ON UNRAMIFIED A_m-EXTENSIONS OF QUADRATIC NUMBER FIELDS

by J. ELSTRODT, F. GRUNEWALD and J. MENNICKE

Dedicated to Professor Robert A. Rankin on his 70th birthday

1. Introduction. Number fields such as described in the title play a rôle in the study of Artin L-functions and automorphic forms for the groups SL_2 over rings of integers in quadratic extensions of $\mathbb{Q}$. They are also of some interest on their own. We have not found many examples in the literature. Lang [**4**] mentions an unramified A_5-extension of a real quadratic number field which is due to E. Artin.

The purpose of the present paper is to provide an easy access to such fields. Our main result is the following theorem.

THEOREM. *Consider the polynomial*

$$f(x) = x^m + a_{m-2}x^{m-2} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x], \qquad m > 2.$$

Suppose:

(i) *the polynomial discriminant* Δf *is square-free*

$$\Delta f = \pm p_1 \ldots p_n,$$

(ii) $f(x)$ *is irreducible over* $\mathbb{Q}$, *and has Galois group* S_m.

Consider the quadratic field

$$k = \mathbb{Q}(\sqrt{(\Delta f)}),$$

and the splitting field S of f. Then S/k is an unramified A_m*-extension.*

S_m, A_m denote the full symmetric and the alternating permutation group on m symbols, respectively. We prove our theorem in Section 2. In Section 3 we give some numerical results on the discriminants of polynomials of degree 5. Our tables contain many cases where the assumptions of the theorem apply.

We acknowledge financial support by the Max-Planck-Institut für Mathematik, Bonn.

2. Proof of theorem. Let $\vartheta_1, \vartheta_2, \ldots, \vartheta_m$ be the roots of $f(x) = 0$, in some fixed order. Introduce the chain of fields

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_{m-1} = S,$$

$$K_{j-1} = \mathbb{Q}(\vartheta_1, \vartheta_2, \ldots, \vartheta_{j-1}).$$

Then

$$K_j = K_{j-1}(\vartheta_j).$$

The extension K_j/K_{j-1} has the degree

$$|K_j : K_{j-1}| = m - j + 1, \qquad 1 \le j \le m-1,$$

https://doi.org/10.1017/S0017089500006054 Published online by Cambridge University Press

and the defining polynomial

$$g_j(x) = \frac{f(x)}{(x-\vartheta_1)(x-\vartheta_2)\dots(x-\vartheta_{j-1})} \in K_{j-1}[x].$$

Put

$$g_1(x) = f(x).$$

Obviously we have

$$g_j(x) = \frac{g_{j-1}(x)}{x-\vartheta_{j-1}}.$$

The polynomial $g_j(x)$ has the roots $\vartheta_j, \vartheta_{j+1}, \dots, \vartheta_m$. Hence we have

$$\Delta g_j = \{(\vartheta_j - \vartheta_{j+1})(\vartheta_j - \vartheta_{j+2}) \dots (\vartheta_j - \vartheta_m)\}^2 \, \Delta g_{j+1}.$$

This can be written as

$$\Delta g_j = g_j'(\vartheta_j)^2 \, \Delta g_{j+1}. \tag{1}$$

The quantity

$$g_j'(\vartheta_j) = \delta_{K_j/K_{j-1}}(\vartheta_j) \tag{2}$$

is the relative different of ϑ_j. We have

$$N_{K_j/K_{j-1}} g_j'(\vartheta_j) = \Delta g_j. \tag{3}$$

Let $\mathfrak{p}_i^{(j)}$, $\mathfrak{q}_i^{(j)}$ denote ideals in K_j. Suppose, inductively,

$$\Delta g_j = \mathfrak{q}_1^{(j-1)} \dots \mathfrak{q}_n^{(j-1)} \quad \text{in} \quad K_{j-1}, \tag{4}$$

where $\mathfrak{q}_i^{(j-1)}$ is square-free, i.e. it is a product of different prime ideals, and

$$N_{K_{j-1}/K_0} \mathfrak{q}_i^{(j-1)} = p_i^{(m-2)(m-3)\dots(m-j)}, \qquad i = 1, \dots, n. \tag{5}$$

For $j = 1$, we have $g_1 = f$. Hence (4) holds by assumption (i). The exponent on the right hand side of (5) is understood to be 1 for $j = 1$. Hence the induction hypothesis holds true for $j = 1$.

We show that (4), (5) hold for $j+1$. Since $\Delta g_j \in K_{j-1}$, we have

$$N_{K_j/K_{j-1}}(\Delta g_j) = (\Delta g_j)^{m-j+1}.$$

Conclude from (1) and (3):

$$N_{K_j/K_{j-1}}(\Delta g_{j+1}) = (\Delta g_j)^{m-j-1} = (\mathfrak{q}_1^{(j-1)} \dots \mathfrak{q}_n^{(j-1)})^{m-j-1}. \tag{6}$$

The ideal (Δg_j) is square-free in K_{j-1}, by induction hypothesis. By assumption (i), it does not contain any inessential divisors. Hence it coincides with the relative discriminant:

$$(\Delta g_j) = (d_{K_j/K_{j-1}}). \tag{7}$$

Hence all prime factors of $\mathfrak{q}_i^{(j-1)}$ ramify in K_j. Since the ramification is tame, by assumption (i), and since $(d_{K_j/K_{j-1}})$ is square-free, the ramification must be of the form

$$\mathfrak{q}_i^{(j-1)} = (\mathfrak{p}_i^{(j)})^2 \mathfrak{q}_i^{(j)}, \tag{8}$$

$$N_{K_j/K_{j-1}} \mathfrak{p}_i^{(j)} = \mathfrak{q}_i^{(j-1)}, \qquad N_{K_j/K_{j-1}} \mathfrak{q}_i^{(j)} = (\mathfrak{q}_i^{(j-1)})^{m-j-1}. \tag{9}$$

https://doi.org/10.1017/S0017089500006054 Published online by Cambridge University Press

The ideals $\mathfrak{p}_i^{(j)}$, $\mathfrak{q}_i^{(j)}$ are square-free in K_j. The ramified primes $\mathfrak{p}_i^{(j)}$ all divide the discriminant $g_j'(\vartheta_j)$:

$$g_j'(\vartheta_j) = \mathfrak{p}_1^{(j)} \dots \mathfrak{p}_n^{(j)} \cdot \mathfrak{r}. \tag{10}$$

Inserting this equation in (1), we obtain

$$\mathfrak{q}_1^{(j)} \dots \mathfrak{q}_n^{(j)} = \mathfrak{r}^2 \Delta g_{j+1}. \tag{11}$$

Taking norms on both sides of (11), we conclude from (6) and (9):

$$N_{K_j/K_{j-1}} \mathfrak{r}^2 = 1, \quad \text{and hence} \quad \mathfrak{r} = 1.$$

Hence we have

$$g_j'(\vartheta_j) = \mathfrak{p}_1^{(j)} \dots \mathfrak{p}_n^{(j)}, \tag{12}$$

$$\Delta g_{j+1} = \mathfrak{q}_1^{(j)} \dots \mathfrak{q}_n^{(j)}. \tag{13}$$

This proves (4) for $j+1$. Use (9) to conclude

$$N_{K_j/K_0} \mathfrak{q}_i^{(j)} = N_{K_{j-1}/K_0} N_{K_j/K_{j-1}} \mathfrak{q}_i^{(j)} = N_{K_{j-1}/K_0} (\mathfrak{q}_i^{(j-1)})^{m-j-1}$$
$$= p_i^{(m-2)(m-3)\dots(m-j)(m-j-1)}.$$

This proves (5) for $j+1$. Hence (4), (5) hold for all j such that $1 \leq j \leq m-1$.

Let $L_j = K_j k$. Hence L_j/K_j is the relative quadratic extension obtained by adjoining $\sqrt{(\Delta f)}$. The extension is of degree 2, by assumption (ii). We use the decomposition laws in quadratic extensions, see Hecke [**2**, p. 148]. We have, by (8):

$$(p_1 \dots p_n) = (\Delta f) = (\mathfrak{p}_1^{(1)} \dots \mathfrak{p}_n^{(1)} \mathfrak{p}_1^{(2)} \dots \mathfrak{p}_n^{(2)} \dots \mathfrak{p}_1^{(j)} \dots \mathfrak{p}_n^{(j)})^2 \mathfrak{q}_1^{(j)} \dots \mathfrak{q}_n^{(j)}. \tag{14}$$

Hence, in L_j/K_j, all prime factors of $\mathfrak{q}_i^{(j)}$ ramify:

$$\mathfrak{q}_i^{(j)} = (\mathfrak{Q}_i^{(j)})^2, \qquad N_{L_j/K_j} \mathfrak{Q}_i^{(j)} = \mathfrak{q}_i^{(j)}. \tag{15}$$

The prime 2 does not ramify in K_j, by assumption (i). Let ℓ be a prime divisor of 2 in K_j:

$$(2) = \ell . \ell_1, \qquad (\ell, \ell_1) = 1.$$

We have to study the congruence

$$\Delta f = \xi^2 \bmod \ell^2. \tag{16}$$

The assumption (i) implies that Δf is a field discriminant, of the field K_1. Use Stickelberger's theorem to conclude

$$\Delta f \equiv 1 \bmod 4.$$

Hence the congruence (16) is solvable in K_j, and hence ℓ does not ramify in L_j. Hence we obtain for the relative different:

$$\mathfrak{D}_{L_j/K_j} = \mathfrak{Q}_1^{(j)} \dots \mathfrak{Q}_n^{(j)}.$$

The different of L_j is

$$\mathfrak{D}_{L_j} = \mathfrak{Q}_1^{(j)} \dots \mathfrak{Q}_n^{(j)} \dots \mathfrak{D}_{K_j}.$$

Taking norms, we obtain

$$N_{L_j/K_j} \mathfrak{D}_{L_j} = \mathfrak{q}_1^{(j)} \dots \mathfrak{q}_n^{(j)} \dots \mathfrak{D}_{K_j}^2.$$

https://doi.org/10.1017/S0017089500006054 Published online by Cambridge University Press

Deduce from (14):

$$\mathcal{D}_{K_j} = \mathfrak{p}_1^{(1)} \ldots \mathfrak{p}_n^{(1)} \ldots \mathfrak{p}_1^{(2)} \ldots \mathfrak{p}_n^{(2)} \ldots \mathfrak{p}_1^{(j)} \ldots \mathfrak{p}_n^{(j)}.$$

Hence we obtain

$$N_{L_j/K_j}\mathcal{D}_{L_j} = (p_1 \ldots p_n),$$
$$N_{L_j/K_0}\mathcal{D}_{L_j} = (p_1 \ldots p_n)^{m(m-1)\ldots(m-j+1)}. \tag{17}$$

For the different $\mathfrak{g} = (\sqrt{(\Delta f)})$ of k, we have

$$N_{L_j/K_0}\mathfrak{g} = (p_1 \ldots p_n)^{m(m-1)\ldots(m-j+1)}.$$

Consider

$$\mathcal{D}_{L_j} = \mathcal{D}_{L_j/k} \cdot \mathfrak{g}.$$

Take absolute norms on both sides, and observe (17), (18), obtaining

$$N_{L_j/K_0}\mathcal{D}_{L_j/k} = 1,$$

and hence

$$\mathcal{D}_{L_j/k} = 1.$$

Hence L_j/k is unramified for $1 \leq j \leq m-1$. For $j = m-1$, this proves the theorem.

REMARK. Invoking class field theory, we find that our result implies congruence relations for certain class numbers. Whenever $k < k_1 < k_2 < S$ is a chain of subfields such that k_2/k_1 is normal with abelian Galois group, the class number h_{k_1} of k_1 is divisible by the degree $|k_2 : k_1|$.

3. Numerical examples. In this section we give some numerical examples where the assumptions of our theorem are satisfied. To do this it is necessary to have an explicit formula for the discriminant Δf of a polynomial f. We report here on the case $m = 5$.

PROPOSITION 1. *Let*

$$f(x) = x^5 + ax^3 + bx^2 + cx + d$$

be a polynomial with rational coefficients. Then its discriminant is

$$\begin{aligned}\Delta f = {} & 5^5d^4 - 2 \cdot 3 \cdot 5^4 \cdot d^3ba + 2^4 \cdot 5^3 \cdot d^2c^2a + 2 \cdot 3^2 \cdot 5^3 \cdot d^2cb^2 \\ & - 2^2 \cdot 3^2 \cdot 5^2 \cdot d^2ca^3 + 3 \cdot 5^2 \cdot 11 \cdot d^2b^2a^2 + 2^2 \cdot 3^3 \cdot d^2a^5 - 2^6 \cdot 5^2 \cdot dc^3b \\ & + 2^4 \cdot 5 \cdot 7 \cdot dc^2ba^2 - 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot dcb^3a - 2^3 \cdot 3^2 \cdot dcba^4 \\ & + 2^2 \cdot 3^3 \cdot db^5 + 2^4 \cdot db^3a^3 + 2^8 \cdot c^5 - 2^7 \cdot c^4a^2 + 2^4 \cdot 3^2 \cdot c^3b^2a \\ & + 2^4 \cdot c^3a^4 - 3^3 \cdot c^2b^4 - 2^2 \cdot c^2b^2a^3.\end{aligned}$$

The occurrence of the prime factors 7 and 11 is somewhat mysterious. The formula is slightly more complicated than the well-known formulae for polynomials of degrees 2, 3, 4. It is, however, still useful for computations for small values of a, b, c, d. After we had finished our computation, we discovered the formula of Proposition 1 in Cayley's work [**1**].

TABLE 1. $f = x^5 + ax^3 + bx^2 + cx + d$

no	a	b	c	d	Δf	h_k
1	−1	−1	−1	1	$-7031 = -79 . 89$	$108 = 2^2 . 3^3$
2	0	−1	−2	1	$-22583 = -11 . 2053$	$90 = 2 . 3^2 . 5$
3	−1	0	−2	1	$-17151 = -3 . 5717$	$110 = 2 . 5 . 11$
4	0	−2	−1	1	-13219	31
5	−1	−2	0	1	$-4511 = -13 . 347$	$84 = 2^2 . 3 . 7$
6	−1	−3	1	1	$-24447 = -3 . 29 . 281$	$92 = 2^2 . 23$
7	−3	−1	−1	1	$-71943 = -3 . 23981$	$130 = 2 . 5 . 13$
8	−2	−1	−1	2	$-72579 = -3 . 13 . 1861$	$72 = 2^3 . 3^2$
9	−2	0	−2	1	$-49163 = -211 . 233$	$50 = 2 . 5^2$
10	−2	1	−2	1	$-19015 = -5 . 3803$	$106 = 2 . 53$
11	−2	−1	−2	1	$-77063 = -7 . 101 . 109$	$276 = 2^2 . 3 . 23$
12	1	−2	−2	1	$-54967 = -11 . 19 . 263$	$104 = 2^3 . 13$
13	−1	−2	−2	1	$-60023 = -193 . 311$	$252 = 2^2 . 3^2 . 7$
14	−2	−2	−2	1	$-91363 = -211 . 433$	$56 = 2^3 . 7$
15	0	0	−3	1	-59083	37
16	−1	0	−3	1	$-90691 = -89 . 1019$	$76 = 2^2 . 19$
17	−3	0	−1	1	-56123	43
18	0	−3	0	1	$-23119 = -61 . 379$	$124 = 2^2 . 31$
19	1	−1	−3	1	$-105887 = -19 . 5573$	$256 = 2^8$
20	−1	−3	−1	1	$-40711 = -11 . 3701$	$148 = 2^2 . 37$
21	−3	1	−1	1	-28927	$65 = 5 . 13$
22	−3	−1	1	1	-5519	97
23	0	−2	−3	1	-179827	$51 = 3 . 17$
24	2	0	−3	1	-46411	$49 = 7^2$
25	−2	0	−3	1	-168523	61
26	−2	−3	0	1	-15919	$51 = 3 . 17$
27	0	−3	−1	2	-95531	$123 = 3 . 41$
28	0	−3	−2	1	$-118959 = -3 . 39653$	$236 = 2^2 . 59$
29	−3	0	−2	1	$-132711 = -3 . 31 . 1427$	$380 = 2^2 . 5 . 19$
30	−3	−1	−1	2	$-268183 = -233 . 1151$	$204 = 2^2 . 3 . 17$
31	−1	−2	−2	3	$-249119 = -13 . 19163$	$820 = 2^2 . 5 . 41$
32	−2	−1	−2	3	$-345559 = -17 . 20327$	$226 = 2 . 113$
33	−2	−2	−1	3	$-253163 = -383 . 661$	$108 = 2^2 . 3^3$
34	−2	1	−3	2	$-124763 = -17 . 41 . 179$	$68 = 2^2 . 17$
35	−2	−3	1	2	$-46259 = -167 . 277$	$94 = 2 . 47$
36	2	−3	−2	1	$-170319 = -3 . 56773$	$308 = 2^2 . 7 . 11$
37	2	−2	−3	1	$-249707 = -71 . 3517$	$148 = 2^2 . 37$
38	−2	2	−3	1	$-33131 = -7 . 4733$	$92 = 2^2 . 23$
39	−2	−3	−2	1	-96263	$301 = 7 . 43$
40	3	−2	−2	1	$-44503 = -191.233$	$74 = 2 . 37$
41	−3	2	−2	1	-25679	239
42	−3	−2	2	1	-8647	31
43	−3	−2	−2	1	$-188695 = -5 . 13 . 2903$	$164 = 2^2 . 41$
44	−3	0	−3	1	$-340531 = -503 . 677$	$98 = 2 . 7^2$
45	−1	−3	−1	3	$-240871 = -79 . 3049$	$258 = 2 . 3 . 43$
46	−3	−1	1	3	$-32519 = -31 . 1049$	$178 = 2 . 89$
47	−3	−3	1	1	$-14631 = -3 . 4877$	$58 = 2 . 29$
48	−3	−1	−1	3	-545911	$321 = 3 . 107$
49	−3	−3	−1	1	$-41591 = -11 . 19 . 199$	$256 = 2^8$
50	3	−1	−3	1	$-147463 = -239 . 617$	$142 = 2 . 71$
51	1	−3	−3	1	$-369223 = -17 . 37 . 587$	$292 = 2^2 . 73$

Table (contd.)

https://doi.org/10.1017/S0017089500006054 Published online by Cambridge University Press

TABLE 1. (*contd.*)

no	a	b	c	d	Δf	h_k
52	−1	−3	−3	1	−259783	$315=3^2.5.7$
53	0	−3	−2	3	−322247	461
54	−1	−2	−3	3	−666507 = −3 . 29 . 47 . 163	$120=2^3.3.5$
55	−3	0	−2	3	−673463 = −7 . 23 . 47 . 89	$776=2^3.97$
56	−3	−2	−1	3	−707419 = −599 . 1181	$198=2.3^2.11$
57	−3	1	−3	2	−447871 = −227 . 1973	$350=2.5^2.7$
58	−3	2	−3	1	−101923 = −227 . 449	$60=2^2.3.5$
59	−3	−2	−3	1	−480427	123 = 3 . 41
60	−2	−3	2	3	−11551	57 = 3 . 19
61	−3	−2	2	3	−18463 = −37 . 499	$54=2.3^3$
62	−3	−2	−2	3	−1338863	555 = 3 . 5 . 37
63	2	−3	−3	2	−517243	$121=11^2$
64	−3	−3	1	3	−125951 = −7 . 19 . 947	$408=2^3.3.17$
65	3	−3	−3	1	−636991 = −47 . 13553	$608=2^5.19$
66	−3	3	−3	1	−27007 = −113 . 239	$68=2^2.17$
67	−3	−3	3	1	−144079 = −13 . 11083	310 = 2 . 5 . 31
68	−3	−3	−3	1	−453823	353
69	−3	−3	−3	2	−1264063	407 = 11 . 37

We have produced, in Table 1, all extensions of imaginary quadratic fields such as described in the title in the range $-3 \leq a, b, c, d \leq 3$. In Table 2, we have listed a few examples of unramified A_5-extensions of real quadratic number fields, including Artin's example which is the first in our table.

Using the formula of Proposition 1, it is a trivial matter to write a computer program which computes $\Delta(f)$ for small values of a, b, c, d. We have carried out the computations for a, b, c, d of absolute value ≤ 3. We list the results in the subsequent tables. The column headed by h_k contains the class number of k.

TABLE 2. $f = x^5 + ax^3 + bx^2 + cx + d$

no	a	b	c	d	Δf
1	0	0	−1	1	2863 = 19 . 151
2	0	1	0	1	3017 = 7 . 431
3	0	−1	0	1	3233 = 53 . 61
4	1	1	1	1	13033
5	1	1	−1	1	4897 = 59 . 83
6	1	−1	1	1	2297
7	−1	1	1	1	1609
8	−1	1	−1	1	3857 = 7 . 19 . 29
9	−1	−1	1	1	8329
10	0	0	2	1	11317
11	1	0	−2	1	2665 = 5 . 13 . 41
12	−1	0	2	1	3089
13	0	1	1	2	56245 = 5 . 7 . 1607
14	0	−1	1	2	62213
15	0	−1	−1	2	37301 = 11 . 3391

PROPOSITION 2. *In Table* 1, *we have listed all polynomials* $f = x^5 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ *with* $-3 \leq a, b, c, d \leq 3$ *satisfying the conditions* (i), (ii) *of Theorem* 1 *for* $m = 5$ *and satisfying* $\Delta f < 0$.

In Table 2 we have listed a few examples, including Artin's example.

REFERENCES

1. A. Cayley, On a new auxiliary equation in the theory of equations of the fifth order, *Philos. Trans. Roy. Soc. London*, **CLI,** (1861), 263–276.

2. H. Hasse, *Zahlentheorie* (Akademie, 1949).

3. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen* (Akademische Verlagsgesellschaft, 1954).

4. S. Lang, *Algebraic Number Theory* (Addison-Wesley, 1970).

5. B. L. van der Waerden, *Moderne Algebra* (Springer, 1950).

MÜNSTER (WESTFALEN) BONN BIELEFELD

https://doi.org/10.1017/S0017089500006054 Published online by Cambridge University Press