Class Groups of Number Fields: Numerical Heuristics

By H. Cohen and J. Martinet

Dedicated to Dan Shanks on his 70th birthday

Abstract. Extending previous work of H. W. Lenstra, Jr. and the first author, we give quantitative conjectures for the statistical behavior of class groups and class numbers for every type of field of degree less than or equal to four (given the signature and the Galois group of the Galois closure). The theoretical justifications for these conjectures will appear elsewhere, but the agreement with the existing tables is quite good.

1. Introduction and Notations. In [3], H. W. Lenstra, Jr., and the first author developed a method for conjecturing quantitative results on class groups of quadratic fields and cyclic extensions of prime degree. In a forthcoming paper [4] we shall show that this technique can be extended to a much wider class of number fields, and also to relative extensions.

The aim of the present paper is to rapidly make available the numerical conjectures obtained, for people not really interested in our heuristic reasoning or not wanting to wait for [4] to appear. Hence, apart from a total lack of justifications for the conjectures that we present, this paper is essentially self-contained. The plan is as follows.

In the rest of this section we present the notations used in the sequel. Some of them being nonstandard (and in general differing from the notations of [3]), we urge the reader to read the notations carefully before applying the conjectures.

In the next section we present templates for the subsequent conjectures, and then the conjectures themselves, illustrated by numerical examples, first for their own sake, and second as a double check for the reader to understand the templates. These conjectures are given for all types of fields of degree less than or equal to four.

In the final section we comment on the consistency of the conjectures with existing tables (which is quite good).

Combinatorial Notations:

★ If X is a set, |X| denotes its cardinality.

★ For an integer \( p \geq 2 \) and \( \alpha \) an integer or \( \infty \), we set: \((p)_{\alpha} = \prod_{1 \leq k \leq \alpha} (1 - p^{-k})\); in particular \((p)_{\infty} = \prod_{k \geq 1} (1 - p^{-k})\), \((p)_{0} = 1\).

Remark. It would have been more consistent with the usual notations of combinatorics to write this as \((1/p)_{\alpha}\), but the present notation is typographically simpler.
Algebraic Notations:

★ The letter $K$ will stand for the generic algebraic number field whose class group we want to study.

★ $H_K$ (resp. $H_{K/k}$ for relative extensions) will denote the subgroup of the class group consisting of elements whose order is not divisible by the given bad prime or primes (resp. and in the kernel of the norm map from $K$ to $k$).

Warning. $H_K$ does not denote the class group itself, in general.

★ $h_K = |H_K|$, $h_{K/k} = |H_{K/k}|$.

★ The letter $M$ will denote a Galois closure of $K$ over $Q$, and $\Gamma = \text{Gal}(M/Q)$.

★ $A$ will denote a direct product of Dedekind domains $A_i$ (in fact, in our cases, $A$ will either be a direct product of copies of $Z$ or a single Dedekind domain).

★ If $G$ is an $A$-module, $\text{Aut}_A G$ (or simply $\text{Aut} G$) will denote the group of $A$-automorphisms of $G$, and $G_i$ will denote the component of $G$ on the factor $A_i$ of $A$ (hence $G = \prod G_i$).

★ If $\mathfrak{p}$ is a maximal ideal of a Dedekind domain $A$, we will write $r^A_{\mathfrak{p}}(G)$ for the $\mathfrak{p}$-rank of $G$ as an $A$-module, i.e., the dimension of $G/\mathfrak{p}G$ over $A/\mathfrak{p}$. We shall write $r^Z_p(G)$ for the $p$-rank of $G$ when $G$ is viewed only as a $Z$-module. Note that when $A$ is the ring of integers of a quadratic field then

(i) if $p$ splits in $A$, say $pA = \mathfrak{p}\mathfrak{p}'$,

$$r^Z_p(G) = r^A_{\mathfrak{p}}(G) + r^A_{\mathfrak{p}'}(G);$$

(ii) if $p$ is inert in $A$,

$$r^Z_p(G) = 2r^A_p(G).$$

If $A = Z$ we write simply $r_p(G)$ instead of $r^Z_p(G)$.

Analytic Notations:

★ In the templates, the letter $f$ will stand for a “nice” function (not further specified!) defined on isomorphism classes of finite $A$-modules.

★ If $A = \prod_{1 \leq i \leq m} A_i$, where the $A_i$ are Dedekind domains, then the zeta function of $A$ is by definition a function of $m$ complex variables defined by analytic continuation to $C^m$ of the following function:

$$\zeta^A(s) = \prod_{1 \leq i \leq m} \zeta^{A_i}(s_i),$$

where $s = (s_1, \ldots, s_m)$ and $\zeta^{A_i}$ is the Dedekind zeta function of $A_i$ (when it is defined).

Warning. This differs from the usual definition of $\zeta^A$, a function of one complex variable $s$, which one recovers by setting $s_1 = \cdots = s_m = s$.

★ The $Z$ function of $A$ is defined by

$$Z^A(s) = \prod_{k \geq 1} \zeta^A(s + k \cdot 1),$$

where $1 = (1, \ldots, 1)$ is an $m$-dimensional vector.

★ The $Z$ function of $A$ relative to the function $f$ is obtained by analytic continuation of

$$Z^A(f; s) = \sum_G f(G) |\text{Aut}_A G|^{-1} |G_1|^{-s_1} \cdots |G_m|^{-s_m},$$

where the summation is over all $A$-isomorphism classes of finite $A$-modules $G$. 
If 1 is the constant function equal to 1 everywhere, then it is a theorem (not a conjecture!) that

\[ Z^A(1, s) = Z^A(s) \]

(see [3, Corollary 3.7] or [4]), whence the notation.

If \( \ell \) is a prime number which we want to exclude (a “bad” prime), we use \( \xi^A_{\ell}(s) \) and \( Z^A_{\ell}(s) \) to mean that we omit the Euler factors corresponding to prime ideals dividing \( \ell \), and more generally \( Z^A_{\ell}(f; s) \) to mean that in the sum defining \( Z^A(f; s) \) we take only finite \( A \)-modules of order not divisible by \( \ell \).

Finally, we set

\[ M^A(f; s) = Z^A_{\ell}(f; s)/Z^A_{\ell}(s), \]

where it is understood that the limit is taken if both the numerator and denominator vanish.

2. The Conjectures. Let \( K \) be a generic algebraic number field, \( M \) a Galois closure of \( K \), and \( \Gamma = \text{Gal}(M/Q) \) as usual.

For a given \( \Gamma \) we first give a diagram indicating interesting subfields of \( M \) and their interrelations (although usually not the conjugates of \( K \)), then the “bad” prime \( \ell \) (when \([K:Q] \leq 4 \) there is only one such), the ring \( A \), and in the non-Galois case, relations between class groups outside the bad prime as always (these relations being theorems, not conjectures!). We indicate the degrees of the field extensions, except when they are equal to two.

We then consider the set \( \mathcal{C} \) of isomorphism classes of fields \( K \) having given \( \Gamma, r_1, r_2 \) (number of real and complex embeddings of \( K \)). If \( f \) is a function (see notations), we define the average of \( f \) as the following limit, if it exists:

\[ \mathcal{M}(f) = \lim_{X \to \infty} \frac{\sum_{K \in \mathcal{C}, |D_K| < X} f(H_K)/\sum_{K \in \mathcal{C}, |D_K| < X} 1}{\sum_{K \in \mathcal{C}, |D_K| < X} 1}, \]

where \( D_K \) is the discriminant of \( K \). (If we work with relative extensions, replace \( H_K \) by \( H_{K/k} \) in this definition.)

We then give a general heuristic prediction linking \( \mathcal{M}(f) \) to the function \( M^A_{\ell}(f; s) \) defined above, and we specialize this prediction to a number of interesting functions \( f \). In many cases, \( f \) will be the characteristic function of a property \( P \) of \( H_K \) (i.e., 1 if \( P \) is true, 0 if not), and in this case we shall speak of the “probability” that \( P \) holds (written \( \text{pr}(P) \)), although evidently \( \mathcal{M}(f) \) is only finitely additive.

For each of the functions \( f \) we give a few numerical examples, the numbers being rounded to six decimals.

In what follows:

- \( \ell \) will be the bad prime.
- \( H \) will be a finite \( A \)-module of cardinality \( h \).
- \( h \) and \( m \) will denote integers not divisible by \( \ell \).
- \( p \) will denote a good prime, and \( \nu \) a prime ideal of \( A \) dividing \( p \).
We shall give in turn:
(a) \( \text{Pr}(H_K \simeq A) \), \( \text{Pr}(h_K = h) \).
(b) \( \text{Pr}(m \mid h_K) \).
(c) \( \text{Pr}(r^A(H_K) = r) \) and similar quantities.
(d) The average of \( (N_p)^{nr^2(H_K)} \) (\( n \) a positive integer).
(e) The average of \( h_K \).
(f) In a few cases, some additional conjectures.

For relative extensions, we of course replace \( H_K \) and \( h_K \) above by \( H_{K/k} \) and \( h_{K/k} \).

Recall once more that \( H_K \) denotes the class group with its \( \ell \)-component removed.

(1) Quadratic Fields.

\[
\begin{array}{c|c}
K & \Gamma = \mathbb{Z}/2\mathbb{Z} \\
\hline
| & \text{bad prime: } \ell = 2 \\
\end{array}
\]

\( \mathcal{Q} \) \( A = \mathbb{Z} \)

(1.1) Complex quadratic fields.

\( (r_1 = 0, r_2 = 1) \),

\[ \mathcal{M}(f) = M^2_{\mathbb{Z}}(f; 0). \]

(a) \( \text{pr}(H_K \simeq H) = 0, \text{pr}(h_K = h) = 0 \).
(b) \( \text{pr}(m \mid h_K) = \prod_{p \mid \infty} (1 - (p)_\infty/(p)_{a-1}). \)

Examples.

\[
\begin{align*}
m = 3 &: 0.439874; & m = 5 &: 0.239667; \\
m = 7 &: 0.163204; & m = 9 &: 0.159811. \\
\end{align*}
\]

(c) \( \text{pr}(r^A(H_K) = r) = p^{-r}(p)_\infty/(p)_1^2. \)

Examples.

\[
\begin{align*}
p = 3 &: r = 0: 0.560126; & r = 1: 0.420095; \\
r = 2: 0.019692; & r \geq 3: 0.000087; \\
p = 5 &: r = 0: 0.760333; & r = 1: 0.237604; \\
r \geq 2: & 0.002063. \\
\end{align*}
\]

(d) \( \mathcal{M}(p^{nr^2(H_K)^r}) = \sum_{i=0}^{n} p^{-r}(p)_n/(p), (p)_{n-i}. \)

Examples.

\[ n = 1: 2; \quad n = 2: p + 3. \]

(e) \( \mathcal{M}(h_K) = \infty. \)

(1.2) Real quadratic fields.

\( (r_1 = 2, r_2 = 0) \),

\[ \mathcal{M}(f) = M_{\mathbb{Z}}^2(f; 1). \]

(a)

\[
\begin{align*}
\text{pr}(H_K \simeq H) &= (2h(2)_\infty C(\mathbb{Z})|\text{Aut } H|)^{-1}, \\
\text{pr}(h_K = h) &= \left(2h^2(2)_\infty C(\mathbb{Z}) \prod_{p \mid h} (p)_n\right)^{-1}. \\
\end{align*}
\]

Examples.

\[
\begin{align*}
h = 1 &: 0.754458; & h = 3 &: 0.125743; \\
h = 5 &: 0.037723; & h = 7 &: 0.017963; \\
h = 9 &: 0.015718 \left( H = \mathbb{Z}/9\mathbb{Z}: 0.013971; H = (\mathbb{Z}/3\mathbb{Z})^2: 0.001746 \right). \\
\end{align*}
\]
(b) \( \text{pr}(m | h_K) = \prod_p \theta_{m}(1 - ((p) \infty/(p)_1) \sum_{0 < \beta \leq m} (p^{2\beta}(p)_\beta)^{-1}). \)

Examples.

\[
\begin{align*}
  m = 3: & \quad 0.159811; \\
  m = 5: & \quad 0.049584; \\
  m = 7: & \quad 0.023739; \\
  m = 9: & \quad 0.019779.
\end{align*}
\]

(c) \( \text{pr}(r_p(H_K) = r) = p^{-(r+1)}((p)_\infty/(p)_r), \)

Examples.

\[
\begin{align*}
  p = 3: & \quad r = 0: 0.840189; \quad r = 1: 0.157535; \\
  & \quad r \geq 2: 0.002275; \\
  p = 5: & \quad r = 0: 0.950416; \quad r = 1: 0.049501; \\
  & \quad r \geq 2: 0.000083.
\end{align*}
\]

(d) \( \mathcal{M}(p^{n r_{r}(H_K)}) = \sum_{i=0}^{n} p^{(n-i-1)}((p)_n,((p)_r),((p)_{n-1})). \)

Examples.

\[
\begin{align*}
  n = 1: & \quad 1 + p^{-1}; \quad n = 2: 2 + p^{-1} + p^{-2}.
\end{align*}
\]

(e) \( \mathcal{M}(H_K) = \infty. \)

(f) (Also conjectured by C. Hooley [11])

\[
\sum_{p \leq x} h_{Q(\sqrt{p})} \sim \frac{x}{8} \text{ as } x \to \infty.
\]

(2) **Cyclic Cubic Fields.**

\[
\begin{align*}
  K = \mathbb{Z}/3\mathbb{Z} \\
  \Gamma = \mathbb{Z}/3\mathbb{Z} \\
  3 \mid \text{bad prime: } \ell = 3 \\
  Q & \quad A = \mathbb{Z}[j] \quad (j = e^{2i\pi/3})
\end{align*}
\]

\( K \) is totally real \( (r_1 = 3, r_2 = 0), \)

\( \mathcal{M}(f) = M_A^3(f; 1). \)

(a) \[ \text{pr}(H_K = \Lambda H) = \left( \frac{9\sqrt{3}}{2\pi} h(3)_\infty C(A)|\text{Aut}_A H| \right)^{-1}. \]

\[ \text{pr}(h_K = h) = \left( \frac{9\sqrt{3}}{2\pi} h^2(3)_\infty C(A) \right)^{-1} \sum_{N_{a} = h} \prod_{\nu^* | a} (N\nu)^{-1}. \]

Here, \( \alpha \) runs through all integral ideals of \( A \) of norm \( h \), and \( \nu \) through prime ideals dividing \( a \).

Examples.

\[
\begin{align*}
  h = 1: & \quad 0.850072; \quad h = 4: 0.070839 \text{ (here } H = z (\mathbb{Z}/2\mathbb{Z})^2); \\
  h = 7: & \quad 0.040480 \text{ (50\% for each of the two } A\text{-isomorphism classes);} \\
  h = 13: & \quad 0.010898 \text{ (50\% for each of the two } A\text{-isomorphism classes);} \\
  h = 16: & \quad 0.004723 \quad (H = z (\mathbb{Z}/4\mathbb{Z})^2; 0.004427; H = z (\mathbb{Z}/2\mathbb{Z})^4: 0.000295). \]
\]
(b) \( p(m | H_K) = P_1 P_2 \), where
\[
P_1 = \prod_{p \equiv 1 \pmod{3}}^\infty \left( 1 - \left( \frac{p}{1} \right) \sum_{0 \leq \beta + \gamma < \alpha} \left( \frac{p^{2\beta + 2\gamma}}{(p)^{\beta}(p)^{\gamma}} \right)^{-1} \right).
\]
\[
P_2 = \prod_{p \equiv 2 \pmod{3}}^\infty \left( 1 - \left( \frac{p^2}{1} \right) \sum_{0 \leq \beta < \alpha/2} \left( \frac{p^{4\beta}}{(p^2)^{\beta}} \right)^{-1} \right).
\]

Examples.
- \( m = 2 \) and \( m = 4 \): 0.081950
- \( m = 5 \): 0.001667
- \( m = 7 \): 0.046914
- \( m = 8 \) and \( m = 16 \): 0.005446

(c) \( \text{pr}(r^A(H_K) = r) = (N_{p'})^{-t(r+1)}(N_{p'})_{\infty}/((N_{p'})_r(N_{p'})_{r+1}) \).

If \( p \equiv 1 \pmod{3} \), then
\[
\text{pr}(r^Z(H_K) = r) = (p^2)_{\infty} \sum_{t + u = r} p^{-t(t+1) - u(u+1)/((p),(p))_{t+1}(p)_u(p)_{u+1}}.
\]

If \( p \equiv 2 \pmod{3} \), then
\[
\text{pr}(r^Z(H_K) = r) = \begin{cases} 
0 & \text{if } r \text{ is odd}, \\
(p^2)_{\infty} / ((p^2)_{r/2}(p^2)_{(r/2)+1}) & \text{otherwise}.
\end{cases}
\]

Examples.
- \( p = 2, r = 0 \): 0.918050
- \( r \geq 4 \): 0.000346
- \( p = 5, r = 0 \): 0.998333
- \( r \geq 2 \): 0.001667
- \( p = 7, r = 0 \): 0.953086
- \( r \geq 2 \): 0.046331
- \( r \geq 2 \): 0.000583

(d) If \( p \equiv 1 \pmod{3} \) then
\[
\mathcal{M}(p^{nr^A(H_K)}) = \sum_{i=0}^n p^{i(n-i-1)}(p)_n / ((p),(p))_{n-i},
\]
\[
\mathcal{M}(p^{nr^Z(H_K)}) = \left( \mathcal{M}(p^{nr^A(H_K)}) \right)^2.
\]

Examples.
- \( n = 1 \): \((1 + p^{-1})^2\)
- \( n = 2 \): \((2 + p^{-1} + p^{-2})^2\)

If \( p \equiv 2 \pmod{3} \) then
\[
\mathcal{M}(p^{2nr^A(H_K)}) = \mathcal{M}(p^{nr^Z(H_K)}) = \sum_{i=0}^n p^{2i(n-i-1)}(p^2)_n / ((p^2),(p^2))_{n-i},
\]

Examples.
- \( n = 1 \): \(1 + p^{-2}\)
- \( n = 2 \): \(2 + p^{-2} + p^{-4}\)

(e) \( \mathcal{M}(h_K) = \infty \).

(3) Non-Galois Cubic Fields.

\[
\begin{array}{ccc}
K & \xrightarrow{3} & M \\
\Gamma = \mathbb{S}_3 & & \\
\text{bad prime: } \ell = 3 & & \\
A = \mathbb{Z} & & \\
H_{M/k} = H_K \times H_K & & \\
\end{array}
\]
(3.1) Complex cubic fields.

\[(r_1 = 1, \ r_2 = 1),\]

\[M(f) = M_{i,3}(f; 1).\]

(a) \[\text{pr}(H_K \approx H) = \left( \frac{3}{2} h(3)_{\infty} C(\mathbb{Z}) | \text{Aut } H \right)^{-1},\]

\[\text{pr}(h_K = h) = \left( \frac{3}{2} h^2(3)_{\infty} C(\mathbb{Z}) \prod_{\mathfrak{p} | h} (p)_{\alpha} \right)^{-1}.\]

Examples.

- \(h = 1: 0.518642;\) \(h = 2: 0.259321;\)
- \(h = 4: 0.086440 (H \approx \mathbb{Z}/4\mathbb{Z}: 0.064830; H \approx (\mathbb{Z}/2\mathbb{Z})^2: 0.021610);\)
- \(h = 5: 0.025932.\)

(b) \[\text{pr}(m | H_K) = \prod_{\mathfrak{p} | m} (1 - ((p)_{\infty}/(p)_1) \sum_{0 < \beta < \alpha} (p^{2\beta}(p)_\beta)^{-1}).\]

Examples.

- \(m = 2: 0.422424;\) \(m = 4: 0.133636;\)
- \(m = 5: 0.049584;\) \(m = 7: 0.023739.\)

(c) \[\text{pr}(r_p(H_K) = r) = p^{-r(r+1)}(p)_{\infty}/((p), (p), r+1).\]

Examples.

- \(p = 2: r = 0: 0.577576;\) \(r = 1: 0.385051;\)
- \(r = 2: 0.036672;\) \(r \geq 3: 0.000702.\)

For \(p \geq 5\) see 1.2(c).

(d), (e) See 1.2(d) and 1.2(e).

(3.2) Totally real non-Galois cubic fields.

\[(r_1 = 3, \ r_2 = 0),\]

\[M(f) = M_{i,3}(f; 2).\]

(a) \[\text{pr}(H_K \approx H) = \left( \frac{81}{8\pi^2} h^2(3)_{\infty} C(\mathbb{Z}) | \text{Aut } H \right)^{-1},\]

\[\text{pr}(h_K = h) = \left( \frac{81}{8\pi^2} h^3(3)_{\infty} C(\mathbb{Z}) \prod_{\mathfrak{p} | m} (p)_{\alpha} \right)^{-1}.\]

Examples.

- \(h = 1: 0.758339;\) \(h = 2: 0.189585;\)
- \(h = 4: 0.031597 (H \approx \mathbb{Z}/4\mathbb{Z}: 0.023698; H \approx (\mathbb{Z}/2\mathbb{Z})^2: 0.007899).\)

(b) \[\text{pr}(m | H_K) = \prod_{\mathfrak{p} | m} (1 - ((p)_{\infty}/(p)_2)\sum_{0 < \beta < \alpha} (p^{3\beta}(p)_\beta)^{-1}).\]

Examples.

- \(m = 2: 0.229898;\) \(m = 4: 0.037373;\)
- \(m = 5: 0.009983;\) \(m = 7: 0.003400.\)

(c) \[\text{pr}(r_p(H_K) = r) = p^{-r(r+2)}(p)_{\infty}/((p), (p), r+2).\]

Examples.

- \(p = 2: r = 0: 0.770102;\) \(r = 1: 0.220029;\)
- \(r = 2: 0.009779;\) \(r \geq 3: 0.000090.\)
- \(p = 5: r = 0: 0.990017;\) \(r = 1: 0.009980;\)
- \(r \geq 2: 3.3 \times 10^{-6}.\)
(d) $\mathcal{M}(p^{nt}(H_k)) = \sum_{i=0}^{n} p^{i(n+i-2)} \frac{(p)}{((p),(p)_{n-i})}$.

Examples.

$n = 1: 1 + p^{-2}; \quad n = 2: 1 + p^{-1} + p^{-2} + p^{-4}$.

(e) $\mathcal{M}(h_K) = 4\pi^2/27 = 1.462164$.

(4) Cyclic Quartic Fields.

$K \quad \Gamma = \mathbb{Z}/4\mathbb{Z}$

bad prime: $\ell = 2$

$k \quad H_K = H_k \times H_{K/k}$

$Q \quad A = \mathbb{Z}[i]$ hence only $H_{K/k}$ is interesting

(4.1) Totally complex cyclic quartic fields.

$(r_1 = 0, r_2 = 2)$.

Here, $k$ is real quadratic.

$\mathcal{M}(f) = M_{A_{2}}^{A}(f; 0)$

Remark. If one wants the full class group $H_K$, then the template is

$\mathcal{M}(f) = M_{A_{2}}^{B}(f; 1, 0)$,

where $B = \mathbb{Z} \times \mathbb{Z}[i]$.

(a) $pr(H_{K/k} = A H) = 0, pr(h_{K/k} = h) = 0$.

(b) $pr(m | h_{K/k}) = P_1 P_3$, where

$$P_1 = \prod_{p \equiv 1 (mod 4)} \left(1 - (p)_{\infty}^2 \sum_{0 < \beta + \gamma < \alpha} (p^{\beta + \gamma}(p)_{\beta}(p)_{\gamma})^{-1}\right),$$

$$P_3 = \prod_{p \equiv 3 (mod 4)} \left(1 - (p^2)_{\infty}/((p^2)_{((a-1)/2)})\right).$$

Examples.

$m = 3$: 0.123440; $m = 5$: 0.421894;

$m = 7$: 0.020825; $m = 9$: 0.123440;

$m = 11$: 0.008333; $m = 13$: 0.158813.

(c) $pr(r_{p}^{A}(H_{K/k}) = r) = (Np)^{-r}((Np)_{\infty}/(Np)^{2})_{r}$. If $p \equiv 1 (mod 4)$, then

$$pr(r_{p}^{Z}(H_{K/k}) = r) = (p)_{\infty}^2 \sum_{t+u=r} p^{-t^2-u^2}/((p)_{t}(p)_{u}^2).$$

If $p \equiv 3 (mod 4)$, then

$$pr(r_{p}^{Z}(H_{K/k}) = r) = \begin{cases} 0 & \text{if } r \text{ is odd}, \\ p^{-r^2/2}((p^2)_{\infty}/(p^2)^{2r^2/2}) & \text{otherwise}. \end{cases}$$

Examples.

$p = 3$: $r = 0$: 0.876560; $r = 2$: 0.123266;

$r \geq 4$: 0.000173;

$p = 5$: $r = 0$: 0.578106; $r = 1$: 0.361316;

$r = 2$: 0.059592; $r \geq 3$: 0.000986.
(d) If \( p \equiv 1 \pmod{4} \), then

\[
\mathcal{M}(p^{nr_0^k(K_{K/k}))} = \sum_{i=0}^{n} p^{i(n-i)}(p)_n / ((p)_i(p)_{n-i})
\]

\[
\mathcal{M}(p^{nr_2^k(K_{K/k}))} = \left( \mathcal{M}(p^{nr_0^k(K_{K/k}))} \right)^2
\]

**Examples.**

\( n = 1; 4; \quad n = 2; (p + 3)^2 \).

If \( p \equiv 3 \pmod{4} \), then

\[
\mathcal{M}(p^{2nr_2^k(K_{K/k}))} = \mathcal{M}(p^{nr_2^k(K_{K/k}))} = \sum_{i=0}^{n} p^{2i(n-i)}(p^2)_n / ((p^2)_i(p^2)_{n-i})
\]

**Examples.**

\( n = 1; 2; \quad n = 2; p^2 + 3 \).

(e) \( \mathcal{M}(h_{K/k}) = \infty \).

(4.2) Totally real cyclic quartic fields.

\( (r_1 = 4, r_2 = 0) \),

\[
\mathcal{M}(f) = M_4^*(f; 1).
\]

**Remark.** For the full class group \( H_K \),

\[
\mathcal{M}(f) = M_2^A(f; 2, 1).
\]

where \( B = \mathbb{Z} \times \mathbb{Z}[i] \).

(a)

\[
\text{pr}(H_{K/k} = A H) = \left( \frac{8}{\pi} h(2)_A C(A) | \text{Aut}_A H \right)^{-1},
\]

\[
\text{pr}(h_{K/k} = h) = \left( \frac{8}{\pi} h^2(2)_A C(A) \right)^{-1} \sum_{N_\alpha = h} \prod_{\nu | \alpha} (N_\nu)^{-1}.
\]

Here, \( \alpha \) runs through all integral ideals of \( A \) of norm \( h \), and \( \nu \) through prime ideals dividing \( \alpha \).

**Examples.**

\( h = 1: \quad 0.864608 \);

\( h = 5: \quad 0.086461 \) (50% for each of the two \( A \)-isomorphism classes);

\( h = 9: \quad 0.012008 \) (here, \( H = \mathbb{Z}/3\mathbb{Z}^2 \));

\( h = 13: \quad 0.011085 \) (50% for each of the two \( A \)-isomorphism classes).

(b) \( \text{pr}(m | h_{K/k}) = P_1 P_3 \), where

\[
P_1 = \prod_{p = 1 \pmod{4}} (1 - ((p)_\infty/(p)_1) \sum_{0 \leq \beta + \gamma \leq \alpha} (p^{2\beta + 2\gamma}(p)_\beta(p)_\gamma)^{-1}).
\]

\[
P_3 = \prod_{p = 3 \pmod{4}} (1 - ((p^2)_\infty/(p^2)_1) \sum_{0 \leq \beta \leq \alpha/2} (p^{4\beta}(p^2)_\beta)^{-1}).
\]
Examples.

\[
m = 3: 0.013870; \quad m = 5: 0.096709;
\]
\[
m = 7: 0.000425; \quad m = 9: 0.013870;
\]
\[
m = 11: 0.000069; \quad m = 13: 0.012774.
\]

(c) \(\text{pr}(r^A(H_{K/k}) = r) = (N\nu)^{-r(r+1)}(N\nu)_{x_t}/(N\nu)_r(N\nu)_{r+1} \).

If \( p \equiv 1 \pmod{4} \), then
\[
\text{pr}(r_p^Z(H_{K/k}) = r) = (p)^{2}_x \sum_{t-u=r} p^{-r(r+1)-u(u+1)/((p),(p))_{t}}(p)^{u}_{u+1}.
\]

If \( p \equiv 3 \pmod{4} \), then
\[
\text{pr}(r_p^Z(H_{K/k}) = r) = \begin{cases} 0 & \text{if } r \text{ is odd}, \\ p^{-r(r+2)/2}(p)^{2}_x/((p^2)_{r/2}(p^2)_{r/2+1}) & \text{otherwise.} \end{cases}
\]

Examples.

\[
p=3: r = 0: 0.986130; \quad r = 2: 0.013867;
\]
\[
r \geq 4: 2.1 \times 10^{-6};
\]
\[
p=5: r = 0: 0.903291; \quad r = 1: 0.094093;
\]
\[
r \geq 2: 0.002617.
\]

(d) If \( p \equiv 1 \pmod{4} \), then
\[
\mathcal{M}(p^{n_r(H_{K/k})}) = \sum_{i=0}^{n} p^{i(n-i-1)}(p)^{(p),(p)}_{n-i},
\]
\[
\mathcal{M}(p^{n_rZ(H_{K/k})}) = \left(\mathcal{M}(p^{n_r(H_{K/k})})\right)^2.
\]

Examples.

\[
n = 1: (1 + p^{-1})^2; \quad n = 2: (2 + p^{-1} + p^{-2})^2.
\]

If \( p \equiv 3 \pmod{4} \), then
\[
\mathcal{M}(p^{2n_r(H_{K/k})}) = \mathcal{M}(p^{nrZ(H_{K/k})}) = \sum_{i=0}^{n} p^{2i(n-i-1)}(p^2)^{(p^2),(p^2)}_{n-i}.
\]

Examples.

\[
n = 1: 1 + p^{-2}; \quad n = 2: 2 + p^{-2} + p^{-4}.
\]

(e) \(\mathcal{M}(h_{K/k}) = \infty\).

(5) Bicyclic Fields.

\[
\Gamma = (\mathbb{Z}/2\mathbb{Z})^2
\]
\[
\text{bad prime: } \ell = 2
\]
\[
H_K = H_{k_1} \times H_{k_2} \times H_{k_3}
\]

Our heuristics predict that these three groups behave independently, hence the desired conjectures for \( H_K \) or \( H_{K/k_1} = H_{k_1} \times H_{k_2} \) can easily be deduced from the conjectures in the quadratic case. For the sake of completeness we give the templates.
For $H_K$ we take $A = \mathbb{Z}^3$.
For $H_{K/k}$, we take $A = \mathbb{Z}^2$.

(5.1) Totally complex bicyclic fields.

$(r_1 = 0, r_2 = 2)$.

For $H_K (A = \mathbb{Z}^3): \mathcal{M}(f) = M_{a_2}(f; 0, 0, 1)$.
For $H_{K/k}, (A = \mathbb{Z}^2)$
if $k_3$ is complex: $\mathcal{M}(f) = M_{a_2}(f; 0, 1)$.
if $k_3$ is real: $\mathcal{M}(f) = M_{a_2}(f; 0, 0)$.

(5.2) Totally real bicyclic fields.

$(r_1 = 4, r_2 = 0)$.

For $H_K (A = \mathbb{Z}^3): \mathcal{M}(f) = M_{a_2}(f; 1, 1, 1)$.
For $H_{K/k}, (A = \mathbb{Z}^2): \mathcal{M}(f) = M_{a_2}(f; 1, 1)$ (here $k_3$ is real).

(6) Dihedral Quartic Fields.

$\Gamma = D_8$
bad prime: $\ell = 2$

Note. In this diagram Gal$(M/k_0) = \mathbb{Z}/4\mathbb{Z}$,
while Gal$(M/k) = Gal(M/k') = (\mathbb{Z}/2\mathbb{Z})^2$.
Only the relative class group $H_{K/k}$ is interesting, and we have
$H_{M/E} \simeq H_{K/k} \times H_{K/k}$ and $H_{K'/k'} \simeq H_{K/k}$.

$(a)$

$\text{pr}(H_{K/k} \simeq H) = \left( \frac{16}{\pi^2} h^2(2)^{\infty} C(\mathbb{Z}) \left| \text{Aut } H \right| \right)^{-1}$,
$\text{pr}(h_{K/k} = h) = \left( \frac{16}{\pi^2} h^3(2)^{\infty} C(\mathbb{Z}) \prod_{p \mid h}(p)^a \right)^{-1}$. 
Examples.

\[ h = 1: 0.930775; \quad h = 3: 0.051710; \]
\[ h = 5: 0.009308; \quad h = 7: 0.003166; \]
\[ h = 9: 0.002155 \left( H = \mathbb{Z}/9\mathbb{Z}: 0.001915; \right) (\mathbb{Z}/3\mathbb{Z})^2: 0.000239. \]

(b) \( \Pr(m | h_{K/k}) = \prod_{\psi | m} \left( 1 - \frac{((p)_\infty/(p)_2) \sum_{\beta < a} (p^{3\beta} (p)_\beta)^{-1})}{\psi} \right) \).

Examples.

\[ m = 3: 0.054787; \quad m = 5: 0.009983; \]
\[ m = 7: 0.003400; \quad m = 9: 0.002275. \]

(c) \( \Pr(r_p(H_{K/k}) = r) = p^{-r(r+2)}((p)_\infty/(p)_r(p)_{r+2}). \)

Examples.

\[ p = 3: r = 0: 0.945213; \quad r = 1: 0.054532; \]
\[ p = 5: r = 0: 0.990017; \quad r = 1: 0.009980; \]
\[ r \geq 2: 3.3 \times 10^{-6}. \]

(d) \( \mathcal{M} \left( p^{n} r_p(h_{K/k}) \right) = \sum_{i=0}^{n} p^{i(n-i-2)}((p)_n/(p)_r(p)_{n-i}). \)

Examples.

\[ n = 1: 1 + p^{-2}; \quad n = 2: 1 + p^{-1} + p^{-2} + p^{-4}. \]

(e) \( \mathcal{M}(h_{K/k}) = \pi^2/8 = 1.233701. \)

Remark. The conjectures that we obtain in the case \( D_8 \) are, as expected, the same as the ones that we would obtain for quadratic extensions of a fixed quadratic field \( k \) (such an extension being of type \( D_8 \) with probability 1).

7. Quartic Fields of Type \( A_4 \).

\[ \Gamma = A_4 \]
\[ \text{bad prime: } \ell = 2 \]
\[ H_{M/C} = H_K \times H_K \times H_K \left( H_K = H_{L_2}/C \right) \]
\[ A = \mathbb{Z} \]

7.1 Totally complex quartic fields of type \( A_4 \).

\( (r_1 = 0, r_2 = 2), \)
\( \mathcal{M}(f) = M_{Z_2}(f;1). \)

For specific \( f \) and examples, see (1.2) (real quadratic fields).

7.2 Complex quartic fields of type \( A_4 \) of mixed signature.

\( (r_1 = 2, r_2 = 1). \)

These fields to not exist!

7.3 Totally real quartic fields of type \( A_4 \).

\( (r_1 = 4, r_2 = 0), \)
\( \mathcal{M}(f) = M_{Z_2}(f;3). \)
(a) \[ \text{pr}(H_K = H) = \left( \frac{128}{7\pi^2 \xi(3)} h^3(2) \infty C(\mathbb{Z}) | \text{Aut } H \right)^{-1}, \]
\[ \text{pr}(h_K = h) = \left( \frac{128}{7\pi^2 \xi(3)} h^4(2) \infty C(\mathbb{Z}) \prod_{p^s | m} (p) \right)^{-1}. \]

Examples.
\[ h = 1: 0.978989; \quad h = 3: 0.018129; \]
\[ h = 5: 0.001958; \quad h = 7: 0.000476; \]
\[ h = 9: 0.000252 \left( H = \mathbb{Z}/9\mathbb{Z}: 0.000224; H = (\mathbb{Z}/3\mathbb{Z})^2: 0.000028 \right). \]

(b) \[ \text{pr}(m | h_K) = \prod p^s | m \left( 1 - \frac{(p \infty)(p)^{3} \log \frac{p}{(p)(p)}}{(p)^{3}} \right)^{-1}. \]
Examples.
\[ m = 3: 0.018433; \quad m = 5: 0.001999; \]
\[ m = 7: 0.000486; \quad m = 9: 0.000256. \]

(c) \[ \text{pr}(r_p(H_K) = r) = p^{-r(r+3)}(p \infty)(p, (p)^{r+3}). \]
Examples.
\[ p = 3: r = 0: 0.981567; \quad r = 1: 0.018404; \]
\[ r \geq 2: 0.000029; \]
\[ p = 5: r = 0: 0.998001; \quad r = 1: 0.001999. \]

(d) \[ \mathcal{M} \left( p^{n_r}(H_K^1) \right) = \sum_{i=0}^{n} p^{(n-i-3)}(p, (p)^{(n-i)}(p_n - i). \]
Examples.
\[ n = 1: 1 + p^{-3}; \quad n = 2: 1 + p^{-2} + p^{-3} + p^{-6}. \]

(e) \[ \mathcal{M}(h_K) = \frac{4}{\zeta(3)} = 1.051800. \]
(f) \[ \mathcal{M}(h_K^2) = \frac{4}{\zeta(3)} \pi^2 \xi(3) = 1.297606. \]

(8) Quartic Fields of Type $S_4$.

(8.1) Totally complex quartic fields of type $S_4$.
\[ (r_1 = 0, r_2 = 2), \]
\[ \mathcal{M}(f) = M_{x_2}(f; 1). \]

For specific $f$ and examples, see (1.2) (real quadratic fields).

(8.2) Quartic fields of type $S_4$ and mixed signature.
\[ (r_1 = 2, r_2 = 1), \]
\[ \mathcal{M}(f) = M_{x_2}(f; 2). \]
For specific $f$ and examples, see (6.4) (totally real dihedral quartic fields).

(8.3) **Totally real quartic fields of type $S_4$:**

\[ (r_1 = 4, r_2 = 0). \]

\[ \mathcal{M}(f) = M_{S_4}^2(f; 3). \]

For specific $f$ and examples, see (7.3) (totally real quartics of type $A_4$).

3. **Discussion.** The tables that we have at our disposal (some of which having been extended specifically to test our conjectures) are as follows:

- Complex quadratic fields, $|D_K| \leq 2.5 \times 10^7$ [2].
- Real quadratic fields $\mathbb{Q}(\sqrt{p})$ with $p$ prime, $p \leq 10^8$ [15].
- Cyclic cubic fields, $D_K \leq 2.56 \times 10^8$ ([9], [8]).
- Noncyclic complex cubic fields, $|D_K| \leq 2 \times 10^4$ [1].
- Pure cubic fields $\mathbb{Q}(\sqrt[3]{p})$ with $p$ prime, $p \leq 10^6$ ([13], [15]).
- Noncyclic totally real cubic fields, $|D_K| \leq 5 \times 10^5$ [7].
- Some tables for fields of degree 4 and 6, which are not sufficiently extensive to make any significant statistics ([10], [12], [6]). In addition, C. P. Schnorr [14] kindly computed for us a few samples for $|D_K| \approx 5 \times 10^8$ for complex quadratic fields.

The first observation is that for imaginary and real quadratic fields, and for cyclic cubics, the agreement with the tables is very good.

The second observation is that for noncyclic complex cubic fields, the agreement is not so good. Now in the non-Galois cubic case, as will be explained in [4], we have every reason to believe that the prime 2 behaves like a good prime. The poor agreement with the tables would seem to indicate that, either our whole strategy in the non-Galois case is wrong, or at least that 2 should be considered also a bad prime. However, the discriminants involved in the table of [1] are not very large. If we look at the subtable of pure cubic fields, the discriminant of $\mathbb{Q}(\sqrt[3]{p})$ is $3p^2$ or $27p^2$, according as $p \equiv \pm 1 \pmod{9}$ or not, hence in the table of [15] the discriminants go up to more than $3 \times 10^{12}$. If we assume that, as a whole, pure cubics behave like any other complex cubics, then ordering them as usual by discriminants (and not by $p$) we find very good agreement with the tables. Thus we believe that the poor agreement with [1] is due to the fact that the discriminants are not sufficiently large.

However, there is another phenomenon which has been stressed several times ([13], [15]) and which we repeat here: If one considers only $\mathbb{Q}(\sqrt[3]{p})$ with $p \equiv 2 \pmod{3}$ prime (so as not to be bothered by the 3-part), and if one distinguishes between $p \equiv -1 \pmod{9}$ and $p \equiv 2, 5 \pmod{9}$, one notes a marked distinction in the behavior of the class group. For example, class number 1 seems to occur with probability 0.60 for $p \equiv -1 \pmod{9}$, but with probability 0.40 for $p \equiv 2, 5 \pmod{9}$. This is apparently due to the higher 2-part of the class group in the second case, and although a sort of reinterpretation of this phenomenon has been given in [5], no satisfactory heuristic explanation has yet been found.

Since $D_K \leq x$ is equivalent to $p \leq \sqrt{3x/\sqrt[3]{p}}$ for $p \equiv -1 \pmod{9}$ and $p \leq \sqrt{27x/27}$ for $p \equiv 2, 5 \pmod{9}$, by taking together all the $\mathbb{Q}(\sqrt[3]{p})$ with $p \equiv 2 \pmod{3}$ and discrimini-
nant \( \leq x \), we find an approximate probability of
\[
\frac{1}{2} \times 0.60 + \frac{3}{4} \times 0.40 = 0.52
\]
of having class number 1, very close to the predicted probability 0.5186.
A similar remark can be made about quartic extensions of type \( A_4 \) and \( S_4 \): The prime 3 could be bad. However, we think that this is not the case.

**Acknowledgments.** We are very grateful to D. A. Buell, H. C. Williams and D. Shanks for computing for us, or making available to us, tables which we used to check the validity of our conjectures. It is also a pleasure to thank G. Henniart, H. W. Lenstra, Jr., and J. Oesterlé for very fruitful discussions.

U.A. au C.N.R.S. No. 040226
U.E.R. de Mathématique et Informatique
Université de Bordeaux 1
351, cours de la Libération
F-33405 Talence, Cedex, France

14. C. P. Schnorr, Personal communication.