# CLASS GROUPS OF DIHEDRAL EXTENSIONS

FRANZ LEMMERMEYER

Abstract. Let $L/F$ be a dihedral extension of degree $2p$, where $p$ is an odd prime. Let $K/F$ and $k/F$ be subextensions of $L/F$ with degrees $p$ and 2, respectively. Then we will study relations between the $p$-ranks of the class groups $\mathrm{Cl}(K)$ and $\mathrm{Cl}(k)$.

## 1. A Short History of Reflection Theorems

Results comparing the $p$-rank of class groups of different number fields (often based on the interplay between Kummer theory and class field theory) are traditionally called 'reflection theorems'; the oldest such result is due to Kummer himself: let $h^+$ and $h^-$ denote the plus and the minus $p$-class number of $K = \mathbb{Q}(\zeta_p)$, respectively; then Kummer observed that $p \mid h^+$ implies $p \mid h^-$, and this was an important step in verifying Fermat's Last Theorem (that is, checking the regularity of $p$) for exponents $< 100$. Kummer's result was improved by Hecke [13] (see also Takagi [32]):

**Proposition 1.1.** *Let $p$ be an odd prime, $K = \mathbb{Q}(\zeta_p)$, and let $\mathrm{Cl}_p(K)$ denote the $p$-class group of $K$. Let $\mathrm{Cl}_p^+(k)$ (or $\mathrm{Cl}_p^-(K)$, resp.) be the subgroup of $\mathrm{Cl}_p(K)$ on which complex conjugation acts trivially (or as $-1$, resp.). Then $\mathrm{rk}\ \mathrm{Cl}_p^+(k) \le \mathrm{rk}\ \mathrm{Cl}_p^-(k)$.*

Analogous inequalities hold for the eigenspaces of the class group $\mathrm{Cl}(K)$ under the action of the Galois group; see e.g. [15].

Scholz [30] and Reichardt [28] discovered a similar connection between the 3-ranks of class groups of certain quadratic number fields:

**Proposition 1.2.** *Let $k^+ = \mathbb{Q}(\sqrt{m}\,)$ with $m \in \mathbb{N}$, and put $k^- = \mathbb{Q}(\sqrt{-3m}\,)$; then the 3-ranks $r_3(k^+)$ and $r_3(k^-)$ of $\mathrm{Cl}(k^+)$ and $\mathrm{Cl}(k^-)$ satisfy the inequalities $r_3(k^+) \le r_3(k^-) \le r_3(k^+) + 1$.*

Leopoldt [21] later generalized these propositions considerably and called his result the "Spiegelungssatz". For expositions and generalizations, see Kuroda [19], Oriat [23, 26], Satgé [29], Oriat & Satgé [27], and G. Gras [10].

Damey & Payan [4] found an analog of Proposition 1.2 for 4-ranks of class groups of quadratic number fields:

**Proposition 1.3.** *Let $k^+ = \mathbb{Q}(\sqrt{m}\,)$ be a real quadratic number field, and put $k^- = \mathbb{Q}(\sqrt{-m}\,)$. Then the 4-ranks $r_4^+(k^+)$ and $r_4(k^-)$ of $\mathrm{Cl}^+(k^+)$ (the class group of $k^+$ in the strict sense) and $\mathrm{Cl}(k^-)$ satisfy the inequalities $r_4^+(k^+) \le r_4(k^-) \le r_4^+(k^+) + 1$.*

Other proofs were given by G. Gras [8], Halter-Koch [12], and Uehara [33]; for a generalization, see Oriat [24, 25].

In 1974, Callahan [2] discovered the following result; although it gives a connection between $p$-ranks of class groups of different number fields, its proof differs considerably from those of classical reflection theorems:

**Proposition 1.4.** *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 $d$ (then $Kk/k$ is a cyclic unramified extension of $k$), and let $r_3(k)$ and $r_3(K)$ denote the 3-ranks of $\mathrm{Cl}(k)$ and $\mathrm{Cl}(K)$, respectively. Then $r_3(K) = r_3(k) - 1$.*

Callahan could only prove that $r_3(k) - 2 \le r_3(K) \le r_3(k) - 1$, but conjectured that in fact $r_3(K) = r_3(k) - 1$. This was verified later by G. Gras [9] and Gerth [7]. Callahan's result was generalized by Bölling [1]:

**Proposition 1.5.** *Let $L/\mathbb{Q}$ be a normal extension with Galois group the dihedral group of order $2p$, where $p$ is an odd prime, and let $K$ be any of its subfields of degree $p$. Assume that the quadratic subfield $k$ of $L$ is complex, and that $L/k$ is unramified. Then*

$$r_p(k) - 1 \le r_p(K) \le \frac{p-1}{2}(r_p(k) - 1),$$

*where $r_p(k)$ and $r_p(K)$ denote the $p$-ranks of the class groups of $k$ and $K$, respectively.*

It is this result that we generalize to arbitrary base fields in this article. Our proof will be much less technical than Bölling's, who used the Galois cohomological machinery presented in Koch's book [17].

We conclude our survey of reflection theorems with the following result by Kobayashi [16] (see also Gerth [6]):

**Proposition 1.6.** *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 $L = K(\sqrt{-3}\,)$. Then $\mathrm{rk}\ \mathrm{Cl}_3(L) = 2 \cdot \mathrm{rk}\ \mathrm{Cl}_3(K)$.*

This was generalized subsequently by G. Gras [9] to the following result; $\mathrm{Spl}(k/\mathbb{Q})$ denotes the set of primes in $\mathbb{Q}$ that split in $k$.

**Proposition 1.7.** *Let $K$ be a cubic number field with normal closure $L$. Assume that $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$, and let $k$ denote the quadratic subfield of $L$. If no prime $p \in \mathrm{Spl}(k/\mathbb{Q})$ ramifies in $L/k$, and if $3 \nmid h(k)$, then $\mathrm{rk}\ \mathrm{Cl}_3(L) = 2 \cdot \mathrm{rk}\ \mathrm{Cl}_3(K)$.*

It seems plausible that the results of Proposition 1.5 hold for a large variety of nonabelian extensions. Computer experiments suggest a rather simple result normal extensions of $\mathbb{Q}$ with Galois group $A_4$. In fact, consider a cyclic cubic extension $k/\mathbb{Q}$, and let $2r$ denote the 2-rank of $\mathrm{Cl}(k)$. Then there exist $r$ nonconjugate quartic extensions $K/\mathbb{Q}$ such that (cf. [14])

1. $Kk$ is the normal closure of $K/\mathbb{Q}$, and $\mathrm{Gal}(Kk/\mathbb{Q}) \simeq A_4$;
2. $Kk/k$ is an unramified normal extension with $\mathrm{Gal}(Kk/k) \simeq (2,2)$.

**Conjecture 1.** *Let $L/\mathbb{Q}$ be an $A_4$ extension unramified over its cubic subfield $k$, and let $K$ denote one of the four conjugate quartic subfields of $L$. Then we have the following inequalities:*

$$\begin{aligned} \mathrm{rk}\ \mathrm{Cl}_2(k) &\ \ge\ \mathrm{rk}\ \mathrm{Cl}_2(K) &&\ \ge\ \mathrm{rk}\ \mathrm{Cl}_2(k) - 2, \\ \mathrm{rk}\ \mathrm{Cl}_2^+(k) + 1 &\ \ge\ \mathrm{rk}\ \mathrm{Cl}_2^+(K) &&\ \ge\ \mathrm{rk}\ \mathrm{Cl}_2^+(k) - 1 \end{aligned}$$

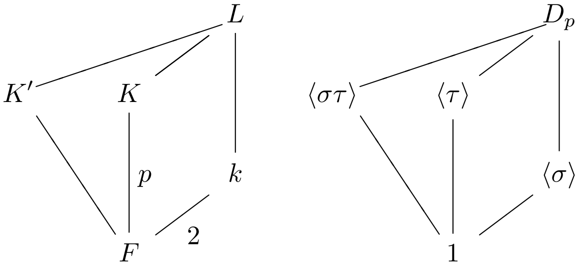
Examples show that these inequalities are best possible. In fact, consider the cyclic cubic extension $k$ generated by a root of the cubic polynomial $f(x) = x^3 - ax^2 - (a+3)x - 1$; choose $b \in \mathbb{N}$ odd and $a = \frac{1}{2}(b^2-3)$. Then $L = k(\sqrt{\alpha-2}, \sqrt{\alpha'-2}\,)$ is an $A_4$-extension of $\mathbb{Q}$, $L/k$ is unramified, and using PARI we find that $\mathrm{Cl}(k) \simeq (4,4,2,2)$, $\mathrm{Cl}(K) \simeq (2,2)$ for $a = 143$, and $\mathrm{Cl}(k) \simeq (114,2)$, $\mathrm{Cl}(K) \simeq (4,2)$ for $a = 1011$.

## 2. The Main Results

Let $p = 2m+1$ be an odd prime and let

$$D_p = \langle \sigma, \tau : \sigma^p = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$$

denote the dihedral group of order $2p$. Put $\nu = 1 + \sigma + \sigma^2 + \ldots + \sigma^{p-1}$; then a simple calculation gives $\nu\tau = \tau\nu$ and $\nu\sigma = \sigma\nu$.



Let $F$ be a number field with class number not divisible by $p$, $L/F$ a dihedral extension with Galois group $\mathrm{Gal}(L/F) \simeq D_p$, $k$ its quadratic subfield, and $K$ the fixed field of $\tau$. Note that $K' = K^{\sigma^m}$ is the fixed field of $\sigma\tau$.

In the sequel, $L/k$ will always be unramified. Our main result generalizes Bölling's theorem to base fields $F$ with class number prime to $p$:

**Theorem 2.1.** *Let $F$ be a number field with class number not divisible by $p$, let $L/F$ be a $D_p$-extension such that $L/k$ is unramified, and let $r_p(k)$ and $r_p(K)$ denote the $p$-ranks of the class groups of $k$ and $K$, respectively; then*

$$r_p(k) - 1 - e \le r_p(K),$$

*where $p^e = (E_F : NE_K)$.*

The idea of the proof of Theorem 2.1 is to compare the class groups of $K$ and $k$ by lifting them to $L$ and studying homomorphisms between certain subgroups of $\mathrm{Cl}_p(L)$. We get inequalities for the ranks by computing the orders of elementary abelian $p$-groups.

If $F = \mathbb{Q}$ or if $F$ is a complex quadratic number field (different from $\mathbb{Q}(\sqrt{-3}\,)$ if $p = 3$), then $e = 0$ since in these cases $E_F$ is torsion of order not divisible by $p$.

Actually, Bölling's upper bound from Prop. 1.5 is conjectured to be valid in general:

**Conjecture 2.** *Under the assumptions of Theorem 2.1 we have*

$$r_p(K) \le \frac{p-1}{2}(r_p(k) - 1).$$

We will prove Conjecture 2 if $p = 3$, if $r_p(k) = 1$, or if $\mathrm{Cl}_p(k) = (p,p)$; by Bölling's result, the upper bound holds if $F = \mathbb{Q}$ and $k$ is complex quadratic.

**Conjecture 3.** *Fix an odd prime $p$ and a number field $F$ with class number not divisible by $p$. Then for every integer $e$ with $0 \le e \le \dim E_F/E_F^p$, every integer $r \ge 1$ and every $R \ge 0$ such that $r - 1 - e \le R \le \frac{p-1}{2}(r-1)$ there exist dihedral extensions $L/F$ satisfying the assumptions of Theorem 2.1 such that $r_p(k) = r$, $r_p(K) = R$, and $(E_F : N_{K/F}E_K) = p^e$.*

A proof of Conjecture 3 seems to be completely out of reach; it expresses the expectation that the bounds in Theorem 2.1 and Conjecture 2 are best possible.

Using the results needed for the proof of Theorem 2.1, we get the following class number formula almost for free:

**Theorem 2.2.** *Let $L/F$ be a dihedral extension of degree $2p$, where $p$ is an odd prime, and assume that $L$ is unramified over the quadratic subextension $k$ of $L/K$. Let $q = (E_L : E_K E_{K'} E_k)$ denote the unit index of $L/F$ and write $a = 1 + \lambda(k) - \lambda(F)$, where $\lambda(M)$ denotes the $\mathbb{Z}$-rank of the unit group of a number field $M$. Then*

$$h_L = p^{-a} q h_k \Big(\frac{h_K}{h_F}\Big)^2. \tag{1}$$

In the special case $F = \mathbb{Q}$, an arithmetic proof of the class number formula for dihedral extensions of degree $2p$ (even without the restriction that $L/k$ be unramified) was given by Halter-Koch [11].

A simple application of the lower bound in Theorem 2.1 gives

**Theorem 2.3.** *Let $L/F$ be as in Theorem 2.1. If $r_p(k) \ge e + 2$, then there exists a normal unramified extension $M/k$ (containing $L$) with $\mathrm{Gal}(M/k) \simeq E(p^3)$, the nonabelian group of order $p^3$ and exponent $p$.*

In the special case where $F$ is $\mathbb{Q}$ or a complex quadratic number field $\ne \mathbb{Q}(\sqrt{-3}\,)$ this was proved by Nomura [22] (note that $e = 0$ in these cases).

## 3. Preliminaries

In this section we collect some results that will be needed in the sequel.

Let $\mathrm{Am} = \mathrm{Am}(L/k) = \{c \in \mathrm{Cl}_p(L) : c^\sigma = c\}$ denote the ambiguous $p$-class group and $\mathrm{Am}_{\rm st} = \{c = [\mathfrak a] \in \mathrm{Am} : \mathfrak a^\sigma = \mathfrak a\}$ its subgroup of strongly ambiguous ideal classes. Since $L/k$ is unramified, ambiguous ideals are ideals from $k$, hence $\mathrm{Am}_{\rm st} = \mathrm{Cl}_p(k)^j$, where $j : \mathrm{Cl}(k) \longrightarrow \mathrm{Cl}(L)$ is the transfer of ideal classes. This proves

**Lemma 3.1.** *For unramified extensions $L/k$, the sequence*

$$1 \longrightarrow \kappa_{L/k} \longrightarrow \mathrm{Cl}_p(k) \xrightarrow{\ j\ } \mathrm{Am}_{\rm st} \longrightarrow 1,$$

*where $\kappa_{L/k}$ is the capitulation kernel, is exact.*

The next lemma is classical; it measures the difference between the orders of ambiguous and strongly ambiguous ideal classes:

**Lemma 3.2.** *Let $L/k$ be a cyclic extension of prime degree $p$. Then the factor group $\mathrm{Am}\,/\,\mathrm{Am}_{\rm st}$ is an elementary abelian $p$-group. In fact, we have the exact sequence*

$$1 \longrightarrow \mathrm{Am}_{\rm st} \longrightarrow \mathrm{Am} \xrightarrow{\ \vartheta\ } E_k \cap NL^\times/NE_L \longrightarrow 1. \tag{2}$$

*If, in addition, $L/k$ is unramified, then $E_k \cap NL^\times = E_k$, and we find*

$$1 \longrightarrow \mathrm{Am}_{\rm st} \longrightarrow \mathrm{Am} \xrightarrow{\ \vartheta\ } E_k/NE_L \longrightarrow 1. \tag{3}$$

*Proof.* Let us start by defining $\vartheta$. Write $c = [\mathfrak{a}] \in \mathrm{Am}$; then $\mathfrak{a}^{\sigma-1} = (\alpha)$ and $\varepsilon := N\alpha \in E_k$. Now put $\vartheta(c) = \varepsilon NE_L$. We claim that $\vartheta$ is well defined: in fact, if $c = [\mathfrak{b}]$ and $\mathfrak{b}^{\sigma-1} = (\beta)$, then $\mathfrak{a} = \gamma\mathfrak{b}$ for some $\gamma \in L^\times$; thus $\mathfrak{a}^{\sigma-1} = \gamma^{\sigma-1}\mathfrak{b}^{\sigma-1}$, and this shows that $\alpha = \eta\gamma^{\sigma-1}\beta$, hence $N\alpha = N\eta N\beta$, and therefore $N\alpha \cdot NE_L = N\beta \cdot NE_L$.

We have $c \in \ker\vartheta$ if and only if $\varepsilon = N_{L/k}\eta$ for some unit $\eta$. Then $N(\alpha/\eta) = 1$, hence $\alpha/\eta = \beta^{1-\sigma}$, therefore $\beta\mathfrak{a}$ is an ambiguous ideal, and this implies that $c \in \mathrm{Am}_{\mathrm{st}}$. Conversely, if $c \in \mathrm{Am}_{\mathrm{st}}$, then $c = [\mathfrak{a}]$ with $\mathfrak{a}^{\sigma-1} = (1)$, hence $\vartheta(c) = 1$.

It remains to show that $\vartheta$ is surjective. Given $\varepsilon \in E_k \cap NL^\times$, write $\varepsilon = N_{L/k}\alpha$ for some $\alpha \in L^\times$: then $N_{L/k}(\alpha) = (1)$, hence Hilbert's theorem 90 for ideals implies that $(\alpha) = \mathfrak{a}^{\sigma-1}$ for some ideal $\mathfrak{a}$ in $\mathcal{O}_L$; clearly $\varepsilon NE_L = \vartheta([\mathfrak{a}])$, and this proves the claim.

Finally we have to explain why $E_k \cap NL^\times = E_k$ if $L/k$ is unramified. In this case, every unit is a local norm everywhere (in the absence of global ramification, every local extension is unramified, and units are always norms in unramified extensions of local fields), hence a global norm by Hasse's norm residue theorem for cyclic extensions $L/k$. □

For a cyclic group $G = \langle\sigma\rangle$ of order $n$ acting on an abelian group $A$, we denote by $A[N]$ the submodule of all elements killed by $N = 1 + \sigma + \sigma^2 + \ldots + \sigma^{n-1}$. Clearly $A^{1-\sigma} \subset A[N]$ in this situation.

**Proposition 3.1** (Furtwängler's Theorem 90)**.** *If $L/k$ is a cyclic unramified extension of prime degree $p$ and* $\mathrm{Gal}(L/k) = \langle\sigma\rangle$*, then* $\mathrm{Cl}_p(L)[N] = \mathrm{Cl}_p(L)^{1-\sigma}$.

*Proof.* This is a special case of the principal genus theorem of classical class field theory; see [20]. □

**Lemma 3.3.** *Let $A$ be a $D_p$-module; then $A^{1-\sigma} \subseteq A^{1+\tau}A^{1+\sigma\tau}$.*

*Proof.* For $a \in A$ we have $a^{1-\sigma} = (a^{-\sigma})^{1+\tau}a^{1+\sigma\tau}$. □

## 4. Galois Action

Let $m > 1$ be an integer, $p \equiv 1 \bmod m$ an odd prime, and $r$ an element of order $m$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Consider the Frobenius group

$$F_{mp} = \langle \sigma, \tau : \sigma^p = \tau^m = 1, \tau^{-1}\sigma\tau = \sigma^r \rangle.$$

In the following, let $s \in \mathbb{F}_p$ denote the inverse of $r$; note that $\tau\sigma\tau^{-1} = \tau^s$.

The results proved for $F_{mp}$-extensions will only be needed in the special case $D_p = F_{2p}$.

Let $A$ be an abelian $p$-group and $F_{mp}$-module. Then the action of $H = \langle\tau\rangle \simeq \mathbb{Z}/m\mathbb{Z}$ allows us to decompose $A$ into eigenspaces

$$A = \bigoplus_{j=0}^{m-1} A(j),$$

where $A_j = \{a \in A : a^\tau = a^{r^j}\}$. Note that $A(j) = e_j A$ for

$$e_j = \frac{1}{m}\sum_{k=0}^{m-1} s^{jk}\tau^k;$$

the set $\{e_0, e_1, \ldots, e_{m-1}\}$ is a complete set of orthogonal idempotents of the group ring $(\mathbb{Z}/m\mathbb{Z})[F_{mp}]$. Also observe that $A(0) = A^H$ is the fixed module of $A$ under the action of $H$.

**Lemma 4.1.** *Let $A, B, C$ be abelian $p$-groups and $H$-modules. If*

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota"] & B \arrow[r, "\pi"] & C \arrow[r] & 1 \end{tikzcd}$$

*is an exact sequence of $H$-modules, then so is*

$$\begin{tikzcd} 1 \arrow[r] & A(j) \arrow[r] & B(j) \arrow[r] & C(j) \arrow[r] & 1 \end{tikzcd}$$

*for every $0 \le j \le m-1$.*

*Proof.* This is a purely formal verification based on the fact that, by the assumption that $\iota$ and $\pi$ be $H$-homomorphisms, the action of the $e_j$ commutes with $\iota$ and $\pi$. □

**Proposition 4.1.** *Assume that $A$, $B$, $C$ are abelian $p$-groups and $H$-modules, that*

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota"] & B \arrow[r, "\pi"] & C \arrow[r] & 1 \end{tikzcd}$$

*is an exact sequence of abelian groups, and that $\iota(a^\tau) = \iota(a)^\tau$ and $\pi(b^\tau) = \pi(b)^{s\tau}$. Then*

$$\begin{tikzcd} 1 \arrow[r] & A(j) \arrow[r, "\iota"] & B(j) \arrow[r, "\pi"] & C(j+1) \arrow[r] & 1 \end{tikzcd}$$

*is exact for every $0 \le j \le m-1$.*

*Proof.* Define an $H$-module $C'$ by putting $C = C'$ as an abelian group and letting $\tau$ act on $C'$ via $c \longmapsto c^{s\tau}$. Then

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota"] & B \arrow[r, "\pi"] & C' \arrow[r] & 1 \end{tikzcd}$$

is an exact sequence of $H$-modules, and taking the $e_j$-part we get the exact sequence

$$\begin{tikzcd} 1 \arrow[r] & A(j) \arrow[r] & B(j) \arrow[r] & C'(j) \arrow[r] & 1. \end{tikzcd}$$

But $C'(j) = \{c \in C : c^{s\tau} = c^{r^j}\} = \{c \in C : c^\tau = c^{r^{j+1}}\} = C(j+1)$. □

Before we can apply the results above to our situation, we have to check that the homomorphism $\vartheta$ in (2) satisfies the assumption of Prop. 4.1.

**Lemma 4.2.** *Let $L/F$ be an $F_{mp}$-extension. Then the map $\vartheta$ in* (2) *(and therefore also in* (3)*) has the property $\vartheta(c^\tau) = \vartheta(c)^{s\tau}$.*

*Proof.* Write $c = [\mathfrak{a}]$, $\mathfrak{a}^{\sigma-1} = (\alpha)$, and $N_{L/k}\alpha = \varepsilon$; then $\vartheta(c) = \varepsilon N_{L/k}E_L$. We have $\tau(\sigma-1) = (\sigma^s-1)\tau = (\sigma-1)\phi\tau$ for $\phi = 1 + \sigma + \ldots + \sigma^{s-1}$, hence $(\mathfrak{a}^\tau)^{\sigma-1} = (\mathfrak{a}^{\sigma-1})^{\phi\tau} = (\alpha^{\phi\tau})$. Since the norm $1 + \sigma + \ldots + \sigma^{p-1}$ is in the center of $\mathbb{Z}[F_{mp}]$, we get $N_{L/k}(\alpha^{\phi\tau}) = (N_{L/k}\alpha)^{\phi\tau} = \varepsilon^{s\tau}$, and this shows $\vartheta(c^\tau) = c^{s\tau}$ as claimed. □

Let us now specialize to the case $m = 2$, where $F_{2p} = D_p$ is the dihedral group of order $2p$. For $D_p$-modules $A$ we put

$$A^+ = A(0) = \{a \in A : a^\tau = a\} \quad \text{and} \quad A^- = A(1) = \{a \in A : a^\tau = a^{-1}\}.$$

If $A$ is finite and has odd order, then $A = A^+ \oplus A^-$, $A^+ = A^{1+\tau}$ and $A^- = A^{1-\tau}$. In the following, let $H = \langle \tau \rangle$ denote the subgroup of $D_p$ generated by $\tau$.

The main ingredient in our proof of Theorem 2.1 will be the following result, which was partially proved by G. Gras [9]:

**Theorem 4.1.** *Let $L/F$ be a dihedral extension as above, and assume that the $p$-class group of $F$ is trivial and that $L/k$ is unramified. Then there is an exact sequence*

$$1 \longrightarrow \mathrm{Am}_{\mathrm{st}} \xrightarrow{\iota} \mathrm{Am}^- \xrightarrow{\vartheta} E_F/NE_K \longrightarrow 1. \tag{4}$$

*Moreover, $\mathrm{Am}^+ \simeq (E_k/NE_L)^-$; in particular, $\mathrm{Am}^+$ is an elementary abelian group of order $p^{\rho-1-e}$, where $p^\rho = \#\kappa_{L/k}$ is the order of the capitulation kernel and $p^e = (E_F : NE_K)$.*

*Proof.* We apply Proposition 4.1 with $i = 1$ to (3). Clearly $\tau$ acts as $-1$ on $\mathrm{Am}_{\mathrm{st}}$, hence $\mathrm{Am}_{\mathrm{st}}^- = \mathrm{Am}_{\mathrm{st}}$. Thus we only have to show that the plus part of $E_k/N_{L/k}E_L$ is isomorphic to $E_F/N_{K/F}E_K$. By sending $\varepsilon N_{K/F}E_K$ to $\varepsilon N_{L/k}E_L$ we get a homomorphism $\psi : E_F/N_{K/F}E_K \longrightarrow (E_k/N_{L/k}E_L)^+$.

We claim that $\psi$ is injective; in fact, $\ker\psi = \{\varepsilon N_{K/F}E_K : \varepsilon \in N_{L/k}E_L\}$; but $\varepsilon = N_{L/k}\eta$ implies $\varepsilon^2 = \varepsilon^{1+\tau} = N_{L/k}\eta^{1+\tau} = N_{K/F}\eta^{1+\tau}$. Thus $\varepsilon^2 \in N_{K/F}E_K$, hence so is $\varepsilon^{1+p} = (\varepsilon^2)^{(p+1)/2}$. Since $E_F/N_{K/F}E_K$ is a $p$-group, we have $\varepsilon \in N_{K/F}E_K$.

Moreover, $\psi$ is surjective: in fact, if $\varepsilon N_{L/k}E_L$ is fixed by $\tau$, then $\varepsilon^2 N_{L/k}E_L = \varepsilon^{1+\tau}N_{L/k}E_L$ is clearly in the image of $\psi$, and the claim follows again from the fact that $E_k/N_{L/k}E_L$ is a $p$-group.

Applying Proposition 4.1 with $i = 0$ yields the isomorphism $\mathrm{Am}^+ \simeq (E_k/NE_L)^-$; since $E_k/NE_L$ is elementary abelian, so is $\mathrm{Am}^+$. Moreover, the decomposition into eigenspaces $E_k/NE_L = (E_k/NE_L)^- \oplus (E_k/NE_L)^+$ shows

$$\#\,\mathrm{Am}^+ = \frac{(E_k : NE_L)}{(E_F : NE_K)}.$$

The exact sequence (3.1) shows that $p^\rho = \#\,\mathrm{Cl}_p(k)/\#\,\mathrm{Am}_{\mathrm{st}}$; since

$$\#\,\mathrm{Am}_{\mathrm{st}} = \frac{\#\,\mathrm{Cl}_p(k)}{p(E_k : NE_L)},$$

this implies that $p^\rho = p(E_k : NE_L)$, hence $\#\,\mathrm{Am}^{1+\tau} = \frac{(E_k:NE_L)}{p(E_F:NE_K)} = p^{\rho-1-e}$. □

## 5. The Class Number Formula

As a simple application of the exact sequence (4), let us prove the class number formula (1).

*Proof of Theorem 2.2.* For primes $l \neq p$, equation (1) claims that the $l$-class number of $L$ is given by $h_l(L) = (h_l(K)/h_l(F))^2 h_l(k)$; in fact we have an isomorphism

$$\mathrm{Cl}_l(L) \simeq \mathrm{Cl}_l(k) \times \mathrm{Cl}_l(K/F) \times \mathrm{Cl}_l(K'/F), \tag{5}$$

where $\mathrm{Cl}(K/F)$ is the relative class group of $K/F$ defined by the exact sequence

$$1 \longrightarrow \mathrm{Cl}(K/F) \longrightarrow \mathrm{Cl}(K) \xrightarrow{N_{K/F}} \mathrm{Cl}(F) \longrightarrow 1;$$

note that the norm is surjective since $K/F$ is nonabelian of prime degree.

The isomorphism (5) follows from the fact that the transfer of ideal classes $j_{k\to L}$ : is injective and the norm $N_{L/k}$ is surjective on classes of order coprime to $p$, hence $N_{L/k} \circ j_{k\to L}(c) = c^l$ induces an automorphism of $\mathrm{Cl}_l(k)$, which in turn implies that the sequence

$$1 \longrightarrow \mathrm{Cl}_l(L)[N] \longrightarrow \mathrm{Cl}_l(L) \longrightarrow \mathrm{Cl}_l(k) \longrightarrow 1$$

splits, i.e. $\mathrm{Cl}_l(L) \simeq \mathrm{Cl}_l(k) \times \mathrm{Cl}_l(L)[N]$. We now need the following result of Jaulent (see [3, Thm. 7.8.]) in the special case $G = D_{2p}$, $H = \langle\tau\rangle$, and $\Delta = \langle\sigma\rangle$:

**Proposition 5.1.** *Let $L/k$ be a normal extension with Galois group $G$, and assume that $G$ is a semidirect product of $H$ with a normal subgroup $\Delta$ on which $H$ acts faithfully. Let $K$ and $k$ denote the fixed fields of $\Delta$ and $H$, respectively. Then the homomorphism*

$$j^* : \mathrm{Cl}(K/F) \longrightarrow \mathrm{Cl}(L/k)^H$$

*is an isomorphism.*

This result guarantees that the transfer of ideal classes $\mathrm{Cl}_2(K/F) \longrightarrow \mathrm{Cl}_2(L)$ is injective; for primes $l \nmid 2p$, the injectivity of $\mathrm{Cl}_l(K) \longrightarrow \mathrm{Cl}_l(L)$ is trivial. By Furtwängler's Theorem 90 and Lemma 3.3 we have $\mathrm{Cl}_l(L)[N] = \mathrm{Cl}_l(K/F)\,\mathrm{Cl}_l(K'/F)$.

We claim that $\mathrm{Cl}_l(K/F) \cap \mathrm{Cl}_l(K'/F) = 1$: a class $c \in \mathrm{Cl}_l(K/F) \cap \mathrm{Cl}_l(K'/F)$ is fixed by $\tau$ and $\sigma\tau$, hence by $\sigma$, and since it is killed by the norm, we find $c^p = 1$; since $c$ has $l$-power order, this implies $c = 1$.

It remains to prove the $p$-part of the class number formula. In the rest of the proof, all class numbers and class groups are $p$-class numbers and $p$-class groups.

Let $N = N_{L/k}$ denote the relative norm of $L/k$. Since $L/k$ is unramified and cyclic, we know that $(\mathrm{Cl}(k) : N\,\mathrm{Cl}(L)) = p$. Thus

$$h_L = \#\,\mathrm{Cl}(L) = \#\,\mathrm{Cl}(L)[N] \cdot \#N\,\mathrm{Cl}(L) = \frac{h_K^2}{\#\,\mathrm{Am}^{1+\tau}} \cdot \frac{h_k}{p} = p^{e-\rho} h_K^2 h_k. \tag{6}$$

If $B$ is a subgroup of finite index in an abelian group $A$ and if $f : A \longrightarrow A'$ is a group homomorphism, then $(A : B) = (A^f : B^f)(\ker f : \ker f \cap B)$, where $A^f$ and $B^f$ denote the images of $A$ and $B$ under $f$.

Now let us apply this to the special situation where $f$ is given by the norm map $N : E_L/E_K E_{K'} E_k \longrightarrow E_k/E_k^p N E_K$. We have

$$(E_L : E_K E_{K'} E_k) = (NE_L : N(E_K E_{K'} E_k)) \cdot (E_L[N] : E_L[N] \cap E_K E_{K'} E_k).$$

**Lemma 5.1.** *If $L/k$ is unramified, then $(E_L[N] : E_L[N] \cap E_K E_{K'} E_k) = 1$.*

*Proof.* It suffices to show that $E_L[N] \subseteq E_K E_{K'}$. Assume therefore that $N_{L/k}\varepsilon = 1$ for some $\varepsilon \in E_L$. Then $\varepsilon = \alpha^{1-\sigma}$ for some $\alpha \in L^\times$ by Hilbert's Theorem 90, hence $\mathfrak{a} = (\alpha)$ is ambiguous. Since $L/k$ is unramified, $\mathfrak{a}$ must be an ideal from $k$, and this implies that $\alpha = \eta a$ for some $\eta \in E_L$ and $a \in k^\times$. But then $\varepsilon = \alpha^{1-\sigma} = \eta^{1-\sigma} \in E_L^{1-\sigma}$, and by Lemma 3.3 we have $E_L^{1-\sigma} \subseteq (E_L^{-\sigma})^{1+\tau} E_L^{1+\sigma\tau} \subseteq E_K E_{K'}$. □

Thus $q = (NE_L : N(E_K E_{K'} E_k))$; clearly $N(E_K E_{K'} E_k) = E_k^p N E_K$, and we can transform $q$ as follows:

$$\begin{aligned}(NE_L : N(E_K E_{K'} E_k)) = (NE_L : E_k^p N E_K) \ &= \ \frac{(E_k : E_k^p N E_K)}{(E_k : NE_L)} \\ &= \frac{(E_k : E_k^p)(E_k^p : E_k^p N E_K)}{(E_k : NE_L)} \\ &= \frac{(E_k : E_k^p)(E_k^p E_F : E_k^p N E_K)}{(E_k^p E_F : E_k^p)(E_k : NE_L)}.\end{aligned}$$

Now

$$\begin{aligned}(E_k^pE_F : E_k^pNE_K) = \frac{(E_k^pE_F : E_k^p)}{(E_k^pNE_K : E_k^p)} \ &= \ \frac{(E_F : E_F \cap E_k^p)}{(NE_K : NE_K \cap E_k^p)} \\ = \frac{(E_F : E_F^p)}{(NE_K : E_F^p)} \ &= \ (E_F : NE_K),\end{aligned}$$

as well as

$$(E_k^pE_F : E_k^p) = (E_F : E_F \cap E_k^p) = (E_F : E_F^p),$$

hence we get

$$q \ = \ \frac{(E_k : E_k^p)(E_F : NE_K)}{(E_F : E_F^p)(E_k : NE_L)} \ = \ p^{\lambda(k)-\lambda(F)}p^{e+1-\rho},$$

where $\lambda(M)$ denotes the $\mathbb{Z}$-rank of the unit group of a number field $M$. Note that $W_L = W_k$ (where $W_M$ denotes the group of roots of unity in $M$) since $L/F$ is non-abelian.

Collecting everything we find

$$h_L = p^{e-\rho}h_K^2h_k = p^{-a}qh_K^2h_k$$

for the $p$-class numbers, and this proves the theorem. □

## 6. The Lower Bound for $r_p(K)$

The idea of the proof is to lift parts of $\mathrm{Cl}_p(k)$ and $\mathrm{Cl}_p(K)$ to $L$ and compare their images. We start with the group $\mathrm{Cl}(k)[p]$ of rank $r_p(k)$; its image after lifting it to $\mathrm{Cl}(L)$ has rank $\mathrm{rk}\ \mathrm{Cl}(k)[p]^j = r_p(k) - \rho$. Now observe that $\mathrm{Cl}(k)[p]^j$ is a subgroup of $\mathrm{Cl}_p(L)$ that is killed by $p$, $1+\tau$, $\sigma - 1$, and the relative norm $N = N_{L/k}$. In particular, $\mathrm{Cl}(k)[p]^j \subseteq \mathcal{C}_0$, where $\mathcal{C}_0 = \{c \in \mathrm{Cl}_p(L) : c^p = c^{1+\tau} = c^{1-\sigma} = 1\}$. The key result is the following observation:

**Proposition 6.1.** *There exists a monomorphism $\mathcal{C}_0 \hookrightarrow \mathrm{Cl}(K)[p]/\mathrm{Am}^+$.*

We know that $\mathrm{rk}\ \mathrm{Cl}(K)[p] = r_p(K)$ and $\mathrm{rk}\ \mathrm{Am}^+ = \rho - 1 - e$; since both groups are elementary abelian we deduce that $\mathrm{rk}\ \mathrm{Cl}(K)[p]/\mathrm{Am}^+ = r_p(K) - \rho + e + 1$. Thus from $\mathrm{Cl}(k)[p]^j \subseteq \mathcal{C}_0 \subseteq \mathrm{Cl}(K)[p]/\mathrm{Am}^+$ we deduce that

$$r_p(k) - \rho = \mathrm{rk}\ \mathrm{Cl}(k)[p]^j \le \mathrm{rk}\ \mathrm{Cl}(K)[p]/\mathrm{Am}^+ = r_p(K) - \rho + e + 1,$$

and this proves Theorem 2.1.

It remains to prove Proposition 6.1. The next result (showing in particular that $\mathrm{Am}^+ \subseteq \mathrm{Cl}_p(K)$) can be found in Halter-Koch [11]:

**Lemma 6.1.** *Let $L/F$ be as above; in particular, assume that $L/k$ is unramified. We have $\mathrm{Cl}_p(L)[N] = \mathrm{Cl}_p(K)\,\mathrm{Cl}_p(K')$ and $\mathrm{Cl}_p(K) \cap \mathrm{Cl}_p(K') = \mathrm{Am}^+$, where $K$ and $K'$ are the fixed fields of $\tau$ and $\sigma\tau$.*

*Proof.* Since $(L : K) = 2$, the transfer of ideal classes $\mathrm{Cl}_p(K) \longrightarrow \mathrm{Cl}_p(L)$ is injective, and we can view $\mathrm{Cl}_p(K)$ as a subgroup of $\mathrm{Cl}_p(L)$. Clearly $\mathrm{Cl}_p(K)$ and $\mathrm{Cl}_p(K')$ are killed by $N$, so $\mathrm{Cl}_p(K)\,\mathrm{Cl}_p(K') \subseteq \mathrm{Cl}_p(L)[N]$.

Using Lemma 3.3 we now find

$$\mathrm{Cl}_p(L)^{1-\sigma} \subseteq \mathrm{Cl}_p(L)^{1+\tau}\,\mathrm{Cl}_p(L)^{1+\sigma\tau} \subseteq \mathrm{Cl}_p(K)\,\mathrm{Cl}_p(K') \subseteq \mathrm{Cl}_p(L)[N],$$

and by Furtwängler's Theorem 90 we have equality throughout. □

*Proof of Prop. 6.1.* Given any $c \in \mathrm{Cl}_p(L)[N]$, we can write $c = c_1c_2$ with $c_1 \in \mathrm{Cl}_p(K)$ and $c_2 \in \mathrm{Cl}_p(K')$. Since $\mathrm{Cl}_p(K) \cap \mathrm{Cl}_p(K') = \mathrm{Am}^+$, the $c_i$ are determined modulo $\mathrm{Am}^+$, and we get a homomorphism $\lambda : \mathrm{Cl}_p(L)[N] \longrightarrow \mathrm{Cl}_p(K)/\mathrm{Am}^+$.

We claim that $c_1 \in \mathrm{Cl}(K)[p]$ if $c \in \mathcal{C}_0$. To prove this, assume that $c^\sigma = c$ and $c^p = 1$; from $c_2^{\sigma\tau} = c_2$ we get $c_2^\sigma = c_2^\tau$, and since $c^\tau = c^{-1}$ and $c_1^\tau = c_1$, we find $c^{-1} = c^\tau = c_1c_2^\tau$, that is, $c_2^\tau = c_1^{-2}c_2^{-1}$. This gives $c_1^\sigma = (cc_2^{-1})^\sigma = c_1c_2c_1^2c_2 = c_1^3c_2^2$. Induction shows that $c_1^{\sigma^t} = c_1^{2t+1}c_2^{2t}$ and $c_2^{\sigma^t} = c_1^{-2t}c_2^{1-2t}$. In particular,

$$c_1^\nu \;=\; c_1^{1+3+5+\ldots+2p-1}c_2^{2+4+\ldots+2p-2} \;=\; c_1^{p^2}c_2^{(p-1)p} = c^{(p-1)p}c_1^p.$$

But since $c^p = 1$ and $c_1^\nu = 1$, this implies $c_1^p = 1$, that is, $c_1 \in \mathrm{Cl}(K)[p]$.

Now assume that $c \in \ker\lambda$; then $c_1 \in \mathrm{Am}^+$, hence $c = c_1c_2 \in \mathrm{Cl}(K')$. Thus $c$ is fixed by $\sigma$ and $\sigma\tau$, hence by $\tau$; since $c \in \mathrm{Cl}(L)^-$, this implies $c^2 = c^{1+\tau} = 1$, hence $c = 1$. Thus $\lambda$ is injective. □

## 7. Embedding Problems

Theorem 2.3 on the existence of unramified $E(p^3)$-extensions is a rather simple consequence of our results. Let $k/F$ be a quadratic extensions, $p$ and odd prime such that $p \nmid h(F)$, and $L/F$ a normal extension with $\mathrm{Gal}(L/F) \simeq D_p$ and $L/k$ unramified. If $\mathrm{rk}\ \mathrm{Cl}_p(k) \geq 2 + e$, then Theorem 2.1 guarantees that any nonnormal subextension $K$ of $L/F$ will have class number divisible by $p$. Let $M/K$ be an unramified cyclic extension of $K$, and let $N$ denote the normal closure of $LM/k$. Then $N/k$ is a $p$-extension containing $L$, and its maximal abelian subextension $N^{\mathrm{ab}}$ has type $(p,p)$. Let $E/k$ be a central extension of $N^{\mathrm{ab}}/k$ of degree $p^3$ over $k$; then $\mathrm{Gal}(E/k) = E(p^3)$ or $\mathrm{Gal}(E/k) = \Gamma(p^3)$, where $\Gamma = \Gamma(p^3)$ is the nonabelian group of order $p^3$ and exponent $p^2$. We claim that $\mathrm{Gal}(E/k) = E(p^3)$.

We remark in passing that – in the case where $N \neq E$ – this follows immediately from the fact that $\Gamma(p^3)$ has trivial Schur multiplier. In general, we have to invoke the automorphism group $\mathrm{Aut}(\Gamma)$ of $\Gamma(p^3)$. It is known (see Eick [5] and e.g. Schulte [31]) that $\mathrm{Aut}(\Gamma) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times p$-group, and that $(\mathbb{Z}/p\mathbb{Z})^\times$ acts trivially on exactly one of the two generators of $\Gamma/\Gamma'$. In particular, the unique element of order 2 in $\mathrm{Aut}(\Gamma)$ acts as $-1$ on one and trivially on the other generator.

On the other hand, $\mathrm{Gal}(N^{\mathrm{ab}}/F)$ is a generalized dihedral group by class field theory (since $p$ does not divide the class number of $F$), hence the element of order 2 in $\mathrm{Gal}(k/F)$ acts as $-1$ on both generators of $\mathrm{Gal}(N^{\mathrm{ab}}/k)$: this means that $\mathrm{Gal}(N/k) \neq \Gamma(p^3)$, and Theorem 2.3 follows.

## 8. The Upper Bound for $r_p(K)$

We will start by proving the upper bound in Theorem 2.1 in two special cases: a refinement of our techniques used to derive the lower bound will give the result if $p = 3$, and a simple Galois theoretic argument suffices to prove it in the case $r_p(k) = 1$.

### The Case $p = 3$.

In the special case $p = 3$ we can prove the upper bound $r_p(K) \leq r_p(k) - 1$ using the same techniques we used for deriving the lower bound. Our first ingredient holds in general:

**Lemma 8.1.** *We have* $\mathrm{rk}\ \mathrm{Am}_{\mathrm{st}}[N] = r_p(k) - \rho$ *and* $\mathrm{rk}\ \mathrm{Am}^-[N] \leq r_p(k) - \rho + e$.

*Proof.* Clearly $\mathrm{Cl}(k)[p]^j \subseteq \mathrm{Am}_{\mathrm{st}}[N]$; conversely, if $c \in \mathrm{Cl}_p(k)$ with $c^j \in \mathrm{Am}_{\mathrm{st}}[N]$, then $c^p = 1$, hence we actually have $\mathrm{Cl}(k)[p]^j = \mathrm{Am}_{\mathrm{st}}[N]$, and this proves that $\mathrm{rk}\,\mathrm{Am}_{\mathrm{st}}[N] = r_p(k) - \rho$.

The exact sequence

$$1 \longrightarrow \mathrm{Am}_{\mathrm{st}}[N] \longrightarrow \mathrm{Am}^-[N] \longrightarrow E_F/NE_K$$

derived from (4) shows that $\mathrm{rk}\,\mathrm{Am}^-[N] \le \mathrm{rk}\,\mathrm{Am}_{\mathrm{st}}[N] + e$. □

From now on assume that $p = 3$; then the map $c \longmapsto c^{1+2\sigma}$ defines a homomorphism $\mu : \mathrm{Cl}(K)[p] \longrightarrow \mathcal{C}_0$. In fact, since $c^\nu = c^3 = 1$, we have $\mu(c)^\sigma = c^{\sigma+2\sigma^2} = c^{-2-\sigma} = \mu(c)$ since $c^{\sigma^2} = c^{-1-\sigma}$. Moreover, $\mu(c)^\tau = c^{\tau(1+2\sigma^2)} = c^{-1-2\sigma} = c^{-1}$ since $c^\tau = c$ for $c \in \mathrm{Cl}(K)$; thus $\mu(c)$ is killed by $N$, $p$ and $1+\tau$, hence $\mu(c) \in \mathcal{C}_0$.

Next $c \in \ker\mu$ implies $c = c^\sigma$, i.e., $c \in \mathrm{Am}^+$, and clearly $\mathrm{Am}^+ \subseteq \ker\mu$: thus

**Proposition 8.1.** *If $p = 3$, then $\mathrm{Cl}(K)[p]/\mathrm{Am}^+ \simeq \mathcal{C}_0$.*

In particular, $r_p(K) - \rho + 1 + e = \mathrm{rk}\,\mathcal{C}_0$ if $p = 3$. Since $\mathcal{C}_0 \subseteq \mathrm{Am}^-[N]$, we find $r_p(K) - \rho + 1 + e \le r_p(k) - \rho + e$, and we have proved

**Theorem 8.1.** *If $p = 3$, then $r_p(k) - 1 - e \le r_p(K) \le r_p(k) - 1$.*

**The case $r_p(k) = 1$.**

The second special case of the upper bound that can be proved easily is

**Proposition 8.2.** *If $r_p(k) = 1$, then $r_p(K) = 0$.*

*Proof.* Assume not; then there exists a cyclic unramified extension $M/K$ of degree $p$. Let $N$ denote the normal closure of $ML/k$. If $N = ML$, then $ML/k$ has a Galois group of order $p^2$ and thus is abelian, and since $ML/L$ and $L/k$ are unramified, so is $ML/k$. Since $\mathrm{Cl}_p(k)$ is cyclic by assumption, we conclude that $\mathrm{Gal}(ML/k) = \mathbb{Z}/p^2\mathbb{Z}$, and since $p$ does not divide the class number of $F$, we conclude that $ML/F$ is normal and $\mathrm{Gal}(ML/F) \simeq D_{p^2}$. On the other hand, $\mathrm{Gal}(ML/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ by construction, and since the dihedral group of order $2p^2$ does not contain an abelian subgroup of order $2p$, we have a contradiction. □

**The Case $\mathrm{Cl}_p(k) \simeq (p,p)$.**

Our main tool will be the following result due to G. Gras [9]:

**Proposition 8.3.** *Let $p$ be an odd prime, $G = \langle\sigma\rangle$ a group of order $p$ generated by $\sigma$, and assume that $G$ acts on the abelian $p$-group $A$ in such a way that $\#A^G = \#\{a \in A : a^{\sigma-1} = 1\} = p$. Put $\nu = 1 + \sigma + \sigma^2 + \ldots + \sigma^{p-1}$, let $n$ be the smallest positive integer such that $A^{(\sigma-1)^n} = 1$, and write $n = \alpha(p-1)+\beta$ with $0 \le \beta \le p-2$.*

*If $A^\nu = 1$, then*

$$A \simeq (\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\beta \times (\mathbb{Z}/p^\alpha\mathbb{Z})^{p-1-\beta}.$$

*If $A^\nu \ne 1$, then*

$$A \simeq \begin{cases} (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^{n-2} & \text{if } n < p, \\ (\mathbb{Z}/p\mathbb{Z})^p & \text{if } n = p, \\ (\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\beta \times (\mathbb{Z}/p^\alpha\mathbb{Z})^{p-1-\beta} & \text{if } n > p. \end{cases}$$

*Note that $\#A = p^n$ and that the $p$-rank of $A$ is bounded by $p$.*

Assume now that $\mathrm{Cl}_p(k) \simeq (p,p) = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and put $A = \mathrm{Cl}_p(L)$. Then $\# A^G = \# \mathrm{Am}(L/k) = p$ by the ambiguous class number formula since every unit in $k$ is a norm from $L$. Moreover, $A_k = N_{L/k}A$ has index $p$ in $\mathrm{Cl}_p(k)$ by class field theory, hence $A_k = \langle c \rangle$ for some ideal class $c$ of order $p$, and we have to distinguish two cases:

(A) $c$ capitulates in $L/k$; then $A^\nu = 1$.
(B) $c$ does not capitulate in $L/k$; then $A^\nu \neq 1$.

Moreover, $\rho \geq e+1$ implies that the following classification is complete:

$$\# \mathrm{Cl}_p(K) \cap \mathrm{Cl}_p(K') = \begin{cases} 1 & \text{if } (\rho, e) = (1,0), (2,1) \\ p & \text{if } (\rho, e) = (2,0). \end{cases}$$

Applying the class number formula (6) we get

$$h_p(L) = p^{2+e-\rho} h_K^2 = p^\mu$$

for some integer $\mu \geq 1$. Now we can prove

**Theorem 8.2.** *Let $p$ be a prime and assume that $F$ is a number field whose class number is not divisible by $p$. Let $L/F$ be a normal extension with Galois group $D_p$, and let $L/k$ be unramified. Assume that $\mathrm{Cl}_p(k) \simeq (\mathbb{Z}/p\mathbb{Z})^2$. Then*

a) *$h_p(L) = h_p(K)^2 p^{2-\rho} = p^\mu$ for some $\mu \geq 2$, and in particular $\mu \equiv \rho \bmod 2$.*
b) *Write $\mu = \alpha(p-1) + \beta$ with $0 \leq \beta < p-1$; then the structure of $\mathrm{Cl}_p(L)$ is given by the following table:*

| *case* | $A$ | $B$ |
|---|---|---|
| $\mu > p$ | $(\mathbb{Z}/p^{\alpha+1}\mathbb{Z})^\beta \times (\mathbb{Z}/p^\alpha\mathbb{Z})^{p-1-\beta}$ | |
| $\mu = p$ | $(\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^{p-2}$ | $(\mathbb{Z}/p\mathbb{Z})^p$ |
| $\mu < p$ | $(\mathbb{Z}/p\mathbb{Z})^\mu$ | $(\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^{\mu-2}$ |

c) *Write $\mu - 1 = a(p-1) + b$, $0 \leq b \leq p-2$; note that $b$ is even if $\rho - e$ is odd. The structure of $\mathrm{Cl}_p(L)[N]$ and $\mathrm{Cl}_p(K)$ is given by*

$$\mathrm{Cl}_p(L)[N] \simeq (\mathbb{Z}/p^{a+1}\mathbb{Z})^b \times (\mathbb{Z}/p^a\mathbb{Z})^{p-1-b},$$

$$\mathrm{Cl}_p(K) \simeq \begin{cases} (\mathbb{Z}/p^{a+1}\mathbb{Z})^{b/2} \times (\mathbb{Z}/p^a\mathbb{Z})^{(p-1-b)/2} & \textit{if } \rho = e+1, \\ (\mathbb{Z}/p^{a+1}\mathbb{Z})^{(b+1)/2} \times (\mathbb{Z}/p^a\mathbb{Z})^{(p-2-b)/2} & \textit{if } \rho = 2, e = 0. \end{cases}$$

*Observe that $\mathrm{Cl}_p(K)$ is elementary abelian if and only if $\mu \leq p$. On the other hand, we have $\mathrm{rk}\, \mathrm{Cl}_p(K) = \frac{p-1}{2}$ whenever $\mu \geq p-1$.*

*Proof.* We already proved the class number formula in a), and b) follows by applying Prop. 8.3 to $A = \mathrm{Cl}_p(L)$. Similarly, the claims in c) about the structure of $\mathrm{Cl}_p(L)[N]$ follow by applying Prop. 8.3 to $A = \mathrm{Cl}_p(L)[N]$.

It remains to derive the structure of $\mathrm{Cl}_p(K)$. If $\rho = e+1$, then we have seen that $\mathrm{Cl}_p(K) \cap \mathrm{Cl}_p(K') = 1$, hence $\mathrm{Cl}_p(L)[N] \simeq \mathrm{Cl}_p(K) \oplus \mathrm{Cl}_p(K)$, and this allows us to deduce the structure of $\mathrm{Cl}_p(K)$ from that of $\mathrm{Cl}_p(L)$. If $(\rho, e) = (2,0)$, on the other hand, then $\mathrm{Cl}_p(L)[N] = \mathrm{Cl}_p(K)\,\mathrm{Cl}_p(K')$ with $\mathrm{Cl}_p(K) \cap \mathrm{Cl}_p(K') \simeq \mathbb{Z}/p$, and again the claims follow easily. □

**Examples.** Consider the cubic field $K_a$ generated by a root of the polynomial $x^3 + ax + 1$; let $d = \operatorname{disc} k$.

| $a$ | $d$ | $\mathrm{Cl}_3(k)$ | $\mathrm{Cl}_3(K_a)$ | $\mathrm{Cl}_3(L)$ |
|---|---|---|---|---|
| 29 | $-97583$ | $(3,3)$ | $(3)$ | $(3,3,3)$ |
| 10 | $-4027$ | $(3,3)$ | $(3)$ | $(3^2,3)$ |
| 70 | $-1372027$ | $(3,3)$ | $(3^2)$ | $(3^3,3^2)$ |
| 94 | $-3322363$ | $(3,3)$ | $(3^3)$ | $(3^4,3^3)$ |
| 755 | $-1721475527$ | $(3,3)$ | $(3^4)$ | $(3^5,3^4)$ |
| 409 | $-273671743$ | $(3,3)$ | $(3^5)$ | $(3^6,3^5)$ |

The data suggest that the exponent of $\mathrm{Cl}_3(K_a)$ is not bounded.

## 9. Examples

It is expected that the upper bounds are best possible even if $p > 3$. The following family of simplest dihedral quintics extracted from Kondo [18] show that the upper bound is attained for $p = 5$. Let $\alpha$ denote a root of

$$f(x) = x^5 - 2x^4 + (b+2)x^3 - (2b+1)x^2 + bx + 1,$$

and put $K = \mathbb{Q}(\alpha)$. Then $\operatorname{disc} K = d^2$ for some odd $d$, and if we choose the sign of $d$ such that $d \equiv 1 \bmod 4$, then then the splitting field $L$ of $f$ (which has Galois group $D_5$) is unramified over its quadratic subfield $k = \mathbb{Q}(\sqrt{d}\,)$ if $d$ is squarefree.

| $b$ | $d$ | $\mathrm{Cl}(k)$ | $\mathrm{Cl}(K)$ | $\mathrm{Cl}(L)$ |
|---|---|---|---|---|
| 1 | $-103$ | $(5)$ | 1 | 1 |
| 19 | $-38047$ | $(15,5)$ | $(20,4)$ | $(300,20,4,4)$ |
| 39 | $-280847$ | $(20,20)$ | $(55,5)$ | $(1100,220,5,5)$ |

Using $F = \mathbb{Q}(\sqrt{5}\,)$ as the base field, we find

| $b$ | $d$ | $\mathrm{Cl}(k)$ | $\mathrm{Cl}(K)$ |
|---|---|---|---|
| 41 | 47 | $(5)$ | 1 |
| 9 | 5447 | $(60,20)$ | $(55)$ |
| 16 | 23983 | $(50,10,5)$ | $(305)$ |
| 17 | 28199 | $(480,15)$ | $(4,4)$ |
| 39 | 280847 | $(1080,40)$ | $(55,5)$ |

Here are a few examples for $p = 3$ that also show that the term $e$ in our lower bound is necessary: let $d$ be the discriminant of a dihedral cubic number field $k_0$, and consider the fields $F = \mathbb{Q}(\sqrt{-3}\,)$, $K = k_0(\sqrt{-3}\,)$, $k = \mathbb{Q}(\sqrt{-3}, \sqrt{d}\,)$ and $L = Kk$.

| $d$ | $\mathrm{Cl}(k)$ | $\mathrm{Cl}(K)$ |
|---|---|---|
| $-31$ | $(3)$ | $(1)$ |
| $-107$ | $(3,3)$ | $(1)$ |
| $-4027$ | $(3,3,3)$ | $(6,2)$ |
| $-8751$ | $(12,3,3)$ | $(3,3)$ |
| 229 | $(6,3)$ | $(2)$ |
| 469 | $(6,6)$ | $(3)$ |
| 26821 | $(72,3)$ | $(18)$ |
| 2813221 | $(198,6,6,6)$ | $(285,3)$ |
| 13814533 | $(270,3,3,3,3)$ | $(360,3,3)$ |

## Acknowledgement

I thank Bettina Eick for her emails concerning the automorphism groups of the nonabelian groups of order $p^3$, and Robin Chapman as well as the referees for their comments on the manuscript.

## References

[1] 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 2

[2] T. Callahan, *The* 3*-class groups of non-Galois cubic fields I, II*, Mathematika **21** (1974), 72–89; 168–188 2

[3] H. Cohen, J. Martinet, *Étude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math. 404 (1990), 39–76 8

[4] 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 1

[5] B. Eick, *email 03.07.2002* 10

[6] F. Gerth, *On* 3*-class groups of pure cubic fields*, J. Reine Angew. Math. **278/279** (1975), 52-62 2

[7] F. Gerth, *Ranks of* 3*-class groups of non-Galois cubic fields*, Acta Arith. **30** (1976), 307–322 2

[8] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier* $\ell$; Ann. Inst. Fourier **23.3** (1973), 1–48; ibid. **23.4** (1973), 1–44 1

[9] G. Gras, *Sur les $\ell$-classes d'idéaux des extensions non galoisiennes de degré premier impair $\ell$ à la clôture galoisiennes diédrale de degré* $2\ell$, J. Math. Soc. Japan **26** (1974), 677–685 2, 6, 11

[10] G. Gras, *Théorèmes de réflexion*, J. Théor. Nombres Bordeaux **10** (1998), 399–499 1

[11] F. Halter-Koch, *Einheiten und Divisorenklassen in Galoisschen algebraischen Zahlkörpern mit Diedergruppe der Ordnung* 2*l für eine ungerade Primzahl l*, Acta Arith. **33** (1977), 353–364 4, 9

[12] F. Halter-Koch, *Über den* 4*-Rang der Klassengruppe quadratischer Zahlkörper*, J. Number Theory **19** (1984), 219–227 1

[13] E. Hecke, *Über nicht-reguläre Primzahlen und den Fermatschen Satz*, Nachr. Akad. Wiss. Göttingen (1910), 420–424 1

[14] H. Heilbronn, *On the* 2*-class group of cubic fields*, Studies in Pure Math., Academic Press 1971, 117–119; Collected Works, p. 248–250 2

[15] K. Ireland, M. Rosen, *A classical introduction into modern number theory*, Springer-Verlag 1

[16] 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 2

[17] H. Koch, *Galoissche Theorie der p-Erweiterungen*, VEB 1970; Engl. Transl.: *Galois Theory of p-Extensions*, Springer-Verlag 2002 2

[18] T. Kondo, *Some examples of unramified extensions over quadratic fields*, Sci. Rep. Tokyo Woman's Christian Univ., No. 120–121 (1997), 1399–1410. 13

[19] S.-N. Kuroda, *Über den allgemeinen Spiegelungssatz für Galoissche Zahlkörper*, J. Number Theory **2** (1970), 282–297 1

[20] F. Lemmermeyer, *The development of the principal genus theorem*, Gauss proceedings, Springer-Verlag 2003 5

[21] H. W. Leopoldt, *Zur Struktur der $\ell$-Klassengruppe galoisscher Zahlkörper*, J. Reine Angew. Math. **199** (1958), 165–174 1

[22] A. Nomura, *On the existence of unramified p-extensions*, Osaka J. Math. **28** (1991), 55–62 4

[23] B. Oriat, *Spiegelungssatz*, Publ. Math. Fac. Sci. Besançon 1975/76 1

[24] B. Oriat, *Relations entre les 2-groupes d'idéaux de $k(\sqrt{d}\,)$ et $k(\sqrt{-d}\,)$*, Astérisque **41–42** (1977), 247–249 1

[25] 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 1

[26] B. Oriat, *Generalisation du 'Spiegelungssatz'*, Astérisque **61** (1979), 169–175 1

[27] B. Oriat, P. Satgé, *Un essai de generalisation du 'Spiegelungssatz'*, J. Reine Angew. Math. **307/308** (1979), 134–159 1

[28] H. Reichardt, *Arithmetische Theorie der kubischen Körper als Radikalkörper*, Monatsh. Math. Phys. **40** (1933), 323–350 1

[29] P. Satgé, *Inégalités de miroir*, Sem. Delange-Pisot-Poitou (1967/77), **18** 4pp 1

[30] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math. **166** (1932), 201–203 1

[31] M. Schulte, *Automorphisms of metacyclic p-groups with cyclic maximal subgroups*, Rose-Hulman Undergraduate Research Journal, 2 (2), (2001). 10

[32] T. Takagi, *Zur Theorie des Kreiskörpers*, J. Reine Angew. Math. **157** (1927), 246–255 1

[33] T. Uehara, *On the 4-rank of the narrow ideal class group of a quadratic field*, J. Number Theory **31** (1989), 167–173 1

[34] W.C. Waterhouse, *The normal closures of certain Kummer extensions*, Canad. Math. Bull. **37** (1994), 133–139

Bilkent University, Department of Mathematics, 06800 Bilkent, Ankara, Turkey
*E-mail address*: franz@fen.bilkent.edu.tr