TOKYO J. MATH.
VOL. 16, NO. 2, 1993

On Unramified Galois Extensions of Certain Algebraic Number Fields

Kenzo KOMATSU and Takashi NODERA

Keio University

Abstract. Let $a \in \boldsymbol{Z}$ such that $a \neq 1$, $a \neq -2^{17}$ and $(17, a)=1$. Let $\alpha_1, \alpha_2, \cdots, \alpha_{17}$ denote the roots of $x^{17}+ax+a=0$. It is shown that every prime ideal is unramified in $\boldsymbol{Q}(\alpha_1, \alpha_2, \cdots, \alpha_{17})/\boldsymbol{Q}(\alpha_1)$ if and only if $a=2^{62}n^2+4605612312119580521n+1149886651258880054$ for some $n \in \boldsymbol{Z}$.

1. Introduction.

Let $l \equiv 1 \pmod 8$ denote a prime number, and let a denote a rational integer with $(l, a)=1$ such that

$$f(x)=x^l+ax+a$$

is irreducible over the rational number field $\boldsymbol{Q}$. If $(l-1)^{l-1}a+l^l$ is a square, then the Galois group of $f(x)=0$ over $\boldsymbol{Q}$ is a non-cyclic simple group, and every prime ideal is unramified in $\boldsymbol{Q}(\alpha_1, \alpha_2, \cdots, \alpha_l)/\boldsymbol{Q}(\alpha_1)$, where $\alpha_1, \alpha_2, \cdots, \alpha_l$ denote the roots of $f(x)=0$ ([3], Theorem 2). This leads to the following problem: Find all the integer solutions x, y of the equation

$$(l-1)^{l-1}x+l^l=y^2 . \tag{1.1}$$

In theory it is easy to solve (1.1). In practice the numbers $(l-1)^{l-1}$ and l^l are *so large* that one has to use computer even for the simplest case $l=17$. In the present paper we confine ourselves to the case $l=17$, and solve the Diophantine equation

$$16^{16}x+17^{17}=y^2 , \qquad y>0 . \tag{1.2}$$

Since the coefficient of x is a power of 2, our equation (1.2) has very simple structure, as we shall see in the next section.

2. Integer solutions of $16^{16}x+17^{17}=y^2$.

$\boldsymbol{Z}$ denotes the ring of rational integers.

THEOREM 1. *For each $n \in \boldsymbol{Z}$, let*

Received May 15, 1992

$$t_n=2^{62}n^2+b_0n+a_0\,,\qquad s_n=|\,2^{63}n+b_0\,|\,,$$

where the constants a_0 *and* b_0 *are defined by*

$$a_0=1149886651258880054\,,$$
$$b_0=4605612312119580521\,.$$

Then the integer solutions of the equation

$$16^{16}x+17^{17}=y^2\,,\qquad y>0 \tag{2.1}$$

are given by

$$\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}t_n\\s_n\end{pmatrix}\qquad (n=0,\ \pm1,\ \pm2,\ \cdots)\,.$$

The integers t_n $(n\in\boldsymbol{Z})$ *satisfy*

$$0<t_0<t_{-1}<t_1<t_{-2}<t_2<t_{-3}<t_3<\cdots\,. \tag{2.2}$$

Moreover, t_n *is divisible by* 17 *if and only if* $n\equiv5\pmod{17}$.

PROOF. Define y_i $(i=4,\ 5,\ \cdots,\ 64)$ by

$$y_4=1\,,$$
$$y_{i+1}=\begin{cases}2^{i-1}-y_i & \text{if}\quad (y_i^2-17^{17})/2^i \text{ is odd}\,,\\ y_i & \text{if}\quad (y_i^2-17^{17})/2^i \text{ is even}\,.\end{cases} \tag{2.3}$$

Then, by induction, we see that

$$\frac{y_i^2-17^{17}}{2^i}\in\boldsymbol{Z}\,,\qquad y_i\in\boldsymbol{Z}\quad\text{and}\quad 0<y_i<2^{i-2}\,. \tag{2.4}$$

We obtain

$$y_{64}=4605612312119580521=b_0\,,$$
$$\frac{y_{64}^2-17^{17}}{2^{64}}=1149886651258880054=a_0\,,$$

so that

$$2^{64}a_0+17^{17}=b_0^2\,. \tag{2.5}$$

For every $n\in\boldsymbol{Z}$, $\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}t_n\\s_n\end{pmatrix}$ is a solution of (2.1):

$$\begin{aligned}16^{16}t_n+17^{17}&=2^{126}n^2+2^{64}b_0n+2^{64}a_0+17^{17}\\&=2^{126}n^2+2^{64}nb_0+b_0^2\end{aligned} \tag{2.6}$$

$$=(2^{63}n+b_0)^2=s_n^2\,.$$

Conversely, suppose that

$$16^{16}x+17^{17}=y^2\,,\qquad y>0\,,\quad x\in\boldsymbol{Z}\,,\ y\in\boldsymbol{Z}\,.$$

Then, by (2.5),

$$2^{64}(x-a_0)=y^2-b_0^2=(y-b_0)(y+b_0)\,,$$

and so

$$2^{62}(x-a_0)=\frac{y-b_0}{2}\cdot\frac{y+b_0}{2}\,.$$

Clearly, y is odd. Since either $(y-b_0)/2$ or $(y+b_0)/2$ is odd, it follows that either $(y+b_0)/2$ or $(y-b_0)/2$ is divisible by 2^{62}. Hence

$$y+b_0=2^{63}k\quad\text{or}\quad y-b_0=2^{63}k$$

for some $k\in\boldsymbol{Z}$. Since $y>0$, we obtain $y=s_n$ for some $n\in\boldsymbol{Z}$, and so $x=t_n$.

Now we prove (2.2). In fact, for every $n\geq 0$, we have

$$t_{-(n+1)}-t_n=(2n+1)(2^{62}-b_0)>0\,,$$

since $b_0=y_{64}<2^{62}$. Clearly,

$$t_k-t_{-k}=2b_0k>0$$

for every $k>0$. Hence

$$t_0<t_{-1}<t_1<t_{-2}<t_2<\cdots\,.$$

The last assertion follows from the following congruences:

$$2^{62}\equiv 13\pmod{17}\,,\quad a_0\equiv 2\pmod{17}\,,\quad b_0\equiv 6\pmod{17}\,.$$ □

3. Irreducibility.

THEOREM 2. *Let $a\in\boldsymbol{Z}$. Then $f(x)=x^{17}+ax+a$ is irreducible over $\boldsymbol{Q}$ if and only if $a\neq 0$, $a\neq 1$ and $a\neq -2^{17}$.*

PROOF. It is easily seen that, if $a\neq k^{17}$ $(k\in\boldsymbol{Z})$, $f(x)$ is irreducible over $\boldsymbol{Q}$ ([2], Lemma 1). Suppose that $a=k^{17}$ $(k\in\boldsymbol{Z},\ k\neq 0)$. Then

$$f(x)=a((x/k)^{17}+k(x/k)+1)\,.$$

The irreducibility of $f(x)$ is equivalent to the irreducibility of

$$g(y)=y^{17}+ky+1\,.$$

If $|k|\geq 3$, $g(y)$ is irreducible ([4], Theorem 2). On the other hand, $y^{17}+y+1$ is divisible

by y^2+y+1; $y^{17}-y+1$ is irreducible; $y^{17}+2y+1$ is irreducible; $y^{17}-2y+1$ is divisible by $y-1$. This completes the proof. □

4. Unramified Galois extensions.

THEOREM 3. *Let $a\in\boldsymbol{Z}$ such that $a\neq 1$, $a\neq -2^{17}$ and $(17, a)=1$. Let $\alpha_1, \alpha_2, \cdots, \alpha_{17}$ denote the roots of*

$$f(x)=x^{17}+ax+a=0\,.$$

Then the following two statements are equivalent:

(1) *Every prime ideal is unramified in $\boldsymbol{Q}(\alpha_1, \alpha_2, \cdots, \alpha_{17})/\boldsymbol{Q}(\alpha_1)$;*

(2) $a=t_n=2^{62}n^2+4605612312119580521n+1149886651258880054$ *for some $n\in\boldsymbol{Z}$.*

PROOF. It follows from Theorem 2 that $f(x)$ is irreducible over $\boldsymbol{Q}$. Now the result follows from Theorem 1, [3] (Theorem 2) and [1] (Theorem 4). □

It is an open problem to determine the Galois groups of $x^{17}+t_nx+t_n=0$ over $\boldsymbol{Q}$ $(n=0, \pm 1, \pm 2, \cdots)$. The prime factors of the constants a_0 and b_0 (§2) are as follows:

$$a_0=2\cdot 13\cdot 2039\cdot 21690245053361\,. \tag{4.1}$$

$$b_0=313\cdot 14714416332650417\,. \tag{4.2}$$

References

[1] K. KOMATSU, Discriminants of certain algebraic number fields, J. Reine Angew. Math., **285** (1976), 114–125.

[2] K. KOMATSU, On certain homogeneous Diophantine equations of degree $n(n-1)$, Tokyo J. Math., **12** (1989), 231–234.

[3] K. KOMATSU, On the Galois group of $x^p+ax+a=0$, Tokyo J. Math., **14** (1991), 227–229.

[4] E. S. SELMER, On the irreducibility of certain trinomials, Math. Scand., **4** (1956), 287–302.

Present Address:
DEPARTMENT OF MATHEMATICS, KEIO UNIVERSITY
HIYOSHI, KOHOKU-KU, YOKOHAMA 223, JAPAN