Mathematica Slovaca

Antonín Dvořák; David Jedelský; Juraj Kostra

The fields of degree seven over rationals with a normal basis generated by a unit

Mathematica Slovaca, Vol. 49 (1999), No. 2, 143--153

Persistent URL: http://dml.cz/dmlcz/136747

Math. Slovaca, 49 (1999), No. 2, 143–153

THE FIELDS OF DEGREE SEVEN OVER RATIONALS WITH A NORMAL BASIS GENERATED BY A UNIT

Antonín Dvořák* — David Jedelský** — Juraj Kostra***

(Communicated by Stanislav Jakubec)

ABSTRACT. In this paper we determine all fields of degree seven over rationals which have an integral normal basis generated by a unit.

In this paper we determine all fields of degree 7 over rationals which have integral normal basis generated by a unit. In [1] the following necessary condition was found for the existence of such a basis in the prime extensions of rationals.

Theorem 1. *Let K be a tamely ramified extension of $\mathbb{Q}$ of prime degree l and let $m = p_1 \cdot p_2 \dots p_s$ be a conductor of the field K. Let there exist an integral normal basis generated by a unit in the field K. Then*

$$l^l \equiv 1 \pmod{p_i}, \qquad i = 1, 2, \dots, s,$$

or

$$l^l \equiv -1 \pmod{p_i}, \qquad i = 1, 2, \dots, s.$$

Let $[K : \mathbb{Q}] = 7$ with the conductor m. If there exists an integral normal basis generated by a unit in the field K, then the above theorem determines the possible values of m. We have to find all primes p, $p \equiv 1 \pmod 7$, for which

$$7^7 \equiv 1 \pmod p,$$

and all primes p, $p \equiv 1 \pmod 7$, for which

$$7^7 \equiv -1 \pmod p.$$

From the first congruence we get three possible values of the conductor m:

$$m = 29, \quad m = 4733, \quad m = 29 * 4733.$$

AMS Subject Classification (1991): Primary 11R33.
Key words: normal basis, unit, circulant matrix.

This paper has been supported by grant 201/97/0433 of GA ČR

From the second congruence we get the three remaining possible values of the conductor m:

$$m = 113, \quad m = 911, \quad m = 113 * 911 .$$

Let m be a prime number. Then there exists only one field K, $[K : \mathbb{Q}] = 7$, with Galois group $G(\mathbb{Q}(\zeta_m)/K)$ generated by $\sigma^{\frac{m-1}{7}}$, where σ is the generator of $G(\mathbb{Q}(\zeta_m)/K)$.

Let $m = p_1 p_2$ be a product of two primes p_1 and p_2, then, by [2; Lemma 2], an arbitrary $K \subset \mathbb{Q}(\zeta_m)$, $[K : \mathbb{Q}] = 7$, is a subfield of the composite $L = K_1 K_2$ where $[K_1 : \mathbb{Q}] = 7$, $[K_2 : \mathbb{Q}] = 7$ and $K_1 \subset \mathbb{Q}(\zeta_{p_1})$, $K_2 \subset \mathbb{Q}(\zeta_{p_2})$. The Galois group is $G(K_1 K_2/\mathbb{Q}) = G(K_1/\mathbb{Q}) \times G(K_2/\mathbb{Q})$, where $G(K_1/\mathbb{Q})$ is generated by ρ and $G(K_2/\mathbb{Q})$ is generated by τ.

In this situation, there exist six fields K with conductor m and $[K : \mathbb{Q}] = 7$. They are determined by the subgroups $G(L/K)$ of $G(L/\mathbb{Q})$ generated by

1. $[\rho, \tau]$	4. $[\rho, \tau^4]$
2. $[\rho, \tau^2]$	5. $[\rho, \tau^5]$
3. $[\rho, \tau^3]$	6. $[\rho, \tau^6]$.

In any such field K, there exists an integral normal basis generated by

$$\alpha = \mathrm{Tr}_{\mathbb{Q}(\zeta_m)/K}(\zeta_m),$$

where ζ_m is a primitive mth root of unity.

We have the following possibilities for the fields K:

(1) For $m = 29$, $\mathbb{Q} \subset K_1 \subset \mathbb{Q}(\zeta_{29})$, $N_{K_1/\mathbb{Q}}(\alpha) = -1$.

(2) For $m = 4733$, $\mathbb{Q} \subset K_2 \subset \mathbb{Q}(\zeta_{4733})$, $N_{K_2/\mathbb{Q}}(\alpha) = -28161351$.

(3) For $m = 29{*}4733$, fields $K_3, \dots, K_8$ correspond to subgroups of $G(L/K)$ generated by the restrictions of automorphism $\delta \in G(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, in the following table:

K_i	δ	$N_{K_i/\mathbb{Q}}(\alpha)$
3	$\zeta_m \mapsto \zeta_m^{85537}$	251154785688281
4	$\zeta_m \mapsto \zeta_m^{41921}$	898325927423
5	$\zeta_m \mapsto \zeta_m^{41921}$	-76788374021713
6	$\zeta_m \mapsto \zeta_m^{16807}$	91709057071919
7	$\zeta_m \mapsto \zeta_m^{75735}$	-144070291575808
8	$\zeta_m \mapsto \zeta_m^{111260}$	179069050883

(1) For $m = 113$, $\mathbb{Q} \subset K_9 \subset \mathbb{Q}(\zeta_{113})$, $N_{K_9/\mathbb{Q}}(\alpha) = 1$.
(2) For $m = 911$, $\mathbb{Q} \subset K_{10} \subset \mathbb{Q}(\zeta_{911})$, $N_{K_{10}/\mathbb{Q}}(\alpha) = 225929$.
(3) For $m = 113 * 911$, the fields $K_{11}, \ldots, K_{16}$ correspond to subgroups of $G(L/K)$ generated by the restrictions of the automorphism $\delta \in G(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, in the following table:

K_i	δ	$N_{K_i/\mathbb{Q}}(\alpha)$
11	$\zeta_m \mapsto \zeta_m^{49}$	-24680042975707
12	$\zeta_m \mapsto \zeta_m^{5134}$	-41156429602663
13	$\zeta_m \mapsto \zeta_m^{48413}$	52987176319235
14	$\zeta_m \mapsto \zeta_m^{7281}$	-84808664064
15	$\zeta_m \mapsto \zeta_m^{50673}$	150145053959387
16	$\zeta_m \mapsto \zeta_m^{15078}$	-143192889457

For K_1 $(m = 29)$ and K_9 $(m = 113)$ the generator α of the normal basis is a unit. For the remaining K_i we shall investigate the set of all integral normal bases as follows: We shall use the fact that, in our case, the linear mapping which transforms an integral normal basis of the field K into an integral normal basis of the field K is represented by a unimodular circulant matrix of degree 7. By [1] the group of all unimodular circulant matrices of degree 7 is isomorphic to the subgroup E of finite index in the group of all units of the field $\mathbb{Q}(\zeta_7)$.

For the subgroup E we have

$$E = \{\gamma \in \mathbb{Q}(\zeta_7);\ \gamma \text{ is a unit},\ \gamma \equiv \pm 1 \pmod{(1-\zeta_7)}\}.$$

The group of all units of the field $\mathbb{Q}(\zeta_7)$ is generated by two fundamental units, e.g.

$$\eta_1' = 1 + \zeta_7 + \zeta_7^2 + \zeta_7^4 + \zeta_7^5$$

and

$$\eta_2' = 1 + \zeta_7^2 + \zeta_7^3 + \zeta_7^5.$$

The group E generated by

$$\eta_1 = -\eta_1'\eta_2 = -1 + \zeta_7 + \zeta_7^6$$

and

$$\eta_2 = (\eta_2')^3 = -1 + 2\zeta_7 - \zeta_7^3 + 2\zeta_7^5 - \zeta_7^6$$

is of index 3 in the group of all units of the field $\mathbb{Q}(\zeta_7)$. We obtain an arbitrary integral normal basis of the field K by the transformation of an integral normal basis generated by α by means of a unimodular circulant matrix which corresponds to E.

Let

$$\mathbf{A} = \mathrm{circ}_7(-1,1,0,0,0,0,1)$$

corresponds to η_1 and

$$\mathbf{B} = \mathrm{circ}_7(-1,2,0,-1,0,2,-1)$$

corresponds to η_2. That means that any integral normal basis $\beta_1,\beta_2,\dots,\beta_7$ of the field K (up to sign and order) can be obtained as follows

$$(\beta_1,\beta_2,\dots,\beta_7) = (\alpha_1,\alpha_2,\dots,\alpha_7)\cdot \mathbf{A}^{\iota}\cdot \mathbf{B}^{\nu}.$$

Now we shall investigate the set

$$\{N_{K/\mathbb{Q}}(\beta_1);\ (\beta_1,\beta_2,\dots,\beta_7) = (\alpha_1,\alpha_2,\dots,\alpha_7)\cdot \mathbf{A}^{\iota}\cdot \mathbf{B}^{\nu},\ \ \iota,\nu\in\mathbb{Z}\} \qquad (*)$$

modulo p_i, where p_i is appropriate prime number. If there exists an integral normal basis generated by a unit β_1 in the field K, clearly $N_{K/\mathbb{Q}}(\beta_1) \equiv \pm 1 \pmod{p_i}$.

Let the period of the matrix $\mathbf{M}$ modulo p_i be denoted as $r^{\mathbf{M}}_{p_i}$, i.e. we have the following:

$$\mathbf{M}^k \mod p_i = \mathbf{I}', \qquad k = r^{\mathbf{M}}_{p_i},$$

where $\mathbf{I}'$ is either the unit matrix or the unit matrix with permuted rows.

Let the norm $N_{K/\mathbb{Q}}(\beta_1) \equiv \rho \pmod{p_1}$, where ρ is either 1 or -1, for some $\iota = \iota_1$, $\nu = \nu_1$ from $(*)$. If there exists an integral normal basis generated by a unit in the field K then there should exist powers ι_t and ν_t such that for some $k \in \mathbb{N}$

$$\left.\begin{aligned} \iota_t &= (k\cdot r^A_{p_1} + \iota_1) \mod r^A_{p_t}\\ \nu_t &= (k\cdot r^B_{p_1} + \nu_1) \mod r^B_{p_t}\\ N_{K/\mathbb{Q}}(\beta_1) &\equiv \rho \pmod{p_t}. \end{aligned}\right\} \qquad (\diamond)$$

If such powers do not exist then no integral normal basis generated by unit exists in the field.

Prime numbers $p_1,p_2,\dots$ were chosen such that the periods $r^{\mathbf{A}}_{p_i}$, $r^{\mathbf{B}}_{p_i}$, $i = 2,3,\dots$ are multiples of periods $r^{\mathbf{A}}_{p_1}$, $r^{\mathbf{B}}_{p_1}$, respectively. The prime numbers which were used for computations are shown in following table.

i	p_i	$r_{p_i}^{\mathsf{A}}$	$r_{p_i}^{\mathsf{B}}$
1	43	42	14
2	127	$3 * 42$	$3 * 14$
3	211	$5 * 42$	$5 * 14$
4	883	$7 * 42$	$21 * 14$

The results of the computations are in the tables at the end of this paper. The columns p_i contain those primes which satisfy ($\diamond$).

The Tables show that in none of the fields $K_2, \ldots, K_8, K_{10}, \ldots, K_{16}$ does there exist an integral normal basis generated by a unit. Thus the integral normal basis generated by a unit exists only in the fields K_1 and K_9.

Remark. All the fields of prime degree l so far known with an integer normal basis generated by a unit have a prime conductor and they are generated by a Gaussian period α. For $l = 3$, $\mathbb{Q} \subset K = \mathbb{Q}(\zeta_3)$ and $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_5)$. For $l = 5$, $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_{11})$ and $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_{71})$. For primes equal to $2l + 1$ or $4l + 1$ fields K of degree l, $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_p)$, have an integral normal basis generated by a unit, because a sum of two or four roots of unity is a unit.

Results for $m = 911$ and $m = 4733$, fields K_{10} and K_2.

ι	ν	ρ	p_i
1	1	-1	43,127
4	4	1	43
6	12	1	43
7	6	1	43
7	7	1	43
8	9	-1	43
8	11	-1	43
11	11	1	43
12	14	1	43
13	12	-1	43,127
15	9	1	43
20	3	1	43
20	12	1	43,127
23	14	1	43
24	6	1	43
25	3	-1	43
26	14	1	43
30	6	1	43
33	5	1	43
34	2	-1	43
34	3	1	43
34	10	1	43,127
37	3	-1	43
39	1	-1	43
39	6	-1	43
41	10	-1	43
42	5	1	43
42	7	-1	43

ι	ν	ρ	p_i
2	7	1	43
4	11	-1	43
5	5	-1	43
8	2	-1	43
9	11	1	43
10	13	-1	43
10	14	1	43
13	12	1	43
14	7	-1	43
15	12	1	43
15	13	-1	43
17	11	-1	43
17	13	-1	43
18	9	-1	43
22	5	1	43
23	6	1	43
23	10	1	43,127
30	9	-1	43
38	2	-1	43
39	3	1	43
40	2	-1	43
40	5	1	43,127

Results for $m = 29 * 4733$, fields K_3, K_4 and K_5.

ι	ν	ρ	p_i
3	1	1	43
4	3	-1	43
4	7	-1	43
6	3	1	43
8	10	-1	43
9	7	1	43
10	3	-1	43
11	2	-1	43
11	12	-1	43,127
12	1	-1	43,127
12	14	1	43
15	11	-1	43
17	5	-1	43
18	2	1	43
20	2	1	43
20	5	1	43
20	8	-1	43
21	2	1	43
21	8	-1	43
21	9	1	43
21	10	-1	43
22	5	-1	43
22	10	-1	43
23	1	-1	43
24	8	1	43
25	11	-1	43
27	6	1	43,127
27	13	-1	43
29	1	-1	43
30	12	1	43
31	9	1	43,127
34	11	-1	43
35	7	1	43,127,211
37	13	-1	43
37	14	-1	43
38	4	1	43
39	11	-1	43
40	3	-1	43
41	4	-1	43

ι	ν	ρ	p_i
1	7	-1	43
6	11	-1	43
10	4	-1	43
10	11	1	43
11	14	-1	43
12	4	1	43
12	5	1	43
12	7	1	43
15	5	-1	43
17	10	-1	43
18	14	-1	43
19	6	1	43
20	4	-1	43
20	7	1	43,127
22	3	1	43
22	4	-1	43
23	9	1	43
24	12	-1	43
28	2	1	43
28	5	-1	43
30	10	-1	43
31	8	1	43
32	9	1	43,127
33	3	-1	43,127
34	7	1	43
37	7	1	43
37	11	-1	43
38	12	1	43
42	10	-1	43

ι	ν	ρ	p_i
1	10	1	43
3	14	1	43,127
4	5	-1	43
7	8	-1	43
7	9	1	43
8	5	-1	43
9	11	-1	43
11	4	-1	43
11	11	-1	43
16	1	1	43,127
17	13	-1	43
18	7	-1	43
19	9	-1	43
20	5	1	43
23	12	1	43
26	3	1	43
26	10	-1	43
26	11	-1	43
28	9	-1	43
31	4	1	43
33	1	1	43
33	14	1	43
34	4	1	43
34	7	-1	43,127
36	6	1	43
39	9	1	43
40	9	1	43

Results for $m = 29 * 4733$, fields K_6, K_7 and K_8.

ι	ν	ρ	p_i
3	1	-1	43
6	13	1	43
8	9	1	43
10	6	-1	43
11	4	1	43
12	10	1	43
14	2	-1	43
15	2	-1	43
15	6	1	43
16	6	1	43
16	10	1	43
20	9	1	43
21	8	-1	43
22	4	1	43
25	4	1	43
26	2	-1	43
26	5	-1	43
26	11	1	43
28	14	-1	43
29	5	1	43
29	6	-1	43
29	10	1	43
32	6	-1	43
32	11	1	43,127,211
33	1	1	43
37	8	-1	43
39	5	-1	43
39	14	-1	43
40	7	1	43
42	1	-1	43

ι	ν	ρ	p_i
1	11	1	43
5	13	-1	43,127
6	13	-1	43
6	14	-1	43
8	11	-1	43
11	2	-1	43
11	13	1	43
15	1	1	43
15	2	-1	43
15	5	-1	43
18	7	1	43
19	10	1	43
20	8	1	43
21	2	-1	43
24	6	-1	43
28	1	-1	43
30	4	1	43
31	2	1	43
31	12	-1	43
31	14	-1	43
33	2	-1	43
33	5	-1	43
35	1	-1	43
35	3	-1	43
35	6	1	43
35	7	1	43
37	12	-1	43,127
41	7	1	43
41	12	1	43
41	13	1	43
42	4	1	43

ι	ν	ρ	p_i
1	12	1	43
2	14	-1	43
4	4	-1	43,127
4	7	1	43
5	4	1	43
8	7	-1	43
11	2	-1	43
14	8	1	43
17	8	1	43
19	6	1	43
22	7	-1	43
22	12	-1	43
23	4	-1	43
24	7	1	43
25	12	-1	43
29	10	1	43
33	4	1	43
37	1	1	43
38	3	-1	43

Results for $m = 113 * 911$, fields K_{11}, K_{12} and K_{13}.

ι	ν	ρ	p_i
5	4	-1	43
6	7	-1	43
6	8	1	43
8	1	1	43
11	6	-1	43
12	11	1	43,127,211
15	5	1	43
15	9	1	43,127,211
16	12	-1	43
18	3	1	43
19	2	1	43
19	3	1	43
21	12	1	43
22	10	-1	43
25	6	-1	43
27	3	-1	43
31	10	-1	43
32	10	1	43
33	7	1	43
35	2	-1	43
36	5	1	43
37	5	-1	43
39	2	1	43
39	6	-1	43
39	13	1	43
40	4	1	43
40	9	-1	43
41	10	-1	43

ι	ν	ρ	p_i
4	9	1	43,127
5	2	1	43
6	8	1	43
15	7	-1	43
15	14	1	43
16	1	-1	43
16	11	-1	43
17	2	1	43
18	13	-1	43,127
21	9	1	43
27	4	-1	43
29	12	1	43
36	13	-1	43
37	3	-1	43
37	10	-1	43
39	9	1	43
40	7	1	43
41	13	1	43

ι	ν	ρ	p_i
1	6	1	43
1	7	-1	43
2	10	1	43
3	5	1	43
10	2	-1	43
10	9	1	43
11	8	-1	43
12	3	1	43
12	11	-1	43
13	7	-1	43
14	3	1	43
18	5	-1	43
21	2	-1	43
27	7	1	43
29	10	1	43
30	4	-1	43
31	3	1	43
32	5	1	43
33	4	1	43
33	6	-1	43
34	4	1	43,127
34	5	1	43
35	4	-1	43
35	9	-1	43
38	12	1	43
40	8	-1	43
42	7	1	43

Results for $m = 113 * 911$, fields K_{14}, K_{15} and K_{16}.

ι	ν	ρ	p_i
2	12	-1	43
6	9	1	43
7	9	-1	43
10	4	1	43
11	2	-1	43
12	1	-1	43
13	10	-1	43
14	4	1	43
21	13	1	43
23	1	1	43
24	12	1	43
26	1	-1	43
27	9	-1	43
30	4	1	43
33	2	1	43
33	10	1	43
35	11	1	43
36	3	-1	43
39	14	-1	43
40	14	-1	43
42	5	1	43
42	8	1	43,127

ι	ν	ρ	p_i
1	5	1	43
4	3	-1	43
4	4	1	43
5	1	-1	43
5	14	-1	43
16	5	-1	43
19	14	1	43
20	3	1	43
20	12	-1	43
21	3	-1	43
22	4	-1	43
25	3	-1	43
25	4	1	43
29	11	1	43
30	2	-1	43,127
31	7	-1	43
33	7	-1	43
33	10	-1	43
35	5	1	43
35	7	1	43
35	8	1	43
38	10	1	43
42	6	-1	43
42	14	-1	43

ι	ν	ρ	p_i
5	12	1	43
6	7	1	43
7	10	1	43
8	1	1	43
9	12	-1	43
10	2	1	43
11	7	-1	43
11	10	1	43
15	10	1	43
17	5	1	43
19	10	-1	43
22	3	-1	43
25	5	1	43
25	8	1	43
26	7	1	43
29	9	1	43
31	1	1	43
31	9	-1	43
35	12	-1	43
36	7	-1	43
39	8	1	43
39	10	-1	43
42	11	1	43,127

REFERENCES

[1] JAKUBEC, S.—KOSTRA, J.—NEMOGA, K.: *On the existence of an integral normal basis generated by a unit in prime extensions of rational numbers*, Math. Comp. **56** (1991), 809–815.

[2] JAKUBEC, S.—KOSTRA, J.: *A note on normal bases of ideals*, Math. Slovaca **42** (1992), 677–684.

Received July 16, 1997

* *IRAFM and Department of Mathematics*
University of Ostrava
Bráfova 7
CZ–701 03 Ostrava
CZECH REPUBLIC
E-mail: dvoraka@osu.cz

** *IRAFM*
University of Ostrava
Bráfova 7
CZ–701 03 Ostrava
CZECH REPUBLIC
E-mail: jedelsky@osu.cz

*** *Department of Mathematics*
University of Ostrava
Bráfova 7
CZ–701 03 Ostrava
CZECH REPUBLIC
E-mail: kostra@osu.cz