TABLES OF UNIT GROUPS AND CLASS GROUPS OF QUINTIC FIELDS AND A REGULATOR BOUND

M. POHST AND K. WILDANGER

ABSTRACT. Using a new regulator bound we determine unit groups and class groups of the 289040 quintic algebraic number fields with absolute discriminant less than 2×10^7 (totally real fields), respectively 5×10^6 (other signatures). We list significant data.

1. INTRODUCTION

In [5] a table of all quintic number fields with absolute discriminant less than 2×10^7 (totally real fields), respectively 5×10^6 (other signatures) was presented. In this paper the unit groups and the class groups of these fields are determined. Because of an error in [4] we also develop a new lower bound for regulators.

2. UNIT GROUPS, CLASS GROUPS AND A REGULATOR BOUND

The unit groups and class groups of algebraic number fields F are nowadays computed jointly by producing sufficiently many *relations*, i.e. integers α of F which generate principal ideals which factor over a given factor basis of prime ideals [1], [3]. If we do not assume GRH, then a lower regulator bound is required to guarantee the correctness of the obtained result. Such a bound is given in [4, Theorem (6.17) and Corollary (6.19)]. However, recently H. Cohen showed that (6.17) is e.g. not correct for $n > 2$ by producing a counterexample. Hence, we use the opportunity to correct that theorem.

Let R be an order of the algebraic number field F of degree $n \geq 3$ under consideration. Let $F = F^{(1)}, \ldots, F^{(n)}$ be the conjugates of F and define

$$T_2 : F \to \mathbb{R}^{\geq 0} : \alpha \mapsto \sum_{j=1}^{n} |\alpha^{(j)}|^2.$$

Clearly, $T_2(\alpha) \geq n$ for $\alpha \in R \backslash \{0\}$ and $T_2(\alpha) = n$ if and only if α is a torsion unit of R. Every element $\varepsilon \in U(R)$ (the unit group of R), which is not a root of unity, therefore satisfies $T_2(\varepsilon) > n$. For units $\varepsilon \in U(R)$ satisfying $T_2(\varepsilon) \geq K$, $T_2(\varepsilon^{-1}) \geq K$ for some $K > n$ we obtain a lower bound for $\sum_{j=1}^{n} (\log |\varepsilon^{(j)}|)^2$ as follows.

We set $x_j := \log |\varepsilon^{(j)}|$ $(1 \leq j \leq n)$ and minimize

$$f(\mathbf{x}) := \sum_{j=1}^{n} x_j^2$$

under suitable side conditions.

Lemma. *The function*

$$f(\mathbf{x}) = \sum_{j=1}^{n} x_j^2$$

has a global minimum at a point $\mathbf{y}$ *of the set*

$$S = \left\{ \mathbf{x} \in \mathbb{R}^n \ \Big| \ \sum_{j=1}^{n} x_j = 0, \ \sum_{j=1}^{n} e^{2x_j} \geq K, \ \sum_{j=1}^{n} e^{-2x_j} \geq K \right\}$$

with at most three different coordinates.

Proof. The existence of a global minimum is obvious. Because of $K > n$ we have $\mathbf{0} \notin S$. If we assume that one of the conditions

$$\sum_{j=1}^{n} e^{2x_j} \geq K, \quad \sum_{j=1}^{n} e^{-2x_j} \geq K$$

is not active, i.e. $>$ holds, then the problem is reduced to the one of (6.17) in [4]. We obtain a minimum at a point $\mathbf{y}$ with at most two different coordinates.

Finally, we assume that equality holds in both cases. Since we want to apply Lagrange multipliers, we need to show that the rank of the matrix

$$A(\mathbf{x}) = \begin{pmatrix} 1 & \cdots & 1 \\ 2e^{2x_1} & \cdots & 2e^{2x_n} \\ -2e^{-2x_1} & \cdots & -2e^{-2x_n} \end{pmatrix}$$

is three for $\mathbf{x} = \mathbf{y}$. Because of $\sum_{j=1}^{n} x_j = 0$ and $\mathbf{x} \neq \mathbf{0}$ any $\mathbf{x} \in S$ must have positive and negative coordinates, hence the rows 1 and 2 of $A(\mathbf{x})$ are independent. Let us assume that the third row of $A(\mathbf{x})$ is linearly dependent from the first and the second. This implies that $\mathbf{x}$ has exactly two different coordinates. We again obtain the solution of [4] in this case.

Finally, we need to consider local minima for which the rank of $A(\mathbf{x})$ is three. As we saw above this is tantamount to $\mathbf{x}$ having at least three different coordinates. Applying Lagrange multipliers to the function

$$F(\mathbf{x}) := f(\mathbf{x}) + \lambda \sum_{j=1}^{n} x_j + \mu \left(\sum_{j=1}^{n} e^{2x_j} - K \right) + \nu \left(\sum_{j=1}^{n} e^{-2x_j} - K \right)$$

we obtain for a local minimum in $\mathbf{x} \in S$ the system of equations

$$2x_j + \lambda + 2\mu e^{2x_j} - 2\nu e^{-2x_j} = 0.$$

If we fix the triple (λ, μ, ν) we must show that the function

$$g(x) := 2x + \lambda + 2\mu e^{2x} - 2\nu e^{-2x}$$

has at most three zeros. The corresponding derivative is

$$g'(x) = 2 + 4\mu e^{2x} + 4\nu e^{-2x}.$$

Obviously, $g'(x)$ has at most two zeros. Therefore $g(x)$ has at most two extremal values and consequently at most three zeros. $\qquad \square$

For a computation of the global minimum of $f(\mathbf{x})$ on S we therefore need to look only at the elements $\mathbf{x}$ of S with at most three different coordinates. As we already pointed out, the premise $K > n$ guarantees that any $\mathbf{x} \in S$ has at least two different coordinates, a positive and a negative one. The extremal values at points with exactly two different coordinates are obtained in [4]. They need to be compared with the ones which we obtain in the sequel.

Let x, y, z be the three different coordinates of an element $\mathbf{x} \in S$. Let us assume that their frequencies in $\mathbf{x}$ are $n_1, n_2, n_3 \in \mathbb{N}$ subject to $n_1 \geq n_2 \geq n_3$ and $n_1 + n_2 + n_3 = n$. For a fixed triple (n_1, n_2, n_3) the potential minima $\mathbf{x} \in S$ can be calculated from the three equations

$$
\begin{aligned}
n_1 x + n_2 y + n_3 z &= 0, \\
n_1 e^{2x} + n_2 e^{2y} + n_3 e^{2z} &= K, \\
n_1 e^{-2x} + n_2 e^{-2y} + n_3 e^{-2z} &= K.
\end{aligned}
$$

This is not at all difficult since we can transform these equations into a pair of algebraic equations. We set

$$
z = -\frac{n_1 x + n_2 y}{n_3}, \quad u = e^{2x/n_3}, \quad v = e^{2y/n_3}
$$

and obtain

(1)
$$
\begin{aligned}
n_1 u^{n_3} + n_2 v^{n_3} + n_3 u^{-n_1} v^{-n_2} &= K, \\
n_1 u^{-n_3} + n_2 v^{-n_3} + n_3 u^{n_1} v^{n_2} &= K.
\end{aligned}
$$

We summarize what we derived.

Theorem. *Let $\varepsilon \in U(R)$ subject to $T_2(\varepsilon) \geq K$, $T_2(\varepsilon^{-1}) \geq K$ for some constant $K > n$. Let*

$$
T := \left\{ (n_1, n_2, n_3, u, v) \in \mathbb{N}^3 \times (\mathbb{R}^{>0})^2 \ \middle| \ \begin{array}{c} n_1 \geq n_2 \geq n_3, \ n_1 + n_2 + n_3 = n, \\ (u, v) \text{ solution of (1)} \end{array} \right\}.
$$

Then $\sum_{j=1}^{n} (\log |\varepsilon^{(j)}|)^2$ is bounded from below by the minimum of the set

$$
\left\{ \frac{n_3}{4} \left(n_1(n_1 + n_3)(\log u)^2 + n_2(n_2 + n_3)(\log v)^2 + 2n_1 n_2 \log u \log v \right) \ \middle| \right.
$$

$$
\left. (n_1, n_2, n_3, u, v) \in T \right\}
$$

$$
\cup \left\{ \frac{n}{4} \left(\log \left(\frac{K}{n} + \sqrt{\frac{K^2}{n^2} - 1} \right) \right)^2 \right\}.
$$

(*We note that the single element of the second set comes from [4, (6.17)].*)

We conclude this section by showing that for $n = 5$ the set T consists of just three elements which can be easily calculated. Namely, for $n = 5$ there are just two possibilities for the triple (n_1, n_2, n_3).

Case I. $n_1 = n_2 = 2 = 2n_3$.

We have $z = -2(x + y)$, $u = e^{2x}$, $v = e^{2y}$ and (1) becomes

$$
2u + 2v + \frac{1}{u^2 v^2} = K = \frac{2}{u} + \frac{2}{v} + u^2 v^2.
$$

Setting $U = u + v$, $V = uv$ we obtain

$$
2V^2 U + 1 = KV^2, \quad KV = V^3 + 2U.
$$

Hence, V is a zero of the quintic polynomial

$$g_K(t) = t^5 - 1 - Kt^2(t-1).$$

There are exactly three positive zeros of g_K, say

$$V_1 = 1, \ V_2 > 1, \ V_3 = \frac{1}{V_2}.$$

Since with V also $\frac{1}{V}$ is a zero of $g_K(t)$ we obtain

$$V_2 = \frac{1}{4}\left(-1 + \sqrt{4K+5} + \sqrt{2}\sqrt{2K-5 - \sqrt{4K+5}}\right).$$

As corresponding U-values we get

$$U_1 = \frac{K-1}{2}, \quad U_2 = \frac{V_2}{2}(K - V_2^2) = \frac{1}{2}(K - V_2^{-2}).$$

Replacing U_2 by U_3 is tantamount to replacing u_2, v_2 by $\frac{1}{u_2}, \frac{1}{v_2}$. But the latter gives the same lower bound as we immediately see from the structure of the function to be minimized, in this case

$$
\begin{aligned}
Z(V) \ &= \ 2\left(\frac{\log u}{2}\right)^2 + 2\left(\frac{\log v}{2}\right)^2 + (\log u + \log v)^2 \\
&= \ \frac{3}{2}(\log V)^2 + \log u \ \log\frac{u}{V},
\end{aligned}
$$

where $\log v = \log V - \log u$ and w.l.o.g.

$$u = \frac{U}{2} + \sqrt{\frac{U^2}{4} - V}.$$

Hence, we obtain two elements

$$\left(2,2,1, u_1 = \tfrac{K-1}{4} + \sqrt{\left(\tfrac{K-1}{4}\right)^2 - 1}, \tfrac{1}{u_1}\right), \quad (2,2,1, u_2, v_2)$$

of T in this case.

Case II. $n_1 = 3 = 3n_2 = 3n_3$.

Then $z = -3x - y$, $u = e^{2x}$, $v = e^{2y}$ and (1) becomes

$$3u + v + u^{-3}v^{-1} = K = 3u^{-1} + v^{-1} + u^3 v.$$

Eliminating v we obtain that $u \neq 0$ must be a zero of the quintic polynomial

$$h_K(t) = t^5 - 1 - \frac{K}{3}t(t^3 - 1).$$

There are exactly three real zeros:

$$
\begin{aligned}
u_1 \ &= \ 1, \\
u_2 \ &= \ \frac{1}{12}\left(K - 3 + \sqrt{K^2 + 6K + 45}\right. \\
&\qquad \left. + \sqrt{2}\,\sqrt{K^2 - 45 + (K-3)\sqrt{K^2 + 6K + 45}}\right), \\
u_3 \ &= \ \frac{1}{u_2}.
\end{aligned}
$$

The transition from u_2 to u_3 has no effect on the function to be minimized:

$$Z(u) = \frac{1}{4}\left(3\,(\log u)^2 + (\log v)^2 + (3\log u + \log v)^2\right)$$

$$= 3\,(\log u)^2 + \frac{1}{2}(\log v)(3\log u + \log v).$$

Here we can choose v without loss of generality as

$$v = \frac{K-3u}{2} + \sqrt{\left(\frac{K-3u}{2}\right)^2 - u^{-3}}.$$

The radicand of that expression is negative for $K > 5$, however. Hence, in this case the only remaining solution is

$$\left(3, 1, 1, 1, \frac{K-3}{2} + \sqrt{\left(\frac{K-3}{2}\right)^2 - 1}\right).$$

As a demonstration of this new result we list the results of the theorem for $n = 5$ and several K-values. The minimum is always obtained in case II.

K	5	10	15	20	25	30
2 different coordinates	0	2.17	3.88	5.32	6.57	7.67
3 different coordinates, case I, $u = 1$	0	2.10	3.71	5.02	6.14	7.13
3 different coordinates, case I, $u > 1$	0	2.05	3.56	4.78	5.82	6.72
3 different coordinates, case II	0	1.85	3.07	4.00	4.77	5.43

3. RESULTS ON UNIT GROUPS

Since we cannot present all fundamental units, we give a short overview on the size of the regulators R_F that occur. With respect to the Galois group we get the following distributions:

Totally real fields

	A_5	C_5	D_5	$\mathrm{Hol}(C_5)$	S_5	Σ
$0 < R_F < 5$	0	1	0	0	4	5
$5 \le R_F < 10$	0	0	1	0	19	20
$10 \le R_F < 50$	0	2	2	0	1074	1078
$50 \le R_F < 100$	3	1	10	3	3735	3752
$100 \le R_F < 500$	15	1	12	12	17288	17328
$500 \le R_F$	0	0	1	0	556	557
Σ	18	5	26	15	22676	22740

$\mathrm{Hol}(C_5)$, the holomorph of the group C_5, is the semidirect product of C_5 (as normal subgroup) with its automorphism group.

Fields with signature $r_1 = 3$ and $r_2 = 1$

	S_5
$0 < R_F < 5$	258
$5 \leq R_F < 10$	1070
$10 \leq R_F < 50$	29883
$50 \leq R_F < 100$	32242
$100 \leq R_F < 500$	15941
$500 \leq R_F$	0
Σ	79394

Fields with signature $r_1 = 1$ and $r_2 = 2$

	A_5	D_5	$\mathrm{Hol}(C_5)$	S_5	Σ
$0 < R_F < 5$	7	16	3	1782	1808
$5 \leq R_F < 10$	17	7	2	6944	6970
$10 \leq R_F < 50$	140	56	47	91975	92218
$50 \leq R_F < 100$	68	23	26	60445	60562
$100 \leq R_F < 500$	26	27	3	25292	25348
$500 \leq R_F$	0	0	0	0	0
Σ	258	129	81	186438	186906

4. RESULTS ON CLASS GROUPS

We conclude with a detailed survey of the class group structures that occur. With respect to the Galois group the following tables show the frequency of each class group and the corresponding minimal absolute field discriminant (if less than 10^7, respectively 5×10^6). For a field F we denote its class number by h_F and the stucture of its class group by CL_F.

Totally real fields

h_F	CL_F	A_5	C_5	D_5	$\mathrm{Hol}(C_5)$	S_5	Σ
1	C_1	18 (3104644)	5 (14641)	26 (160801)	15 (2382032)	22550 (24217)	22614
2	C_2	—	—	—	—	119 (4010276)	119
3	C_3	—	—	—	—	6 (8481512)	6
4	C_4	—	—	—	—	1 (13664837)	1
Σ		18	5	26	15	22676	22740

Fields with signature $r_1 = 3$ and $r_2 = 1$

h_F	CL_F	C_5
1	C_1	77598 (4511)
2	C_2	1536 (243219)
3	C_3	222 (977483)
4	C_4	32 (2468924)
5	C_5	6 (3982352)
Σ		79394

Fields with signature $r_1 = 1$ and $r_2 = 2$

h_F	CL_F	A_5	D_5	$\mathrm{Hol}(C_5)$	S_5	Σ
1	C_1	221 (18496)	124 (2209)	79 (35152)	166348 (1609)	166772
2	C_2	9 (1132096)	—	—	13724 (41381)	13733
3	C_3	26 (287296)	—	—	3822 (130925)	3848
4	C_4	1 (4981824)	—	—	1122 (370913)	1123
4	$C_2 \times C_2$	—	2 (1868689)	—	97 (1002341)	99
5	C_5	1 (4743684)	2 (717409)	2(1830125)	890 (557220)	895
6	C_6	—	—	—	175 (1219509)	175
7	C_7	—	—	—	173 (1298349)	173
8	C_8	—	—	—	40 (2002568)	40
8	$C_2 \times C_4$	—	—	—	1 (4255620)	1
9	C_9	—	—	—	31 (2803812)	31
10	C_{10}	—	—	—	7 (2761273)	7
11	C_{11}	—	1 (3825936)	—	7 (3965816)	8
12	C_{12}	—	—	—	1 (4892116)	1
	Σ	258	129	81	186438	186906

All computations were done on HP 735 and IBM RS 6000 workstations. We used the number-theoretic program library **KANT V4** [2], which is developed in Berlin. All data are accessible with the **KANT** shell **KASH** from our data base. **KASH** can be obtained via ftp from `ftp.math.tu-berlin.de`. Large parts of the data are also available on the ftp server in Bordeaux.

REFERENCES

1. H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1993. MR **94i:**11105
2. M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig and K. Wildanger, *KANT V4*, to appear in J. Symbolic Comp.
3. M. Pohst, *Computational Algebraic Number Theory*, DMV Seminar 21, Birkhäuser, Basel 1993. MR **94j:**11132
4. M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge Univ. Press, Cambridge 1989. MR **92b:**11074
5. A. Schwarz, M. Pohst and F. Diaz y Diaz, *A Table of Quintic Number Fields*, Math. Comp. **63** (1994), 361–376. MR **94i:**11108

TECHNISCHE UNIVERSITÄT BERLIN, FACHBEREICH 3 MATHEMATIK, SEKR. MA 8-1, STRASSE DES 17. JUNI 136, D–10623 BERLIN, GERMANY
E-mail address: `pohst@math.tu-berlin.de`

TECHNISCHE UNIVERSITÄT BERLIN, FACHBEREICH 3 MATHEMATIK, SEKR. MA 8-1, STRASSE DES 17. JUNI 136, D–10623 BERLIN, GERMANY
E-mail address: `wildan@math.tu-berlin.de`