, 48–62

[20] M. Gut, *Kubische Klassenkörper über quadratisch-imaginären Grundkörpern*, N. Arch. Wiskunde (2) **23** (1951), 185–189

[21] A. Aigner, *Weitere Ergebnisse über* $x^3 + y^3 + z^3$ *in quadratischen Körpern*, Monatsh. Math. Phys. **56** (1952), 240–252

[22] L. Rédei, *Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung*, Acta Math. Acad. Sci. Hungaricae **4** (1953) 31–87

[23] M. Gut, *Relativquadratische Zahlkörper, deren Klassenzahl durch eine vorgegebene ungerade Primzahl teilbar ist*, Comment. Math. Helvet. **28** (1954), 270–277

[24] C. S. Herz *Construction of Class Fields*, Seminar on complex multiplication (Chowla et al. eds.) (1957), Lecture Notes Math. 21, Springer Verlag

[25] T. Honda, *On absolute class fields of certain algebraic number fields*, J. Reine Angew. Math. **203** (1960), 80–89

[26] H. Hasse, *Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante* -47, Acta Arith. **9** (1964), 419–434

[27] T. Honda, *On real quadratic fields whose class numbers are multiples of* 3, J. Reine Angew. Math. **233** (1968), 101–102

[28] H. Bauer, *Über die kubischen Klassenkörper zyklischer kubischer Zahlkörper*, Diss. Karlsruhe (1969),

[29] H. Hasse, J. Liang, *Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante* -47, Acta Arith. **16** (1969), 89–97

[30] J. Liang, H. Zassenhaus, *On a problem of Hasse*, Math. Comp. **23** (1969), 315–319

[31] G. Gras, *Extensions abéliennes non ramifiées de degré premier d'un corps quadratique*, Thèse 3^e cycle, Grenoble (1970),

[32] K. Uchida, *Unramified extensions of quadratic number fields I, II*, Tôhoku Math. J. **22** (1970), 138–141, 220–224

[33] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76

[34] T. Honda, *Pure cubic fields whose class numbers are multiples of three*, J. Number Theory **3** (1971), 7–12

[35] M. Ishida, *On algebraic number fields with even class numbers*, J. Reine Angew. Math. **247** (1971), 118–122

[36] C. J. Theusch, *Determination of the Hilbert class field for certain algebraic number fields*, Ph. D. Diss. Michigan State Univ., 42 pp. (1971)

[37] G. Gras, *Extensions abéliennes non ramifiées de degré premier d'un corps quadratique*, Bull. Soc. Math. France **100** (1972), 177–193

[38] P. Barrucand, H. Cohn, *On some class fields related to primes of type* $x^2 + 32y^2$, J. Reine Angew. Math. **262/263** (1973), 400–414

[39] A. Deobald, *Unverzweigte Erweiterungen von algebraischen Zahlkörpern – konstruiert durch Polynome der Form* $X^n + aX + b$, Diplomarbeit Heidelberg

[40] M. Gut, *Erweiterungskörper von Primzahlgrad mit durch diese Primzahl teilbarer Klassenzahl*, L'Enseign. Math. (2) **19** (1973), 119–123

[41] O. Neumann, *Relativ-quadratische Zahlkörper, deren Klassenzahlen durch* 3 *teilbar sind*, Math. Nachr. **56** (1973), 281–306

[42] K. Uchida, *On a cubic cyclic field with discriminant* 163^2, J. Number Theory **8** (1973), 346–349

[43] K. Uchida, *Class numbers of cubic cyclic fields*, J. Math. Soc. Japan **26** (1973), 447–453

[44] P. Barrucand, *Quelques aspects de la théorie des corps cubiques*, Sém. Delange-Pisot-Poitou **16** (1974/75), no 18

[45] G. Cooke, *Construction of Hilbert class field extension of* $K = \mathbb{Q}(\sqrt{-41}\,)$, Lecture Notes Cornell Univ. Ithaca (1974),

[46] M. Ishida, *On* 2*-rank of the ideal class groups of algebraic number fields*, J. Reine Angew. Math. **273** (1975), 165–169

[47] K. Ribet, *Sur la recherche des p-extensions non ramifiées de* $\mathbb{Q}(\mu_p)$, Groupe Étude Algèbre, Univ. P. et M. Curie I **2** (1975/76), 1–3

[48] H. Cohn, G. Cooke, *Parametric form of an eight class field*, Acta Arith. **30** (1976), 367–377

[49] K. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. **34** (1976), 151–162

[50] Ph. Satgé, P. Barrucand, *Une classe de corps résolubles, les corps tchebycheviens*, C. R. Acad. Sci. Paris **282** (1976), 947–949

[51] D. Shanks, *A survey of quadratic, cubic and quartic number fields (from a computational point of view)*, Proc. VIIth Southeastern Conf., Congr. Numer. **17** (1976), 15–40

[52] K. Györy, W. Leahey, *A note on Hilbert class fields of algebraic number fields*, Acta Math. Acad. Sci. Hungar. **29** (1977), 251–254

[53] P. Kaplan, *Unités de norme* -1 *de* $\mathbb{Q}(\sqrt{p}\,)$ *et corps de classes de degré* 8 *de* $\mathbb{Q}(\sqrt{-p}\,)$ *où* p *est un nombre premier congru à* 1 mod 8, Acta Arith. **32** (1977), 239–243

[54] C. J. Parry, *Real quadratic fields with class numbers divisible by five*, Math. Comp. **31** (1977), 1019–1029

[55] Ph. Satgé, *Construction de corps résolubles non ramifiées*, Sém. de l'Université Caen (1977)

[56] J.-P. Serre, *Modular forms of weight one and Galois representations*, Algebraic Number Fields (A. Fröhlich, ed.) 193–268, Academic Press 1977

[57] S. K. Gogia, I. S. Luthar, *Quadratic unramified extensions of* $\mathbb{Q}(\sqrt{d}\,)$, J. Reine Angew. Math. **298** (1978), 108–111

[58] A. Kerkour, *Sur les extensions cycliques de degré* ℓ^n, ℓ *premier, galoisiennes sur certains sous corps du corps de base*, Doctorat d'état, Université de Franche-Comté, Besançon 131, 1978

[59] C. J. Parry, *On the class number of relative quadratic fields*, Math. Comp. **32** (1978), 1261–1270

[60] H. Cohn, *Cyclic sixteen-class fields for* $\mathbb{Q}(\sqrt{-p}\,)$ *by modular arithmetic*, Math. Comp. **33** (1979), 1307–1316

[61] J.-Ch. Hwang, *Unramified quadratic extensions of pure cubic fields*, Ph. D. City Univ. New York, 1979

[62] P. Llorente, *Cuerpos cúbicos y cuerpo de clases de cuerpos quadráticos reales*, Publ. Secc. Mat. Univ. Auton. Barcelona **26** (1982), 93–109; see also Acta 2^o Congr. Mat. Venezuela, 1979

[63] J.-F. Mestre, *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, Sém Théor. Nombres Bordeaux (1979/80), 18pp

[64] Ph. Satgé, *Divisibilité du nombre de classes de certains corps cycliques*, Journées Arithm. Luminy, Astérisque **61** (1979), 193–203

[65] Ph. Satgé, *Corps résolubles et divisibilité du nombre de classes d'idéaux*, L'Enseign. Math. **25** (1979), 165–188

[66] H. Cohn, *The explicit Hilbert* 2*-cyclic class field for* $\mathbb{Q}(\sqrt{-p}\,)$, J. Reine Angew. Math. **321** (1980), 64–77

[67] H. Cohn, *The next Pellian equation*, in: Analytic number theory, Philadelphia 1980, Lecture Notes in Math. 221–230

[68] A. Wiles, *Modular curves and class groups of* $\mathbb{Q}(\zeta_p)$, Invent. Math. **58** (1980), 1–35

[69] W. Hettkamp, *Quadratischer Restcharakter von Grundeinheiten und* 2*-Klassengruppen quadratischer Zahlkörper*, Diss. Münster (1981)

[70] H. Ichimura, *On* 2*-rank of the ideal class groups of totally real number fields*, Proc. Japan Acad. **58** (A) (1982), 329–332

[71] J.-F. Mestre, *Courbes elliptiques et groupes de classes d'idéaaux de certains corps quadratiques*, J. Reine Angew. Math. **343** (1982), 23–35

[72] S. Nakano, *Class numbers of pure cubic fields*, Proc. Japan Acad. **59** (1983), 263–265

[73] S. Nakano, *On the construction of certain number fields*, Tokyo J. Math **6** (1983), 389–395

[74] H. S. Pzena, *The explicit construction of ring class fields with applications to quadratic forms*, Diss. City Univ. New York (1983),

[75] J. Therond, *Existence d'une extension cyclique cubique monogène de discriminant donné*, Arch. Math. **41** (1983), 243–255

[76] M. Watabe, *On certain cubic fields IV*, Proc. Japan Acad. **59** (1983), 387–389

[77] S. Nakano, *On ideal class groups of algebraic number fields*, Proc. Japan Acad. **60** (1984), 74–77

[78] S. Nakano, *On the* 2*-rank of the ideal class groups of pure number fields*, Arch. Math. **42** (1984), 53–57

[79] N. Nakagoshi, *A construction of unramified abelian* ℓ*-extensions of regular Kummer extensions*, Acta Arith. **44** (1984), 47–58

[80] Y. Odai, *Some unramified cyclic cubic extensions of pure cubic fields*, Tokyo J. Math. **7** (1984), 391–398

[81] Th. P. Vaughan, *The construction of unramified abelian cubic extensions of a quadratic field*, Acta Arith. **44** (1984), 379–387

[82] Y. Yamamoto, *Divisibility by* 16 *of class number of quadratic fields whose* 2*-class groups are cyclic*, Osaka J. Math. **21** (1984), 1–22

[83] H. Cohn, *Introduction to the Construction of Class Fields*, Cambridge 1985

[84] S. Nakano, *On ideal class groups of algebraic number fields*, Thesis, Gakushuin University 1985

[85] S. Nakano, *On ideal class groups of algebraic number fields*, J. Reine Angew. Math. **358** (1985), 61–75

[86] Th. P. Vaughan, *The construction of unramified cyclic quartic extensions of* $\mathbb{Q}(\sqrt{-m}\,)$, Math. Comp. **45** (1985), 233–242

[87] F. Halter-Koch, *Konstruktion von Klassenkörpern und Potenzrestkriterien für quadratische Einheiten*, Manuscripta Math. **54** (1986), 453–492

[88] H. Naito, *Some results on class numbers and unramified extensions of algebraic number fields*, Proceedings Intern. Proc. on Class Number and Fundamental Units of Algebraic Number Fields (1986), 260–274 Corr.: [183]

[89] Y. Odai, *On unramified cyclic extensions of degree* ℓ *of algebraic number fields of degree* ℓ, Nagoya Math. J. **107** (1987), 135–146

[90] L. C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), 371–384

[91] F. Diaz y Diaz, P. Llorente, J. Quer, *Cubic fields, a congruential criterion for Scholz's theorem and new real quadratic fields with* 3*-rank equal to* 4, Arch. Math. **50** (1988), 356–359

[92] Y. Z. Lan, *Arithmetic properties of a class of cubic cyclic fields*, Sci. China Ser. A **32** (1989), 922–928

[93] A. Lbekouri, *Sur la construction d'un corps de Hilbert*, Manuscripta Math. **65** (1989), 257–273

[94] D. Li, *Class groups of cubic cyclic fields* (Chin.), J. Sichuan Univ., Nat. Sci. Ed. **26** (1989), 132–135

[95] N. Nakagoshi, *On the unramified extensions of the prime cyclotomic number field and its quadratic extensions*, Nagoya Math. J. **115** (1989), 151–164

[96] M. Horie, *On central extensions of elementary abelian fields*, J. Number Theory **36** (1990), 95–107

[97] T. Nakahara, *A construction of quadratic fields whose class numbers are divisible by a power of* 3, Diophantine and Algebraic Number Theory (vol. II), Proc. Conf. Budapest, Hungary 1987, Colloqu. Math. Soc. Jánosz Bolyai **51** (1990), 889–897

[98] V. Ennola, *Cubic number fields with exceptional units*, in: Computational Number Theory, Proc. Coll. Comp. Number Theory, Debrecen, Hungary 1989 103–128

[99] N. Nakagoshi, *On the unramified Kummer extensions of quadratic extensions of the prime cyclotomic number field*, Arch. Math. **57** (1991), 566-570

[100] N. Nakagoshi, *On the class number of the* ℓp*-th cyclotomic number field*, Math. Proc. Cambridge Phil. Soc. **109** (1991), 263–276

[101] A. Nomura, *On the existence of unramified* p*-extensions*, Osaka J. Math. **28** (1991), 55–62

[102] S. G. Vladut, *Kronecker's Jugendtraum and modular functions*, Studies in the Development of Modern Mathematics, Gordon and Breach Science Publishers (1991)

[103] K. S. Williams, R. H. Hudson, *Representation of primes by the principal form of discriminant* $-D$ *when the class number* $h(-D)$ *is* 3, Acta Arith. **57** (1991), 131–153

[104] R. Schertz, *Problèmes de construction en multiplication complexe*, Semin. Théor. Nombres Bordx. Ser. II **4** (1992), 239-262

[105] S. Gurak, *Explicit construction of certain split extensions of number fields and constructing cyclic class fields*, Pacific J. Math. **157** (1993), 269–294

[106] J. Cougnard, *Un anneau d'entiers stablement libre et non libre*, Experiment. Math. **3** (1994), 129–136

[107] J. Cougnard, *Base normale dans un corps de classes de Hilbert*, Théorie des nombres, 1992/93–1993/94, 26 pp., Publ. Math. Fac. Sci. Besançon

[108] F. Lemmermeyer, *Construction of Hilbert class fields I*, preprint (1994)

[109] F. Lemmermeyer, *Construction of Hilbert class fields II*, preprint (1994)

[110] K. S. Williams, D. Liu, *Representation of primes by the principal form of negative discriminant* Δ *when* $h(\Delta)$ *is* 4, Tamkang J. Math. **25** (1994), 321–334

[111] D. A. Buell, V. Ennola, *On a parameterized family of quadratic and cubic fields*, J. Number Theory **54** (1995), 134–148

[112] M. Daberkow, *On the explicit arithmetic computation of Hilbert class fields*, Tagungsber. Oberwolfach **21** (1995)

[113] M. Daberkow, M. Pohst, *Computations with relative extensions of number fields with an application to the construction of Hilbert class fields*, Proc. ISAAC '95 (1995), ACM Press, New York, 68–76

[114] T. Kondo, *Algebraic number fields with the discriminant equal to that of a quadratic number field*, J. Math. Soc. Japan **47** (1995), 31–36

[115] F. Lemmermeyer, *Explizite Konstruktion von Hilbert-Klassenkörpern*, Diss. Univ. Heidelberg (1995)

[116] F. Lemmermeyer, A. Pethö, *Simplest cubic fields*, Manuscripta Math. **88** (1995), 53–58

[117] P. J. Sime, *Hilbert class fields of real biquadratic fields*, J. Number Theory **50** (1995), 154–166

[118] H. Cohen, F. Diaz y Diaz, M. Olivier, *Computing ray class groups, conductors and discriminants*, Algorithmic Number Theory (Talence, 1996), 49—57, Lecture Notes Comp. Sci. **1122**, Springer 1996

[119] M. Daberkow, M. Pohst, *On the Computation of Hilbert class fields*, J. Number Theory **69** (1998), 213–230;

[120] M. Daberkow, M. Pohst, *On computing Hilbert class fields of prime degree*, Algorithmic Number Theory (Talence, 1996), 67–74, Lecture Notes Comp. Sci. **1122**, Springer 1996

[121] D.S. Dummit, D.R. Hayes, *Checking the* $\mathfrak{p}$*-adic Stark conjecture when* $\mathfrak{p}$ *is Archimedean*, Algorithmic Number Theory (Talence, 1996), 91–97, Lecture Notes Comp. Sci. **1122**, Springer 1996

[122] F. Lemmermeyer, *Unramified quaternion extensions of quadratic number fields*, J. Théor. Nombres Bordeaux **9** (1997), 51–68

[123] M. Pohst, *Computational aspects of Kummer Theory*, ANTS II (1996)

[124] E. Sasajima, *A family of quintic polynomials with Galois group* D_{10} (Japan.), Master thesis, Tokyo Woman's Chr. Univ. 1996

[125] T. Kondo, *Some examples of unramified extensions over quadratic fields*, Sci. Rep. Tokyo Woman's Chr. Univ. **121–124** (1997), 1399–1410

[126] Y. Kishi, K. Miyake, *Characterization of the quadratic fields whose class numbers are divisible by three*, Tokyo Metrop. Univ. preprint **7** (1997)

[127] A. Gee, P. Stevenhagen, *Generating class fields using Shimura reciprocity*, ANTS 1998, 441–453, Lecture Notes in Comput. Sci. 1423, Springer 1998

[128] Y. Kishi, *A criterion for a certain type of imaginary quadratic fields to have* 3*-ranks of the ideal class groups greater than one*, Proc. Japan Acad. Sci. **74** (1998), 93–97

[129] M. Sase, *On a family of quadratic fields whose class numbers are divisible by five*, Proc. Japan Acad. Math. Sci. **74** (1998), no. 7, 120–123

[130] Y. Kishi, *Spiegelung-relations between* 3*-ranks of absolute ideal class groups and congruent Ones Modulo* $(3)^2$ *in quadratic fields*, Tokyo Metrop. Univ. preprint **2** (1999)

[131] Y. Kishi, *A constructive approach to Spiegelung relations between* 3*-ranks of absolute ideal class groups and congruent one modulo* $(3)^2$ *in quadratic fields*, J. Number Theory **83** (2000), 1–49

[132] Y. Kishi, K. Miyake, *Parametrization of the quadratic fields whose class numbers are divisible by three*, J. Number Theory **80** (2000), 209–217

[133] T. Komatsu, *On unramified cyclic cubic extensions of real quadratic fields*, preprint 2000

[134] A. Azizi, *Construction de la tour des* 2*-corps de classes de Hilbert de certains corps biquadratiques*, Pacific J. Math. **208** (2003), 1–10

[135] Y. Kishi, *A note on the* 3*-rank of quadratic fields*, Arch. Math. **81** (2003), no. 5, 520–523

II. Class Field Towers

[136] A. Scholz, *Zwei Bemerkungen zum Klassenkörperturm*, J. Reine Angew. Math. **161** (1929), 201–207

[137] A. Scholz, *Über das Verhältnis von Idealklassen- und Einheitengruppen in Abelschen Körpern von Primzahlpotenzgrad*, Sitzungsber. Heidelberger Akad. Wiss. **3** (1930), 31–55

[138] Moriya, *Eine Bemerkung ueber die Klassenzahl der absoluten Klassenkörper*, Proc. Imp. Acad. Jap. **10** (1934), 623–625

[139] L. Holzer, *Aufgabe 192*, Jahresber. DMV **45** (1935), 23–24

[140] H. Hasse, *Lösung der Aufgabe 192*, Jahresber. DMV **46** (1936), 58

[141] O. Taussky, *A remark on the class field tower*, J. London Math. Soc. **12** (1937), 82–85

[142] O. Taussky, *A remark on unramified class fields*, J. London Math. Soc. **12** (1937), 86–88

[143] A. Fröhlich, *A note on the class field tower*, Quart. J. Math. Oxford (2) **5** (1954), 141-144

[144] A. Fröhlich, *A remark on the class field tower of* $\mathbb{Q}(\sqrt[\ell]{m})$, J. London Math. Soc. **37** (1962), 193–194

[145] J. Browkin, *On the generalized class field tower*, Bull. Acad. Pol. Sci. ser. sci. math. astr. phys. **27** (1963), 143–145

[146] J. Browkin, *Examples of maximal* 3*-extensions with two ramified places*, Izv. Akad. Nauk. **27** (1963), 613–620

[147] H. Koch, *Über den* 2*-Klassenkörperturm eines quadratischen Zahlkörpers. I*, J. Reine Angew. Math. **214/215** (1963), 201–206

[148] E. S. Golod, I. R. Shafarevich, *Infinite class field towers of quadratic fields (Russ.)*, Izv. Akad. Nauk. SSSR **28** (1964), 273–276; see also AMS Transl. **48** (1965), 91–102, or the Collected Papers of Safarevic, p. 317–328

[149] K. Hoechsmann, *Tagungsbericht der AG über das Klassenkörperturmproblem*, Tagungsber. Math. Forsch.-Inst. Oberwolfach, 18.–23.10.1964

[150] A. Brumer, *Ramification and class field towers of number fields*, Michigan Math. J. **12** (1965), 129–131

[151] E. B. Vinberg, *On the dimension theorem of associative algebras* (Russ.), Izv. Ak. Nauk. SSSR **29** (1965), 209–214

[152] G. Panella, *Un teorema di Golod-Safarevic e alcune sue conseguenze*, Confer. Sem. Math. Univ. Bari **104** (1966), 1-17

[153] J. P. Serre, *Existence de tours infinies de corps de classes d'après Golod et Safarevic*, Coll. papers **III** (1960–1971), 289–296

[154] E. Lamprecht, *Existenz von Zahlkörpern mit nicht abbrechendem Klassenkörperturm*, Arch. Math. **18** (1967), 140–152

[155] P. Roquette, *On class field towers*, Algebraic number theory (J. W. Cassels, A. Fröhlich, eds), Academic Press New York 1967 231–249

[156] H. Koch, *Zum Satz von Golod-Schafarewitsch*, Math. Nachr. **42** (1969), 321–333

[157] J. H. Smith, *A remark on fields with unramified composition*, J. London Math. Soc. (2) **2** (1969), 1–2

[158] W. Gaschütz, M. F. Newman, *On presentations of finite p-groups*, J. Reine Angew. Math. **245** (1970), 172–176

[159] Y. Furuta, *On class field towers and the rank of ideal class groups*, Nagoya Math. J. **48** (1972), 147–157

[160] J. Martinet, *Tours de corps de classes et estimations de disriminants*, Séminaire de Théorie des Nombres Bordeaux 1974, Astérisque **24/25** 57–67

[161] B. B. Venkov, H. Koch, *The p-tower of class fields for an imaginary quadratic field* (russ.), Zapiski nauch. Sem. Leningrad. Otd. mat. Inst. Steklov. **46** (1974), 5-15

[162] E. W. Zink, *Über die Klassengruppe einer absolut zyklischen Erweiterung*, Diss. Humboldt Univ. Berlin (1974)

[163] H. Koch, B. B. Venkov, *Über den p-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers*, Journées arithmetiques Bordeaux 1974, Astérisque **24/2**5 (1975), 57–67

[164] S. Shirai, *Central class numbers in central class field towers*, Proc. Japan Acad. **51** (1975), 389–393

[165] N. Matsumura, *On the class field tower of an imaginary quadratic number field*, Mem. Fac. Sci. Kyushu Univ. **A 31** (1977), 165–177

[166] J. Martinet, *Tours de corps de classes et estimations de disriminants*, Invent. Math. **44** (1978), 65–73

[167] B. B. Venkov, H. Koch, *The p-tower of class fields for an imaginary quadratic field* (russ.), J. Sov. Math. **9** (1978), 291–299

[168] R. Schoof, *Class field towers*, Doctoraalskriptie Amsterdam (1979)

[169] T. Takeuchi, *Note on the class field towers of cyclic fields of degree ℓ*, Tôhoku Math. J. **31** (1979), 301–307

[170] B. Schmithals, *Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturm*, Arch. Math. **34** (1980), 307–312

[171] T. Takeuchi, *On the ℓ-class field towers of cyclic fields of degree ℓ*, Sci. Rep. Niigata Univ. A **17** (1980), 23–25

[172] M. Hamamura, *On absolute class fields of certain algebraic number fields*, Natur. Sci. Rep. Ochanomitu Univ. **32** (1981), 23–34

[173] G. Cornell, *Exponential growth of the ℓ-rank of the class group of the maximal real subfield of cyclotomic fields*, Bull. Amer. Math. Soc. **8** (1983), 55–58

[174] R. Schoof, *Infinite class field towers of quadratic fields, Elliptic Curves and class groups*; thesis, Amsterdam (1983)

[175] J. R. Brink, *The class field tower of imaginary quadratic number fields of type* $(3,3)$ Ph. D. Diss. Ohio State Univ (1984), 121pp

[176] Y. Furuta, *Supplementary notes on Galois groups of central extensions of algebraic number fields*, Sci. Rep. Kanazawa Univ. **29** (1984), 9–14

[177] H. Hayashi, *Elliptic units and genus theory*, Abh. Math. Semin. Univ. Hamb. **55** (1985), 19–29

[178] H. Naito, *On the ideal class groups of totally imaginary quadratic extensions*, J. Fac. Sci. Univ. Tokyo **32** (1985), 205–211

[179] R. Schoof, *Infinite class field towers of quadratic fields*, J. Reine Angew. Math. **372** (1986), 209–220

[180] K. Yamamura, *On infinite unramified Galois extensions of algebraic number fields with many primes decomposing completely*, J. Math. Soc. Japan **38** (1986), 599–605

[181] X. Zhang, *Counterexample and correction about genus fields of number fields*, J. Number Theory **23** (1986), 318–321

[182] J. R. Brink, R. Gold, *Class field towers of imaginary quadratic fields*, Manuscripta Math. **57** (1987), 425–450

[183] H. Naito, *On ℓ^3-divisibility of class numbers of ℓ-cyclic extensions*, Proc. Symbp. RIMS, Algebraic Number Theory, Kyoto/Jap. 1986, RIMS Kokyuroku **603** (1987), 87–92

[184] H. Kisilevsky, J. Labute, *On a sufficient condition for the p-class field tower of a CM-field to be infinite*, Sém. Théor. Nombres, Univ. Laval (1987), 556–560

[185] N. Boston, *Some cases of the Fontaine-Mazur conjecture*, J. Number Theory **42** (1992), 285–291

[186] K. Miyake, *On the ideal class groups of the p-class fields of quadratic number fields*, Proc. Japan Acad., Ser. A **68** (1992), 62–67

[187] K. Miyake, *Notes on the ideal class groups of the p-class fields of some algebraic number fields*, Proc. Japan Acad., Ser. A **68** (1992), 79–84

[188] K. Miyake, *Some p-groups with two generators which satisfy certain conditions arising from arithmetic in imaginary quadratic number fields*, Tôhoku Math. J. **44** (1992), 443–469

[189] E. Benjamin, *Results concerning the 2-Hilbert class field of imaginary quadratic number fields*, Bull. Austral. Math. Soc. **48** (1993), 379–383 Corr.: ibid **50** (1994), 352–352

[190] A. Nomura, *On the class number of certain Hilbert class fields*, Manuscr. Math. **79** (1993), 379–390

[191] K. Wingberg, *On the maximal unramified p-extension of an algebraic number field*, J. Reine Angew. Math. **440** (1993), 129–156

[192] F. Hajir, *Calculating the class number of certain Hilbert class fields*, (Abstract) Algorithmic number theory. 1st international symposium, ANTS-I, Ithaca, NY, USA, May 6-9, 1994, Lect. Notes Comput. Sci. **877** (1994), 248

[193] F. Lemmermeyer, *On the 2-class field tower of imaginary quadratic number fields*, J. Théorie d. Nombres Bordeaux **6** (1994), 261–272

[194] S. Louboutin, *Calcul des nombres de classes relatifs de certain corps de classes de Hilbert*, C. R. Acad. Sci. Paris **319** (1994), 321–325

[195] M. Arrigoni, *On Schur σ-Groups*, Tokyo Metropolitan University Mathematics Preprint Series, 1995

[196] E. Benjamin, Ch. Snyder, *Real Quadratic Number fields with* 2*-class groups of type* (2, 2), Math. Scand. **76** (1995), 161-178

[197] N. Boston, *Some cases of the Fontaine-Mazur conjecture, II*, (to appear)

[198] F. Hajir, *On the growth of p-class groups in p-class field towers*, J. Algebra **188** (1997), 256-271

[199] F. Hajir, *On a theorem of Koch*, Pac. J. Math. **176** (1996), 15–18; Corr: ibid ?? (2001),

[200] A. Nomura, *A remark on Boston's question concerning the existence of unramified p-extensions*, J. Number Theory **58** (1996), 66–70

[201] E. Benjamin, *Lower bounds on the* 2*-class number of the* 2*-Hilbert class field of imaginary quadratic number fields with elementary abelian* 2*-class group of rank* 3, Houston J. Math. **22** (1996), 11–37

[202] E. Benjamin, F. Lemmermeyer, C. Snyder, *Imaginary quadratic fields k with cyclic* $\mathrm{Cl}_2(k^1)$, J. Number Theory **67** (1997), 229–245

[203] F. Lemmermeyer, *The* 4*-class group of real quadratic number fields*, preprint 1996

[204] S. Louboutin, *Corps quadratiques à corps de classes de Hilbert principaux et à multiplication complexe*, Acta Arith. **74** (1996), 121–140

[205] S. Louboutin, R. Okazaki, *The class number one problem for some non-abelian normal CM-fields of* 2*-power degrees*, Proc. London Math. Soc. **76** (1998), 523–548

[206] C. Maire, *Finitude de tours et p-tours T-ramifiées modérées, S-décomposées*, J. Théor. Nombres Bordeaux **8** (1996), 47–73

[207] C. Maire, *Tours de Hilbert des extensions cubiques cycliques de* $\mathbb{Q}$, Manuscr. Math. **92** (1997), 303–323

[208] C. Maire, *Compléments à un résultat de Safarevic*, Math. Nachr. **198** (1999), 149–168

[209] C. Maire, *Un raffinement du théorème de Golod-Safarevic*, Nagoya Math. J. **150** (1998), 1–11

[210] K. Yamamura, *The maximal unramified extensions of the imaginary quadratic number fields with class number two*, J. Number Theory **60** (1996), 42–50

[211] K. Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors*, Proc. Japan Acad. **73** (1997), 67-71

[212] K. Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors*, J. Théor. Nombres Bordeaux **9** (1997), 405–448

[213] M. Arrigoni, *On Schur σ-Groups*, Math. Nachr. **192** (1998), 71–89

[214] E. Benjamin, F. Lemmermeyer, C. Snyder, *Real quadratic fields with Abelian* 2*-class field tower*, J. Number Theory **73** (1998), 182–194

[215] E. Benjamin, *On the second Hilbert* 2*-class field of real quadratic number fields with* 2*-class groups isomorphic to* $(2, 2^n)$, Rocky Mt. J. Math. **29** (1999), 763–788

[216] E. Benjamin, *Lower bounds on the* 2*-class number of the Hilbert* 2*-class field of quadratic number fields with* 2*-class number greater than or equal to* 16, Fat East J. Math. Sci. **1** (1999), 101–119

[217] A. Nomura, *On embedding problems with restricted ramifications*, Arch. Math. **73** (1999), no. 3, 199–204

[218] E. Benjamin, F. Lemmermeyer, C. Snyder, *Imaginary quadratic fields with* $Cl_2(k) = (2, 2^m)$ *and rank* $Cl_2(k^1) = 2$, Pac. J. Math. **198** (2001), no. 1, 15–31

[219] E. Benjamin, Ch. Parry, *Refined lower bounds on the* 2*-class number of the Hilbert* 2*-class field of imaginary quadratic number fields with elementary* 2*-class group of rank* 3, J. Number Theory **76** (1999), no. 2, 167–177

[220] E. Benjamin, *On the second Hilbert* 2*-class field of real quadratic number fields with 2-class group isomorphic to* $(2, 2^n)$*,* $n \geq 2$, Rocky Mountain J. Math. **29** (1999), no. 3, 763–788

[221] A. Nomura, *Embedding problems with restricted ramifications and the class number of Hilbert class fields*, Class field theory—its centenary and prospect (Tokyo, 1998), 79–86, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001

[222] K. Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors. II*, J. Théor. Nombres Bordeaux **13** (2001), no. 2, 633–649

[223] F. Hajir, Ch. Maire, *Unramified subextensions of ray class field towers*, J. Algebra **249** (2002), no. 2, 528–543

[224] E. Benjamin, *On a question of Martinet concerning the* 2*-class field tower of imaginary quadratic number field*, Ann. Sci. Math. Quebec **26** (2002), no. 1, 1–13

[225] M.R. Bush, *Computation of Galois groups associated to the* 2*-class towers of some quadratic fields*, J. Number Theory **100** (2003), 313–325

[226] E. Benjamin, *A note on imaginary quadratic number fields with* $C_{k,2} \cong (4, 4)$, JP J. Algebra Number Theory Appl. **3** (2003), no. 2, 269–276

[227] Y. Sueyoshi, *Infinite* 2*-class field towers of some imaginary quadratic number fields*, Acta Arith. **113** (2004), no. 3, 251–257

[228] K. Yamamura, *On quadratic number fields each having an unramified extension which properly contains the Hilbert class field of its genus field*, Galois theory and modular forms, 271–286, Dev. Math. 11, Kluwer 2004

III. Genus Class Fields

[229] Th. Skolem, *Geschlechter und Reziprozitätsgesetze*, Norsk. Math. Forenings Skrifter (1) **18** (1928), 38pp

[230] J. Herbrand, *Sur les théorèmes du genre principal et des idéaux principaux*, Abh. Math. Sem. Hamburg **9** (1932), 84–92

[231] E. Noether, *Der Hauptgeschlechtssatz für relativ-galoische Zahlkörper*, Math. Ann. **108** (1933), 411–419

[232] E. Inaba, *Klassenkörpertheoretische Deutung der Struktur der Klassengruppe des zyklischen Zahlkörpers*, Proc. Imper. Acad. Japan Tokyo **17** (1941), 125–128

[233] H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3** (1951), 45–51

[234] H. Brandt, *Binäre quadratische Formen im Gaußschen Zahlkörper*, Math. Nachr. **7** (1952), 151–158

[235] H. Brandt, *Das quadratische Reziprozitätsgesetz im Gauss'schen Zahlkörper*, Comment. Math. Helvet. **26** (1952), 42–54

[236] F. Terada, *On the principal genus theorem concerning the abelian extensions*, Tôhoku Math. J. **4** (1952), 141–152

[237] H. W. Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9** (1953), 351–362

[238] F. Terada, *A note on the principal genus theorem*, Tôhoku Math. J. **5** (1953), 211–213

[239] H. Kuniyoshi, S. Takahashi, *On the principal genus theorem*, Tôhoku Math. J. **5** (1955), 128–131

[240] A. Fröhlich, *The genus field and genus group in number fields I*, Mathematica **6** (1959), 40–46

[241] A. Fröhlich, *The genus field and genus group in number fields II*, Mathematica **6** (1959), 142–146

[242] Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. **29** (1967), 281–285

[243] H. Hasse, *A supplement to Leopoldt's theory of genera in abelian number fields*, J. number theory **1** (1969), 4–7

[244] H. Hasse, *Eine Folgerung aus H.-W.- Leopoldts Theorie der Geschlechter abelscher Zahlkörper*, Math. Nachr. **42** (1969), 261–262

[245] Y. Furuta, *Über das Geschlecht und die Klassenzahl eines relativ-Galoischen Zahlkörpers vom Primzahlpotenzgrade*, Nagoya Math. J. **37** (1970), 197–200

[246] H. Wada, *On cubic Galois extensions of* $\mathbb{Q}(\sqrt{-3})$, Proc. Japan Acad. **46** (1970), 397–400

[247] G. Cornell, *Abhyankar's Lemma and the class group*, Number Theory Carbondale 1971, Lecture notes in Math. **751** (1973), 82–88

[248] Y. Furuta, *Über die zentrale Klassenzahl eines relativ-Galoischen Zahlkörpers*, J. Number Theory **3** (1971), 318–322

[249] L. J. Goldstein, *On prime discriminants*, Magoya Math. J. **45** (1971), 119–127

[250] J. Martinet, *A propos de classes d'idéaux*, Sém. Théor. Nombres Bordeaux (1971/72), no. 5, 10pp

[251] J. Sunley, *Remarks concerning generalized prime discriminants*, Proc. of the 1972 number theory conference, Boulder, Colorado 233–237

[252] C. E. Taylor, *The genus number and pure extensions of the rationals*, Ph. D. thesis Kansas (1972)

[253] T. R. Butts, *On the genus field and its application to four problems in algebraic number fields*, Ph.D.-Thesis, Michigan State Univ. (1973)

[254] N. Nakagoshi, *On indices of unit groups related to the genus number of Galois extensions*, Sci. Rep. Kanazawa Univ. **20** (1975), 7–13

[255] R. Gold, *Genera in normal extensions*, Pac. J. Math. **63** (1976), 397–400

[256] M. Ishida, *The genus fields of algebraic number fields*, Lecture Notes Math. **555** (1976), Springer Verlag

[257] H. Stark, *The genus theory of number fields*, Comm. Pure Appl. Math. **29** (1976), 805–811

[258] R. Gold, *The principal genus and Hasse's norm theorem*, Indian J. Math. **26** (1977), 183–189

[259] R. Gold, M. L. Madan, *The principal genus and Hasse's norm theorem*, Indian J. Math. **21** (1977), 66–69

[260] S. J. Gurak, *Ideal-theoretic characterization of the relative genus field*, J. Reine Angew. Math. **296** (1977), 119–124

[261] Y. Kubokawa, *The genus field for composite quadratic fields*, J. Saitama Univ. Fac. Ed. Math. Natur. Sci. **26** (1977), 1–3

[262] M. Razar, *Central and genus class field and the Hasse norm theorem*, Compositio Math. **35** (1977), 281–298

[263] G. Cornell, *Genus fields and class groups of number fields*, Thesis, Brown Univ. (1978)

[264] D. N. Davis, *The prime discriminant factorization of discriminants of algebraic number fields*, Ph. D. Diss. Univ. Florida (1978)

[265] D. A. Garbanati, *The Hasse Norm Theorem for non-cyclic extensions for the rationals*, Proc. London Math. Soc. **37** (1978), 143–164

[266] R. Gold, M. L. Madan, *Some applications of Abhyankar's lemma*, Math. Nachr.**82** (1978), 115–119

[267] F. Halter-Koch, *Eine allgemeine Geschlechtertheorie und ihre Anwendung auf Teilbarkeitsaussagen für Klassenzahlen algebraischer Zahlkörper*, Math. Ann. **233** (1978), 55–63

[268] S. Shirai, *On the central class field mod* $\mathfrak{m}$ *of Galois extensions of an algebraic number field*, Nagoya Math. J. **71** (1978), 61–85

[269] A. A. Antropov, *On the history of the notion of genus of a binary quadratic form*, (Russ.) Istor. Metodol. Estestv. Nauk **36** (1979), 17–27

[270] M. Bhaskaran, *Construction of genus field and some applications*, J. Number Theory **11** (1979), 488–497 Corr.: ibid **19** (1984), 449–451

[271] G. Frei, *On the development of the genus group in number fields*, Ann. Sci. math. Quebec **3** (1979), 5–62

[272] F. Halter-Koch, *Zur Geschlechtertheorie algebraischer Zahlkörper*, Arch. Math. **31** (1979), 137–142

[273] W. Jehne, *On knots in algebraic number theory*, J. Reine Angew. Math. **311/312** (1979), 215–254

[274] S. Shirai, *On the central ideal class group of cyclotomic fields*, Nagoya Math. J. **75** (1979), 133–143

[275] J. Sunley, *Prime discriminants in real quadratic fields of narrow class number one*, Number Theory Carbondale 1971, Lecture Notes Math. **751** 294–301

[276] M. Ishida, *On the genus field of pure number fields I*, Tokyo J. Math. **3** (1980), 163–171

[277] C. J. Parry, *A genus theory for quartic fields*, J. Reine Angew. Math. **314** (1980), 40–71

[278] M. Ishida, *On the genus field of pure number fields II*, Tokyo J. Math. **4** (1981), 213–220

[279] W. Jehne, *Der Hassesche Normensatz und seine Entwicklung*, Mitt. Math. Ges. Hamb. **11** (1982), 143–153

[280] D. Zagier, *Zetafunktionen und quadratische Körper*, Springer Verlag (1981),

[281] G. Cornell, *On the construction of relative genus fields*, Trans. Amer. Math. Soc. **271** (1982), 501–511

[282] H. Furuya, *Ambiguous numbers over* $\mathbb{Q}(\zeta_3)$ *of absolutely abelian extensions of degree* 6, Tokyo J. Math. **5** (1982), 457–462

[283] K. Takase, *Some remarks on the relative genus fields*, Kodai Math. J. **5** (1982), 482–494

[284] T. Takeuchi, *Genus number and* ℓ*-rank of genus group of cyclic extensions of degree* ℓ, Manuscripta Math. **39** (1982), 99–109

[285] G. Cornell, *Relative genus theory and the class group of ℓ-extensions*, Trans. Amer. Math. Soc. **277** (1983), 421–429

[286] A. Fröhlich, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemp. Math **24**, Amer. Math. Soc. 1983

[287] S. B. Watt, *Genus fields and central extensions of number fields*, Diss. Univ. Illinois (1983)

[288] M. Bhaskaran, *Some further remarks on genus field*, J. Number Theory **21** (1985), 256–259

[289] Zh. Xianke, *A simple construction of genus fields of abelian number fields*, Proc. Amer. Math. Soc. **94** (1985), 393–395

[290] G. Cornell, *Genus theory and the class group of number fields*, Proceedings of the Internat. Conf. on Class numbers and Fundamental units of algebraic number fields, Katata Japan (1986), 109–123

[291] M. Horie, *A note on central class fields*, Abh. Math. Sem. Hamburg **57** (1986), 119–125

[292] T. Takeuchi, *Genus group of finite Galois extensions*, Proc. Am. Math. Soc. **98** (1986), 211–214

[293] M. Bhaskaran, *Letter to the editor*, J. Number Theory **27** (1987), 111–112

[294] R. Bond, *Unramified abelian extensions of number fields*, J. Number Theory **30** (1988), 1–10

[295] M. Ishida, *Existence of unramified cyclic extensions and congruence conditions*, Acta Arith. **51** (1988), 75–84

[296] S. V. Ulom, S. B. Watt, *Class number restrictions for certain ℓ-extensions of imaginary quadratic fields*, Illinois J. Math. **32** (1988 422–427

[297] W. Y. Vélez, *The factorization of p in $\mathbb{Q}(a^{1/p^k})$ and the genus field of $\mathbb{Q}(a^{1/n})$*, Tokyo J. Math. **11** (1988), 1–19

[298] D. Cox, *Primes of the form $x^2 + ny^2$; Fermat, Class Field Theory, and Complex Multiplication*, J. Wiley & Sons 1989

[299] S. Louboutin, *Norme relative de l'unité fondamentale et 2-rang du groupe des classes de certains corps biquadratiques*, Acta Arith. **58** (1991), 273–288

[300] F. Lemmermeyer, *Separants of number fields*, Preprint 1994

[301] B. K. Spearman, K. S. Williams, *Unramified quadratic extensions of a quadratic field*, Rocky Mt. J. Math. **25** (1995), 783–788

[302] , B. Anglés, J.-F. Jaulent, *Sur la théorie des genres pour les corps globaux*, Manuscr. Math. **101** (2000), no. 4, 513–532

[303] M. Ozaki, *An application of Iwasawa theory to constructing fields $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ which have class group with large p-rank*, Nagoya Math. J. **169** (2003), 179–190

IV. Ranks of Class Groups

[304] E. Hecke, *Über nicht-reguläre Primzahlen und den Fermatschen Satz*, Nachr. Akad. Wiss. Göttingen (1910), 420–424

[305] H.S. Vandiver, *On the first factor of the class number of a cyclotomic field*, Bull. Amer. Mth. Soc. **25** (1919), 458–461

[306] T. Takagi, *Zur Theorie des Kreiskörpers*, J. Reine Angew. Math. **157** (1927), 246–255

[307] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math. **166** (1932), 201–203

[308] M. Moriya, *über die Klassenzahl eines relativ-zyklischen Zahlkörpers*, Jap. J. Math. **10** (1933), 1–10

[309] O. Grün, *Aufgabe* 153; Lösungen von L. Holzer und A. Scholz, Jahresber. DMV **45** (1934), 74–75 (kursiv)

[310] H. Reichardt, *Arithmetische Theorie der kubischen Körper als Radikalkörper*, Monatsh. Math. Phys. **40** (1933), 323–350

[311] Billing, Nova Acta Regiae Soc. Sci. Uppsal. (4) **11** (1938), 1–165

[312] E. Inaba, *Über die Struktur der ℓ-Klassengruppe zyklischer Zahlkörper von Primzahlgrad ℓ*, J. Fac. Sci. Tokyo **I 4** (1940), 61–115

[313] H. W. Leopoldt, *Zur Struktur der ℓ-Klassengruppe galoisscher Zahlkörper*, J. Reine Angew. Math. **199** (1958), 165–174

[314] K. Shiratani, *Bemerkung zur Theorie der Kreiskörper*, Mem. Fac. Sci. Kyushu Univ. **18** (1964), 121–126

[315] A. Yokoyama, *Über die Relativklassenzahl eines relativ-Galoischen Zahlkörpers von Primzahlpotenzgrad*, Tôhoku Math. J. **18** (1966), 318–324

[316] J. Smith, *A remark on class numbers of number field extensions*, Proc Amer. Math. Soc. **20** (1969), 388–390

[317] P. Damey, J.-J. Payan, *Existence et construction des extensions galoisiennes et non-abéliennes de degré* 8 *d'un corps de caractéristique différente de* 2, J. Reine Angew. Math. **244** (1970), 37–54

[318] S.-N. Kuroda, *Über den allgemeinen Spiegelungssatz für Galoissche Zahlkörper*, J. Number Theory **2** (1970), 282–297

[319] H. Heilbronn, *On the* 2*-classgroup of cubic fields*, in: Studies in Pure Math. (L. Mirsky, ed.) Academic Press 1971 117–119; see also Collected Works, 548–550

[320] A. Kudo, *On the reflection theorem in prime cyclotomic fields*, Mem. Fac. Sci. Kyushu Univ. **26** (1972), 333–337

[321] F. Gerth III, *Ranks of Sylow* 3*-subgroups of ideal class groups of certain cubic fields*, Bull. Amer. Math. Soc. **79** (1973), 521–525

[322] R. Gillard, *Problème de plongement et constraintes galoisiennes sur le groupe des classes*, Sém. Théor. Nombres Grenobles, 1973

[323] G. Gras, *Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ*, Ann. Inst. Fourier **23.3** (1973), 1-48, ibid. **23.4**, 1-44

[324] S. Kobayashi, *On the* 3*-rank of the ideal class groups of certain pure cubic fields*, J. Fac. Sci., Univ. Tokyo, Sect. I A **20** (1973), 209–216

[325] T. Callahan, *The* 3*-class group of non-Galois cubic fields I, II*, Mathematika **21** (1974), 72–89, 168–188

[326] G. Gras, *Sur les ℓ-classes d'idéaux des extensions non galoisiennes de degré premier impair ℓ à la clôture galoisiennes diédrale de degré 2ℓ*, J. Math. Soc. Japan **26** (1974), 677–685

[327] S. Kobayashi, *On the ℓ-class rank in some algebraic number fields*, J. math. Soc. Japan **26** (1974), 668–676

[328] S. Kobayashi, *On the* 3*-rank of the ideal class groups of certain pure cubic fields II*, J. Fac. Sci., Univ. Tokyo, Sect. I A **21** (1974), 263–270

[329] J. Bloom, *On the* 4*-rank of the strict class group of a quadratic number field*, Selected Topics on Ternary Forms and Norms, Sem. Number Theory, Calif. Instit. Tech., Pasadena (1974/75)

[330] G. Frey, *Die Klassengruppe quadratischer und kubischer Zahlkörper und die Selmer-Gruppen gewisser elliptischer Kurven*, Manuscr. Math. **16** (1975), 333–362

[331] F. Gerth, *On* 3*-class groups of pure cubic fields*, J. Reine Angew. Math. **278/279** (1975), 52-62

[332] H. Kisilevsky, *The Rédei-Reichardt-theorem – a new proof*, Selected Topics on Ternary Forms and Norms, Sem. Number Theory, Calif. Instit. Tech., Pasadena (1974/75)

[333] R. Bölling, *Über den* 3*-Rang von quadratischen Zahlkörpern und den Rang gewisser elliptischer Kurven*, Math. Nachr. **73** (1976), 155–170

[334] T. Callahan, *Dihedral field extensions of order* $2p$ *whose class numbers are multiples of* p, Canad. J. Math. **28** (1976), 429–439

[335] F. Gerth III, *On* 3*-class groups of cyclic cubic extensions of certain number fields*, J. Number Theory **8** (1976), 84–98

[336] F. Gerth III, *Rank of* 3*-class groups of non-Galois cubic fields*, Acta Arith. **30** (1976), 308–322

[337] B. Oriat, *Spiegelungssatz*, Publ. Math. Fac. Sci. Besançon 1975/76

[338] P. Satgé, *Inégalités de miroir*, Sem. Delange-Pisot-Poitou (1967/77), **18** 4pp

[339] A. Brumer, K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–743

[340] D. A. Buell, *Elliptic curves and class groups of quadratic fields*, J. London Math. Soc. **15** (1977), 19–25

[341] H. Eisenbeis, *Die Berechnung der* 2*-Klassenzahl des rein kubischen Körpers* $\mathbb{Q}(\sqrt[3]{k})$ *mit Hilfe der Selmergruppen der elliptischen Kurven* $y^2 = x^3 \pm k$, Diss. Univ. Saarbrücken, 1977

[342] B. Ommerborn, *Die Berechnung der* 2*-Klassenzahl des rein kubischen Körpers* $\mathbb{Q}(\sqrt[3]{k})$ *mit Hilfe der Selmergruppen der elliptischen Kurven* $y^2 = x^3 \pm k$, Diss. Univ. Saarbrücken, 1977

[343] S. Kobayashi, *Complete determinations of the* 3*-class rank in pure cubic fields*, J. math. Soc. Japan **29** (1977), 373–384

[344] B. Oriat, *Relations entre les* 2*-groupes d'idéaux de* $k(\sqrt{d})$ *et* $k(\sqrt{-d})$, Astérisque **41–42** (1977), 247–249

[345] B. Oriat, *Relations entre les* 2*-groupes d'idéaux des extensions quadratiques* $k(\sqrt{d})$ *et* $k(\sqrt{-d})$, Ann. Inst. Fourier **27** (1977), 37–60

[346] H. Eisenbeis, G. Frey, B. Ommerborn, *Computation of the* 2*-rank of pure cubic number fields*, Math. Comp. **32** (1978), 559–569

[347] B. Oriat, *Sur le divisibilité par* 8 *et* 16 *des nombres de classes d'idéaux des corps quadratiques* $\mathbb{Q}(\sqrt{2p})$ *et* $\mathbb{Q}(\sqrt{-2p})$, J. Math. Soc. Japan **30** (1978), 279–285

[348] K. Iimura, *Dihedral extensions of* $\mathbb{Q}$ *of degree* 2ℓ *which contain non-Galois extensions with class number not divisible by* ℓ, Acta Arith. **35** (1979), 385–394

[349] B. Oriat, *Generalisation du 'Spiegelungssatz'*, Astérisque **61** (1979), 169–175

[350] B. Oriat, P. Satgé, *Un essai de generalisation du 'Spiegelungssatz'*, J. Reine Angew. Math. **307/308** (1979), 134–159

[351] R. Bölling, *Über einen Homomorphismus der rationalen Punkte elliptischer Kurven*, Math. Nachr. **96** (1980), 207–244

[352] R. Bölling, *Zur Klassenzahl nicht galoisscher Körper in Diedererweiterungen über* $\mathbb{Q}$ *mit besonderer Berücksichtigung kubischer Körper. I*, Math. Nachr. **118** (1984), 271–284

[353] F. Halter-Koch, *Über den* 4*-Rang der Klassengruppe quadratischer Zahlkörper*, J. Number Theory **19** (1984), 219–227

[354] P. Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory **23** (1986), 249–317

[355] J. Quer, *Corps quadratiques de* 3*-rang* 6 *et courbes elliptiques de* 3*-rang* 12, C. R. Acad. Sci. Paris **305** (1987), 215–218

[356] R. Bölling, *On ranks of class groups of fields in dihedral extensions over* $\mathbb{Q}$ *with special reference to cubic fields*, Math. Nachr. **135** (1988), 275–310

[357] J. Brinkhuis, *Galois module and the Spiegelungssatz*, Tagungsber. Oberwolfach, 35/1988

[358] G. Frey, *On the Selmer group of twists of elliptic curves with* $\mathbb{Q}$*-rational torsion points*, Can. J. Math. **40** (1988), 649–665

[359] R. Ernvall, *A generalization of Herbrand's theorem*, Ann. Univ. Turku **193** (1989), 15 pp.

[360] T. Uehara, *On the* 4*-rank of the narrow ideal class group of a quadratic field*, J. Number Theory **31** (1989), 167–173

[361] J. Nekovar, *Class numbers of quadratic fields and Shimura correspondence*, Math. Ann. **287** (1990), 577–594

[362] S. Schild, *Selmer-Gruppen von Twists elliptischer Kurven und ihr Zusammenhang mit Klassengruppen von quadratischen Zahlkörpern*, Diplomarbeit Saarbrücken, 1991

[363] M. Kawachi, S. Nakano, *The* 2*-class groups of cubic fields and* 2*-descents on elliptic curves*, Tôhoku Math. J. **44** (1992), 557–565

[364] N. Aoki, *Selmer groups and ideal class groups*, Comment. Math. Univ. St. Paul **42** (1993), 209–229

[365] J. Top, *Descent by* 3*-isogeny and* 3*-rank of quadratic fields*, Advances in number theory. The proceedings of the third conference of the Canadian Number Theory Association, held at Queen's University, Kingston, Canada, August 18-24, 1991 (F. Q. Gouvea, ed.), Oxford: Clarendon Press 303–317 (1993).

[366] R. Soleng, *Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields*, J. Number Theory **46** (1994), 214–229

[367] J. Brinkhuis, *Normal integral bases and the Spiegelungssatz of Scholz*, Acta Arith. **69** (1995), 1–9

[368] U. Schneiders, *Estimating the* 2*-rank of cubic fields by Selmer groups of elliptic curves*, Diss. Univ. Saarbrücken

[369] U. Schneiders, *Estimating the* 2*-rank of cubic number fields by the Selmer group of the corresponding elliptic curves*, Tagungsber. Oberwolfach **21** (1995)

[370] Y.-M. J. Chen, *The Selmer group and the ambiguous ideal class group of cubic fields*, Bull. Austral. Math. Soc. **54** (1996), 267–274

[371] E. F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), 79–114

[372] M. Ozaki, *On the p-rank of the ideal class group of the maximal real subfield of a cyclotomic field*, preprint 1997

[373] H. Sato, *The order of the p-Selmer groups and the rank of elliptic curves*, Tokyo J. Math. **20** (1997), 173–185

[374] U. Schneiders, *Estimating the 2-rank of cubic fields by Selmer groups of elliptic curves*, J. Number Theory **62** (1997), 375–396

[375] M. Stoll, *On the Mordell–Weil rank of certain CM curves*, preprint 1997

[376] Y. Sueyoshi, *On a comparison of the 4-ranks of the narrow ideal class groups of* $\mathbb{Q}(\sqrt{m})$ *and* $\mathbb{Q}(\sqrt{-m})$, Kyushu J. Math. **51** (1997), 261–272

[377] Y. Sueyoshi, *Relations betwen the narrow 4-class ranks of quadratic number fields*, Adv. Stud. Contemp. Math. **2** (2000), 47–58

V. Capitulation of Ideal Classes

[378] Ph. Furtwängler, *Über das Verhalten der Ideale des Grundkörpers im Klassenkörper*, Monatsh. Math. Phys. **27** (1916), 1–15

[379] W. Schäfer, *Beweis des Hauptidealsatzes der Klassenkörpertheorie für den Fall der komplexen Multiplikation*, Diss. Halle (1929)

[380] O. Taussky, *Über eine Verschärfung des Hauptidealsatzes*, Diss. Wien (1929)

[381] E. Artin, *Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz*, Abh. Math. Sem. Hamburg **7** (1930), 46–51

[382] Ph. Furtwängler, *Beweis des Hauptidealsatzes für Klassenkörper algebraischer Zahlkörper*, Abh. Math. Sem. Hamburg **7** (1930), 14–36

[383] S. Iyanaga, *Über den allgemeinen Hauptidealsatz*, Jap. J. Math. **7** (1930), 315–333

[384] H. Hasse, *Zum Hauptidealsatz der komplexen Multiplikation*, Monatsh. Math. Phys. **38** (1931), 315–322

[385] Ph. Furtwängler, *Über die Verschärfung des Hauptidealsatzes für algebraische Zahlkörper*, J. Reine Angew. Math. **167** (1932), 379–387

[386] K. Taketa, *Neuer Beweis eines Satzes von Herrn Furtwängler über die metabelschen Gruppen*, Japan J. Math. **9** (1932), 199–218

[387] O. Taussky, *Über die Verschärfung des Hauptidealsatzes für algebraische Zahlkörper*, J. Reine Angew. Math. **168** (1932), 193–210

[388] T. Tannaka, *Ein Hauptidealsatz relativ-galoischer Zahlkörper und ein Satz über den Normenrest*, Proc. Imp. Acad. Tokyo **9** (1933), 355–356 Japan J. Math **10** (1934), 183–189

[389] T. Tannaka, *Über einen Satz von Herrn Artin*, Proc. Imp. Acad. Tokyo (1934), 197–198

[390] S. Iyanaga, *Zum Beweis des Hauptidealsatzes*, Abh. Math. Sem. Hamburg **10** (1934), 349–357

[391] W. Magnus, *Über den Beweis des Hauptidealsatzes*, J. Reine Angew. Math. **170** (1934), 235–240

[392] A. Scholz, O. Taussky, *Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper; ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperturm*, J. Reine Angew. Math. **171** (1934), 19–41

[393] T. Tannaka, *Einige Bemerkungen zu den Arbeiten über den allgemeinen Hauptidealsatz*, Japan J. Math. **10** (1934), 163–167

[394] N. Tschebotaröw, *Algebraisch-arithmetische Bemerkungen* (Russ.), Wiss. Eintrag. Math., Ausg. **2** (1934), 94, No.7, 3–16

[395] E. Witt, *Bemerkungen zum Beweis des Hauptidealsatzes von S. Iyanaga*, Abh. Math. Sem. Hamburg **11** (1936), 221

[396] H. G. Schumann, W. Franz, *Zum Beweis des Hauptidealsatzes*, Abh. Math. Sem. Hamburg **12** (1937), 42–47

[397] S. Iyanaga, *Über die allgemeinen Hauptidealformeln*, Monatsh. Math. Phys. **48** (1939), 400–407

[398] N. Hofreiter, *Nachruf auf Ph. Furtwängler*, Monatsh. Math. Phys. **49** (1941), 219–227

[399] T. Tannaka, *Some remarks concerning the principal ideal theorem*, Tôhoku Math. J. **1** (1949), 270–278

[400] T. Tannaka, *An alternative proof of a generalized principal ideal theorem*, Proc. Japan Acad. **25** (1949), 26–31

[401] T. Tannaka, F. Terada, *A generalization of the principal ideal theorem*, Proc. Japan Acad. **25** (1949), 7–8

[402] F. Terada, *On a generalization of the principal ideal theorem*, Tôhoku Math. J. **1** (1949), 229–269

[403] O. Taussky, *Arnold Scholz zum Gedächtnis*, Math. Nachr. **7** (1952), 374–386

[404] F. Terada, *Complex Multiplication and principal ideal theorem*, Tôhoku Math. J. **6** (1954), 21–25

[405] F. Terada, *On a generalized principal ideal theorem*, Tôhoku Math. J. **6** (1954), 95–100

[406] E. Witt, *Verlagerung von Gruppen und Hauptidealsatz*, Proc. Int. Congr. Math. Ser. II Amsterdam **2** (1954), 70–73

[407] F. Terada, *A generalization of the principal ideal theorem*, J. Math. Soc. Japan **7** (1955), 530–536

[408] K. Iwasawa, *A note on the group of units of an algebraic number field*, J. Math. Pures Appl. **35** (1956), 189–192

[409] Z. J. Borevic, *On the demonstration of the principal ideal theorem*, Vestnik Leningrad Univ. **12** (1957), 5–8 (Russ.)

[410] H. Reichardt, *Ein Beweis des Hauptidealsatzes für imaginär-quadratische Zahlkörper*, Mathem. Nachr. **17** (1958), 318–329

[411] T. Tannaka, *A generalized principal ideal theorem and a proof of a conjecture of Deuring*, Ann. Math.**67** (1958), 574–589

[412] H. Reichardt, *Hauptidealsatzes für imaginär-quadratische Zahlkörper*, Atti Sesto Congr. Unione Mat. Ital Tenuto Napoli (1959), 11–16

[413] H. Kempfert, *Zum allgemeinen Hauptidealsatz I*, J. Reine Angew. Math. **210** (1962), 38–64

[414] O. Taussky, *Some computational problems in algebraic number theory*, Survey of numerical analysis 549–557

[415] T. Hsü, *Über den Hauptidealsatz für imaginäre quadratische Zahlkörper*, J. Reine Angew. Math. **212** (1963), 49–62

[416] S. Takahashi, *An explicit representation of the generalized principal ideal theorem for the rational ground field*, Tôhoku Math. J. **16** (1964), 176–182

[417] S. Takahashi, *On Tannaka-Terada's principal ideal theorem for the rational ground field*, Tohoku Math. J. **17** (1965), 87–104

[418] T. Tannaka, *On the generalized principal ideal theorem*, Proc. Japan Acad. **25** (1965), 65–77

[419] H. Kempfert, *Zum allgemeinen Hauptidealsatz II*, J. Reine Angew. Math. **223** (1966), 28–55

[420] M. Rosen, *Two theorems on Galois cohomology*, Proc. Amer. Math. Soc. **17** (1966), 1183–1185

[421] Y. Kawada, *A remark on the principal ideal theorem*, J. Math.Soc. Jap. **20** (1968), 166–169

[422] O. Taussky, *A remark concerning Hilbert's theorem 94*, J. Reine Angew. Math. **239/240** (1969), 435–438

[423] H. Kisilevsky, *Some results related to Hilbert's Theorem 94*, J. Number Theory **2** (1970), 199–206

[424] O. Taussky, *Hilbert's theorem 94*, Computers in Number Theory, Academic Press (1971), 65–71

[425] F. Terada, *A principal ideal theorem in the genus field*, Tôhoku Math. J. **23** (1971), 697–718

[426] N. Adachi, *Report on principal ideal theorems*, Mem. School Sci. & Eng., Waseda Univ. **37** (1973), 81–90

[427] R. Schipper, *A generalization of Hilbert's Theorem 94 and related results*, Ph. D. thesis Univ. Maryland 1974

[428] E. W. Zink, *Zum Hauptidealsatz von Tannaka-Terada*, Math. Nachr. **67** (1975), 317–325

[429] H. Kisilevsky, *Number fields with class number congruent to* 4 *modulo* 8 *and Hilbert's Theorem 94*, J. Number Theory **8** (1976), 271–279

[430] S. M. Chang, *Capitulation problems in algebraic number fields*, Thesis Toronto (1977)

[431] H. Furuya, *Principal ideal theorems in the genus field for absolutely abelian extensions*, J. Number Theory **9** (1977), 4–15

[432] R. Schipper, *On the behavior of ideal classes in cyclic unramified extensions of prime degree*, Number Theory and Algebra (H. Zassenhaus, ed.), New York, Academic Press 1977 303–309

[433] S. M. Chang, R. Foote, *Capitulation in class field extensions of type* (p, p), Canad. J. Math. **32** (1980), 1229–1243

[434] Y. Kida, *ℓ-extensions of CM-fields and cyclotomic invariants*, J. Number Theory **12** (1980), 519–528

[435] K. Miyake, *On the general principal ideal theorem*, Proc. Japan Acad. **56** (1980), 171–174

[436] R. J. Bond, *Some results on the capitulation problem*, J. Number Theory **13** (1981), 246–254

[437] G. Frei (ed.), *Die Briefe von E. Artin an H. Hasse, 1923 – 1953*, Univ. Laval, Québec, and ETH Zürich, Preprint 1981

[438] F.-P. Heider, *Zur Kapitulation der Idealklassen von algebraischen Zahlkörpern*, Tagungsber. Oberwolfach **35/81** (1981)

[439] B. Schmithals, *Kapitulation der Idealklassen in zyklischen Erweiterungen und Einheiten in Diederkörpern vom Grad* 2ℓ, Tagungsber. Oberwolfach **35/81** (1981)

[440] B. Schmithals, *Zur Kapitulation der Idealklassen in zyklischen Zahlkörpererweiterungen und Einheitenstruktur in Diederkörpern vom Grad* 2ℓ, Diss. Univ. Dortmund (1981)

[441] F.-P. Heider, B. Schmithals, *Zur Kapitulation der Idealklassen in unverzweigten primzyklischen Erweiterungen*, J. Reine Angew. Math. **336** (1982), 1–25

[442] B. Nebelung, *Zum Kapitulationsproblem in unverzweigten Erweiterungen*, Staatsarbeit Köln 1983

[443] F.-P. Heider, *Kapitulationsprobleme und Knotentheorie*, Manuscripta Math. **46** (1984), 229–272

[444] K. Iimura, *A note on ramified principal ideals in a non-Galois cubic field*, Abh. Math. Sem. Hamburg **54** (1984), 21–23

[445] K. Miyake, *A generalization of Hilbert's Theorem 94*, Nagoya Math. J. **96** (1984), 83–94

[446] K. Miyake, *On capitulation of ideals of an algebraic number field*, Proc. Japan Acad. **60** (1984), 232–235

[447] K. Miyake, *On the capitulation problem (Look, the class field theory is arising!)* (Japan.), Sugaku **37** (1985), 128–143

[448] R. J. Bond, *Unramified abelian extensions of number fields*, J. Number Theory **30** (1980), 1–10

[449] A. Derhem, *Capitulation dans les extensions quadratiques non ramifiées de corps de nombres cubiques cycliques*, thèse, Université Laval, Québec (1988)

[450] J. F. Jaulent, *L'état actuel du problème de la capitulation*, Sém. Théor. Nombres Bordeaux, (1987/88), **17**

[451] K. Iwasawa, *A note on the capitulation problem for number fields I*, Proc. Japan Acad. **65** (1989), 59–61

[452] K. Miyake, *Algebraic investigations of Hilbert's Theorem 94, the principal ideal theorem, and the capitulation problem*, Expos. Math. **7** (1989), 289–346

[453] B. Nebelung, *Klassifikation metabelscher* 3*-Gruppen mit Faktorkommutatorgruppe vom Typ* $(3,3)$ *und Anwendung auf das Kapitulationsproblem*, Diss. Univ. Köln, (1989)

[454] E. Cremone, W. K. Odoni, *A generalization of a result of Iwasawa on the capitulation problem*, Math. Proc. Cambridge **107** (1990), 1–3

[455] G. Fujisaki, *A note on a paper of Iwasawa*, Proc. Japan Acad. **66** (1990), 61–64

[456] K. Iwasawa, *A note on the capitulation problem for number fields II*, Proc. Japan Acad. **66** (1990), 183–186

[457] D. Mayer, *Principalization in complex* S_3*-fields*, Numerical Mathematics and Computing, Proc. 20th Manitoba Conf. Winnipeg 1990, Congr. Numer. **80** (1991), 73–87

[458] K. Miyake, *H. Suzuki's generalization of Hilbert's theorem 94*, Théorie des nombres, Publ. Math. Fac. Sci. Besançon 1989/90 – 1990/91

[459] H. Suzuki, *A generalization of Hilbert's theorem 94*, Nagoya Math. J. **121** (1991), 161–169

[460] R. Couture, A. Derhem, *Un problème de capitulation*, C. R. Acad. Sci. Paris **314** (1992), 785–788

[461] M.C. Ismaili, *Sur la capitulation des* 3*-classes d'idéaux de la clôture normale s'un corps cubique pur*, Ph.D. thesis Univ. Laval, 1992

[462] F. Gerth III, *Some results on the capitulation problem for quadratic fields*, Expos. Math. **11** (1993), 185–192

[463] E. Benjamin, F. Sanborn, C. Snyder, *Capitulation in unramified quadratic extensions of real quadratic number fields*, Glasg. Math. J. **36** (1994), 385–392

[464] D. Folk, *Extra capitulation and central extensions*, J. Number Theory **50** (1995), no. 2, 226–232

[465] D. Folk, *When are global units norms of units?*, Acta Arith. **76** (1996), 145–147

[466] T. Fukuda, K. Komatsu, *A capitulation problem and Greenberg's conjecture on real quadratic fields*, Math. Comp. **65** (1996), 313–318

[467] D. Hubbard, *The non-existence of certain free pro-p extensions and capitulation in a family of dihedral extensions of* $\mathbb{Q}$, thesis Univ. Washington 1996

[468] C. Maire, $T-S$ *capitulation*, Théorie des nombres, 1994/95–1995/96, 33 pp., Publ. Math. Fac. Sci. Besançon 1997

[469] C. Maire, *Une remarque sur la capitulation du groupe des classes au sens restreint*, Théor. Nombres 1996/97 – 1997/98, Publ. Math. Besançon (1999), 10pp

[470] A. Azizi, *Sur la capitulation des* 2*-classes d'idéaux de* $k = \mathbb{Q}(\sqrt{2pq}, i)$ *où* $p \equiv -q \equiv 1 \bmod 4$, Acta Arith. **94** (2000), no. 4, 383–399

[471] K.W. Gruenberg, A. Weiss, *Capitulation and transfer kernels*, J. Théor. Nombres Bordeaux **12** (2000), 219–226

[472] C. Khare, D. Prasad, *On the Steinitz module and capitulation of ideals*, Nagoya Math. J. **160** (2000), 1–15

[473] C. Thiebaud, *Sur la capitulation dans les corps de genres d'une extension abélienne d'un corps quadratique imaginaire*, J. Number Theory **85** (2000), 92–107

[474] M. Ayadi, A. Azizi, M.C. Ismaili, *The capitulation problem for certain number fields*, Class field theory—its centenary and prospect (Tokyo, 1998), 467–482, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001

[475] H. Suzuki, *On the capitulation problem*, Class field theory—its centenary and prospect (Tokyo, 1998), 483–507, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001

[476] A. Azizi, *Sur une question de capitulation*, Proc. Amer. Math. Soc. **130** (2002), no. 8, 2197–2202

[477] A. Azizi, A. Mouhib, *Capitulation des* 2*-classes d'idéaux de* $\mathbb{Q}(\sqrt{2}, \sqrt{d}\,)$ *où* d *est un entier naturel sans facteurs carrés*, Acta Arith. **109** (2003), 27–63

[478] M. Morishita, *On capitulation problem for 3-manifolds*, Galois theory and modular forms, 305–313, Dev. Math., 11, Kluwer 2004

VI. Kummer Theory and Galois Groups

[479] R. Dedekind, *Konstruktion von Quaternionenkörpern*, Ges. Werke II, Nachlass, Braunschweig (1931), 376–384

[480] N. Tschebotarev, *Zur Gruppentheorie des Klassenkörpers*, J. Reine Angew. Math. **161** (1929), 179–193

[481] E. Rosenblüth, *Die arithmetische Theorie und die Konstruktion der Quaternionenkörper auf klassenkörpertheoretischer Grundlage*, Monatsh. Math. Phys. **41** (1934), 85–125

[482] A. Scholz, *Die Kreisklassenkörper von Primzahlpotenzgrad und die Konstruktion von Körpern mit vorgegebener zweistufiger Gruppe I*, Math. Ann. **109** (1934), 161–190 Corr.: ibid **109** p. 764

[483] W. Magnus, *Beziehung zwischen Gruppen und Idealen in einem speziellen Ring*, Math. Ann. **111** (1935)

[484] A. Scholz, *Die Kreisklassenkörper von Primzahlpotenzgrad und die Konstruktion von Körpern mit vorgegebener zweistufiger Gruppe II*, Math. Ann. **110** (1935), 643–649

[485] L. Holzer, *Lösung der Aufgabe 194 von A. Scholz*, Jahresber. DMV **46** (1936), 83–84 (kursiv)

[486] H. Reichardt, *Über Normalkörper mit Quaternionengruppe*, Math. Z. **41** (1936), 218–222

[487] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. Reine Angew. Math. **174** (1936), 237–245.

[488] W. Magnus, *Neuere Ergebnisse über auflösbare Gruppen*, Jahresber. DMV **47** (1937), 69–78

[489] H. Hasse, *Invariante Kennzeichnung relativ abelscher Zahlkörper mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers*, Abh. d. D. Akad. Wiss. Berlin **8** (1947/48), 5–56 Ges. Abhandl. III, 155–206

[490] H. Hasse, *Invariante Kennzeichnung galoischer Körper mit vorgegebener Galoisgruppe*, J. Reine Angew. Math. **187** (1949), 14–43 Ges. Abhandl. III, 253–282

[491] G. Fujisaki, *On an example of an unramified Galois extension*, (Japan.) Sugaku **9** (1957/58), 97–99

[492] C. R. Hobby, *The derived series of a finite p-group*, Ill. J. Math. **5** (1961), 228–233

[493] Ch. Jensen, *Remark on a characterization of certain ring class fields by their absolute Galois groups*, Proc. Amer. Math. Soc. **14** (1963), 738–741

[494] A. Fröhlich, *On non-ramified extensions with prescribed Galois group*, Mathematika **9** (1966), 133–134

[495] G. Bruckner, *Charakterisierung der galoisschen Zahlkörper, deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind*, Math. Nachr. **32** (1966), 317–326

[496] J.-J. Payan, *Critère de décomposition d'une extension de Kummer sur un sous-corps du corps de base*, Ann. scient. Éc. Norm. Sup. (4) **1** (1968), 445–458

[497] J. Martinet, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre* $2p$, Ann. Inst. Fourier **19** (1969), 1–80

[498] J. Martinet, *Sur les extensiones à groupe de Galois quaternionien*, C. R. Acad. Sci. Paris **303** (1970), 933–935

[499] J.-P. Serre, *Sur une question d'Olga Taussky*, J. Number Theory **2** (1970), 235–236 Œuvres II, 540–541

[500] L. Bouvier, J.-J. Payan, *Construction de certaines extensions de degré p*, Seminaire de théorie des nombres de Grenoble (1972)

[501] J. Martinet, *Sur les extensions à groupe de Galois quaternionien*, C. R. Acad. Sci. Paris **274** (1972), 933–935.

[502] P. Damey, J. Martinet, *Plongement d'une extension quadratique dans une extension quaternionienne*, J. Reine Angew. Math. **262/263** (1973), 323–338

[503] M. R. Jones, *Some inequalities for the multiplier of a finite group*, Proc. Amer. Math. Soc. **49** (1973), 450–456

[504] B. Wyman, *Hilbert class fields and group extensions*, Scripta math. **29** (1973), 141–149

[505] D. Chatelain, *Décomposition des idéaux dans une extension de Kummer cyclique*, Publ. Math. Fac. Sci. Besançon 1975/76, 31pp.

[506] R. Gold, *Hilbert class fields and split extensions*, Ill. J. Math. **21** (1977), 66–69

[507] D. J. Madden, W. Y. Vélez, *A note on the normality of unramified abelian extensions of quadratic extensions*, Manuscr. Math. **30** (1980), 343–349

[508] Ch. Jensen, N. Yui, *Polynomials with D_p as Galois group*, J. Number Theory **15** (1982), 347–375

[509] P. Kolvenbach, *Zur algebraischen Theorie der $SL(2,3)$-Erweiterungen*, Diss. Köln (1982)

[510] F.-P. Heider, P. Kolvenbach, *The construction of $SL(2,3)$-polynomials*, J. Number Theory **19** (1984), 392–411

[511] S.-H. Kwon, *Extensions à groupe de Galois A_4*, Thèse de 3^e cycle, Univ. Bordeaux (1984)

[512] S.-H. Kwon, *Corps de nombres de degré 4 de type alterné*, C. R. Acad. Sci. Paris **299** (1984), 41–43

[513] J. Elstrodt, F. Grunewald, J. Mennicke, *On unramified A_m-extensions of quadratic number fields*, Glasgow Math. J. **27** (1985), 31–37

[514] A. A. Bruen, Ch. U. Jensen, N. Yui, *Polynomials with Frobenius groups of prime degree as Galois groups II*, J. Number Theory **24** (1986), 305–359

[515] Ch. Jensen, *On the representation of a group as a Galois group over an arbitrary field*, Sem. Théor. Nombres, Univ. Laval (1987), 556–560

[516] Ch. Jensen, N. Yui, *Quaternion extensions*, Algebraic Geometry and Commutative Algebra (1987), 155–182

[517] S.-H. Kwon, J. Martinet, *Sur les corps résolubles de degré premier*, J. Reine Angew. Math. **375/376** (1987), 12–23

[518] H. Osada, *The Galois group of the polynomial $X^n + aX^l + b$*, J. Number Theory **25** (1987), 230–238

[519] P. Barrucand, *Unsolved Problem ASI 88:04*, Conf. Number Theory Banff (1988),

[520] G. Cornell, M. I. Rosen, *A note on the splitting of the Hilbert class field*, J. Number Theory **28** (1988), 152–158

[521] J. Nakagawa, *On the Galois group of a number field with square free discriminant*, Comm. Math. Univ. St. Pauli **37** (1989), 95–98

[522] G. Fujisaki, *An elementary construction of galois quaternionic extensions*, Proc. Japan Acad. **66** (1990), 80–83

[523] G. Kientega, P. Barrucand, *On quartic fields with the symmetric group*, Number Theory, Banff Center, Alberta (R. Mollin, ed.) (1990), 287–297

[524] I. Kiming, *Explicit classification of some 2-extensions of a field of characteristic different from 2*, Can. J. Math. **42** (1990), 825–855

[525] J. Minác, T. L. Smith, *A characterization of C-fields via Galois groups*, J. Algebra **137** (1991), 1–11

[526] A. Movahhedi, *Sur une classe d'extensions non ramifiées*, Acta Arith. **59** (1991), 91–95

[527] C. Bachoc, S.-H. Kwon, *Sur les extensions de groupe de Galois $\widetilde{A}_4$*, Acta Arith. **62** (1992), 1–10

[528] R. Bond, *On the splitting of the Hilbert class field*, J. Number Theory **42** (1992), 349–360

[529] L. Schneps, *Explicit realizations of subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$ as Galois groups*, J. Number Theory **39** (1992), 5–13

[530] T. P. Vaughan, *Constructing quaternionic fields*, Glasgow Math. J. **34** (1992), 43–54.

[531] A. Jehanne, *Sur les extensions de $\mathbb{Q}$ à groupe de Galois S_4 et $\widetilde{S}_4$*, Acta Arith. **69.3** (1995), 259–276

[532] A. Jehanne, , Thèse, Univ. Bordeaux

[533] J. Wojcik, *Criterion for a field to be abelian*, Colloq. Math. **68** (1995), 187–191

[534] Ph. Cassou-Noguès, A. Jehanne, *Parité du nombre de classes des S_4-extensions de $\mathbb{Q}$ et courbes elliptiques*, J. Number Theory **57** (1996), 366–384

VII. Governing Fields

[535] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$, Math. Z. **39** (1934), 95–111

[536] H. Cohn, J. Lagarias, *Is there a density for the set of primes p such that the class number of* $\mathbb{Q}(\sqrt{-p})$ *is divisible by* 16*?*, Colloqu. Math. Soc. Bolyai **34** (1981), 257–280

[537] P. Morton, *Density results for the* 2*-class groups of imaginary quadratic fields*, J. Reine Angew. Math. **332** (1982), 156–187

[538] P. Morton, *Density results for the* 2*-classgroups and fundamental units of real quadratic fields*, Studia Sci. Math. Hungary **17** (1982), 21–43

[539] H. Cohn, J. Lagarias, *On the existence of fields governing the* 2*-invariants of the class group of* $\mathbb{Q}(\sqrt{dp})$ *as p varies*, Math. Comp. **41** (1983), 711–730

[540] P. Morton, *The quadratic number fields with cyclic* 2*-classgroups*, Pac. J. Math. **108** (1983), 165–175

[541] P. Stevenhagen, *Class groups and governing fields*, Ph. D. thesis, Berkeley (1988),

[542] P. Stevenhagen, *Ray class groups and governing fields*, Théorie des nombres, Années 1988/89, Publ. Math. Fac. Sci. Besançon (1989)

[543] P. Morton, *Governing fields for the* 2*-classgroups of* $\mathbb{Q}(\sqrt{-q_1q_2p})$ *and a related reciprocity law*, Acta Arith. **55** (1990), 267–290

[544] P. Stevenhagen, *Divisibility by* 2*-powers of certain quadratic class numbers*, J. Number Theory **43** (1993), 1–19

VIII. Odlyzko Bounds

[545] A. Scholz, *Minimaldiskriminanten algebraischer Zahlkörper*, J. Reine Angew. Math. **179** (1938), 16–21

[546] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152

[547] H. M. Stark, *The analytic theory of algebraic numbers*, Bull. Amer. Math. Soc. **81** (1975), 961–972

[548] A. M. Odlyzko, *Some analytic estimates of class numbers and discriminants*, Invent. Math. **29** (1975), 275–286

[549] J. P. Serre, *Minorations de discriminants*, Collected Papers **3** (1986), 240–243

[550] A. M. Odlyzko, *Lower bounds for discriminants of number fields*, Acta Arith. **29** (1976), 275–297

[551] A. M. Odlyzko, *Lower bounds for discriminants of number fields II*, Tôhoku Math. J. 29 (1977), 209–216

[552] A. M. Odlyzko, *On conductors and discriminants*, Algebr. Number Fields, Proc. 1975 Durham Symp. (A. Fröhlich, ed.) (1977), 377–407

[553] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: A survey of recent results*, Semin. Théor. Nombres Bordeaux **1** (1977), 119–141

[554] G. Poitou, *Minorations de discriminants*, Sém. Bourbaki (1975/76) **479** (1977), 136–153

[555] G. Poitou, *Sur les petits discriminants*, Sém. Delange - Pisot - Poitou (1976/77) **6** (1977), 18pp

[556] J. Martinet, *Petits discriminants*, Ann. Inst. Fourier **29** (1979), 159–170

[557] F. Diaz y Diaz, *Tables minorant la racine n-ième du discriminant d'un corps de degré n*, Publ. Math. d'Orsay (1980), 59pp

[558] J. Martinet, *Petits discriminants des corps de nombres*, Journées Arithmétiques 1980 (J. V. Armitage, ed.), Cambridge Univ. Press 1982, 151–193

[559] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sém. Théor. Nombres Bordeaux **2** (1990), 119–141

[560] C. Maire, *On infinite unramified extensions*, Pac. J. Math. **192** (2000), 135–142

[561] F. Hajir, C. Maire, *Tamely ramified towers and discriminant bounds for number fields*, Compositio Math. **128** (2001), 35–53

[562] F. Hajir, C. Maire, *Tamely ramified towers and discriminant bounds for number fields. II*, J. Symbolic Comput.

IX. Knots, p-Groups and Schur Multipliers

[563] I. Schur, *Untersuchungen über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **132** (1907), 85–137

[564] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen I*, J. Reine Angew. Math. **175** (1936), 100-107

[565] A. Scholz, *Abelsche Durchkreuzung*, Monatsh. Math. Phys. **48** (1939), 340–352

[566] A. Scholz, *Zur Abelschen Durchkreuzung*, J. Reine Angew. Math. **182** (1940), 216

[567] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen II*, J. Reine Angew. Math. **182** (1940), 217–234

[568] K. Masuda, *An application of the generalized norm residue symbol*, Proc. Amer. Math. Soc. **10** (1959), 245–252

[569] M. Hall, J. K. Senior, *The groups of order* 2^n $(n \leq 6)$, Macmillan, New York 1964

[570] L. V. Kuzmin, *Homologies of profinite groups, the Schur multiplicator, and class field theory* (Russ.), Izv. Akad. Nauk. **33** (1969), 1220–1254

[571] T. W. Sag, J. Wamsley, *Minimal presentations for groups of order* 2^n*,* $n \leq 6$, J. Austral. Math. Soc. **15** (1973), 461–469

[572] M. R. Jones, J. Wiegold, *Isoclinisms and covering groups*, Bull. Austral. Math. Soc. **11** (1974), 71–76

[573] F. P. Heider, *Strahlknoten und Geschlechterkörper mod* $\mathfrak{m}$, J. Reine Angew. Math. **320** (1980), 52–67

[574] F. Lorenz, *Über eine Verallgemeinerung des Hasseschen Normensatzes*, Math. Z. **173** (1980), 203–210

[575] H. Opolka, *Zur Auflösung zahlentheoretischer Knoten*, Math. Z. **173** (1980), 95–103

[576] A. D. Thomas, G. V. Wood, *Group Tables*, Shiva Publishing Ltd, Kent, UK 1980

[577] F. P. Heider, *Zahlentheoretische Knoten unendlicher Erweiterungen*, Arch. Math. **37** (1981), 341–352

[578] F.R. Beyl, J. Tappe, *Group extensions, representations, and the Schur multiplicator*, Lecture Notes Math. *958*, Springer Verlag 1982

[579] F.-P. Heider, *Strahlknoten und Geschlechterkörper mod* $\mathfrak{m}$, J. Reine Angew. Math. **320** (1980), 52–67

[580] F. Lorenz, *Zur Theorie der Normenreste*, J. Reine Angew. Math. **334** (1982), 157–170

[581] K. Miyake, *Central extensions and Schur's multiplicators of Galois groups*, Prepr. Ser. Nagoya Univ. **3** (1982), 11 p.

[582] H. Opolka, *Der Liftungsindex primitiver Galoisdarstellungen*, J. Algebra **74** (1982), 535–542.

[583] J. Wiegold, *The Schur multiplier: an elementary approach*, in Groups: St. Andrews 1981, LMS Lecture Note Series (C. M. Campbell, E. F. Robertson eds.) **71** Cambridge Univ. Press (1982), 137–154

[584] K. Miyake, *Central extensions and Schur's multiplicators of Galois groups*, Nagoya Math. J. **90** (1983), 137–144

[585] S. Hamada, *Norm theorem on splitting fields of some binomial polynomials*, Kodai Math. J. **6** (1983), 47–50

[586] W. Jehne, *Der Hassesche Normensatz und seine Entwicklung*, Mitt. Math. Ges. Hamburg **11** (1982), 143–153

[587] E. T. Tan, *A remark on Scholz's Abelian crossings*, Arch. Math. **42** (1984), 325–328

[588] H. Opolka, *Normenreste in relativ abelschen Zahlkörpererweiterungen und symplektische Paarungen*, Abh. Math. Sem. Univ. Hamburg **54** (1984), 1–4

[589] G. Steinke, *Über Auflösungen zahlentheoretischer Knoten*, Schriftenreihe Math. Inst. Univ. Münster **25** (1983), 116 pp.

[590] G. Karpilovsky, *The Schur Multiplier*, London Math. Soc. Monographs Oxford (1987)

[591] E. T. Tan, *A note on abundant central extensions of number fields and Scholz's solutions of number knots*, Arch. Math. **54** (1990), 157–161

[592] H. Opolka, *The norm exponent in Galois extensions of number fields*, Proc. Amer. Math. Soc. **99** (1987), 41–43

[593] F. Lorenz, *Schurmultiplikatoren und Zahlknoten*, Sitz.ber. Math.-Nat.wiss. Kl. Akad. Gem.-nütz. Wiss. Erfurt **1** (1991), 13–27

[594] H. Opolka, *Norm exponents and representation groups*, Proc. Amer. Math. Soc. **111** (1991), 595–597

See also [273], [408], [443].

X. Stark Conjectures

[595] H. M. Stark, *Values of L-functions at* $s = 1$. *I. L-functions for quadratic forms*, Adv. Math. **7** (1971), 301–343

[596] H. M. Stark, *Values of L-functions at* $s = 1$. *II. Artin L-functions with rational characters*, Adv. Math. **17** (1975), 60–92

[597] H. M. Stark, *Values of L-functions at* $s = 1$. *III. Totally real fields and Hilbert's twelfth problem*, Adv. Math. **22** (1976), 64–84

[598] H. M. Stark, *Class fields for real quadratic fields and L-series at* 1, Algebraic Number Fields (A. Fröhlich, ed.), Acad. Press, London, 1977, pp. 355–375

[599] H. M. Stark, *Hilbert's twelfth problem and L-series*, Bull. Amer. Math. Soc. **83** (1977), 1972–1074

[600] H. M. Stark, *Values of L-functions at* $s = 1$*. IV. First derivatives at* $s = 0$, Adv. Math. **35** (1980), 197–235

[601] J. Tate, *On Stark's conjectures on the behavior of* $L(s, \chi)$ *at* $s = 0$, J. Fac. Sci. Univ. Tokyo, Sect. I A **28** (1981), 963–978

[602] T. Chinburg, *Stark's conjecture for L-functions with first-order zeroes at* $s = 0$, Adv. Math. **48** (1983), 82–113

[603] J. Sands, *Abelian Fields and the Brumer-Stark conjecture*, Comp. Math. **53** (1984), 337–346

[604] J. Sands, *Galois groups of exponent* 2 *and the Brumer-Stark conjecture*, J. Reine Angew. Math. **349** (1984), 129–135

[605] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en* $s = 0$, Progress in Math. (J. Coates, S. Helgason, eds), Birkhäuser, 1984

[606] J. Sands, *Two cases of Stark's conjecture*, Math. Ann. **272** (1985), 349–359

[607] D. Hayes, *Brumer elements over a real quadratic base field*, Expo. Math. **8** (1990), 137–184

[608] A. Wiles, *On a conjecture of Brumer*, Ann. Math. **131** (1990), 555–565

[609] F. Y. Wang, *Conductors of fields arising from Stark's conjectures*, Ph. D. Thesis MIT, 1991

[610] K. Rubin, *Stark units and Kolyvagin's Euler systems*, J. Reine Angew. Math. **425** (1992), 141–154

[611] X.F. Roblot, *Unités de Stark et corps de classes de Hilbert*, C. R. Acad. Sci. Paris **323** (1996), 1165–1168

[612] K. Rubin, *A Stark conjecture over* $\mathbb{Z}$ *for abelian L-functions with multiple zeros*, Annal. Inst. Fourier, 46 (1996), 33–62

[613] D.S. Dummit, J.W. Sands, B.A. Tangedal, *Computing Stark units for totally real cubic fields*, Math. Comp. **66** (1997), 1239–1267

[614] D. Hayes, *Base change for the conjecture of Brumer-Stark*, J. Reine Angew. Math. **497** (1998), 83–89

[615] S. Dasgupta, *Stark's conjectures*, Honors thesis, Harvard University, 1999.

[616] H. Cohen, X.-F. Roblot, *Computing the Hilbert class field of real quadratic fields*, Math. Comp. **69** (2000), no. 231, 1229–1244

[617] X.-F. Roblot, *Stark's conjectures and Hilbert's twelfth problem*, Experiment. Math. **9** (2000), no. 2, 251–260

[618] D.S. Dummit, B.A. Tangedal, P.B. van Wamelen, *Stark's conjecture over complex cubic number fields*, Math. Comp. **73** (2004), no. 247, 1525–1546

See also [121].

XI. The Rest

[619] L. Dirichlet, *Einige neue Sätze über unbestimmte Gleichungen*, Gesammelte Werke, 219–236

[620] D. Hilbert, *Zahlentheorie* (E. Maus, ed.), Lecture Notes 1897/1898, Göttingen 1990

[621] D. Hilbert, *Über die Theorie des relativquadratischen Zahlkörpers*, Math. Ann. **51** (1899), 1–127

[622] Ph. Furtwängler, *Existenzbeweis für den Klassenkörper*, Math. Ann. **63** (1907),

[623] A. Speiser, *Die Theorie der binären quadratischen Formen mit Koeffizienten und Unbestimmten in einem beliebigen Zahlkörper*, Diss. Göttingen, 1909

[624] E. Hecke, *Zur Theorie der Modulfunktionen von zwei Variablen und ihre Anwendung auf die Zahlentheorie*, Math. Ann. **71** (1912) 1–37

[625] R. Brauer, E. Noether, *Über minimale Zerfällungskörper irreduzibler Darstellungen*, Collected papers of Richard Brauer I, 12–19

[626] S. Kuroda, *Über den Dirichlet'schen Körper*, J. Fac. Sci. Imp. Univ. Tokyo **IV** (1943), 383–406

[627] H. Hasse, Zahlbericht, Würzburg-Wien 1970

[628] H. Cohn, *A numerical study in composite real quartic and octic fields*, Computers in number theory (Atkin, Birch eds.), Academic Press 1971

[629] B. Oriat, *Quelques caractères utiles*

[630] I. M. Isaacs, *Character theory of finite groups*, Academic Press Inc. 1976; 2nd ed. Dover 1995

[631] E. Brown, Ch. Parry, *The* 2*-class group of certain biquadratic number fields*, J. Reine Angew. Math. **295** (1977), 61–71

[632] E. Brown, Ch. Parry, *The* 2*-class group of certain biquadratic number fields II*, Pac. J. Math. **78** (1978), 11–26

[633] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer Verlag 1978.

[634] J. Lagarias, *Signatures of units and congruences (mod* 4*) in certain fields*, J. Reine Angew. Math. **301** (1978), 142–146

[635] E. Lehmer, *Rational reciprocity laws*, Amer. Math. Monthly **85** (1978), 467–472

[636] J. Lagarias, *Signatures of units and congruences (mod* 4*) in totally real fields*, J. Reine Angew. Math. **320** (1980), 1–5

[637] J. Lagarias, *Signatures of units and congruences (mod* 4*) in totally real fields II*, J. Reine Angew. Math. **320** (1980), 115–126

[638] K. S. Williams, *On the evaluation of* $(\varepsilon_{q_1q_2}/p)$, Rocky Mt. J. Math. **11** (1980), 19–26

[639] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Ergebnisse der Mathematik, Springer Verlag Heidelberg, 1983

[640] S. Louboutin, *Calcul des nombres de classes relatifs: application aux corps octiques quaternionique à multiplication complexe*, C. R. Acad. Sci. Paris **317** (1993), 643–646

[641] A. Hahn, *Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups*, Springer Verlag 1994

[642] S. Louboutin, R. Okazaki, *Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one*, Acta Arith. **67** (1994), 47–62.

[643] K. S. Kedlaya, *Complex Multiplication and explicit class field theory*, Thesis, Harvard Univ. 1996

[644] S. Louboutin, *Determination of all quaternion octic CM-fields with class number* 2, J. London Math. Soc. 54 (1996), 227–238