Tohoku Math. J.
56 (2004), 367–370

THE RANK OF THE GROUP OF RELATIVE UNITS OF A GALOIS EXTENSION II

YOSHITAKA ODAI AND HIROSHI SUZUKI

(Received November 28, 2002)

Abstract. In the previous note [2] we calculated the rank of the group of relative units for a Galois extension of number fields. In this note the calculation is concluded.

1. Introduction. A finite extension of the rational number field in the complex number field will be called a number field. For a number field F, we denote by E_F (resp. W_F) the group of units of F (resp. the group of roots of unity in F). For an extension of number fields $L \supsetneq K$, we define

$$E_{L/K} = \{\varepsilon \in E_L \mid N_{L/M}(\varepsilon) \in W_M \text{ for all } M \text{ such that } K \subseteq M \subsetneq L\},$$

where $N_{L/M}$ is the relative norm mapping for L/M. The elements of $E_{L/K}$ are called relative units of L over K. The quotient group $\mathcal{E}_{L/K} = E_{L/K}/W_L$ is a free module over the rational integer ring $\boldsymbol{Z}$. In [2] we calculated the $\boldsymbol{Z}$-rank of $\mathcal{E}_{L/K}$ when L/K is a Galois extension. We denote by G the Galois group of L/K and by $\boldsymbol{R}[G]$ the group ring of G over the real number field $\boldsymbol{R}$. For a subgroup H of G, we denote by Tr_H the element $\sum_{h\in H} h$ of $\boldsymbol{R}[G]$. The left G-endomorphism $x \mapsto x \cdot \mathrm{Tr}_H$ of $\boldsymbol{R}[G]$ is also denoted by Tr_H. We put

$$n_G = \dim_{\boldsymbol{R}} \bigcap_{\{1\}\neq H\subseteq G} \mathrm{Ker}\ \mathrm{Tr}_H .$$

Then we have

$$\mathrm{rank}_{\boldsymbol{Z}} \mathcal{E}_{L/K} = s_{L/K}\, n_G ,$$

where $s_{L/K}$ denotes the number of infinite prime spots of K which are unramified in L (Proposition 1 of [2]).

In Theorem of [2], we have calculated n_G except when $G \cong SL(2, \boldsymbol{F}_p)$ and p is a Fermat prime bigger than 5 (cf. Remark in Section 3 of [2]), where $SL(2, \boldsymbol{F}_p)$ is the special linear group of degree 2 over the field $\boldsymbol{F}_p$ of p elements.

In this note we deal with this exceptional case and show the following:

THEOREM. *If G is isomorphic to $SL(2, \boldsymbol{F}_p)$ and p is a Fermat prime bigger than* 5, *then*

$$n_G = 0 .$$

2000 *Mathematics Subject Classification.* Primary 11R27; Secondary 20D99.

2. Preliminaries. For a finite group G, we denote by $\mathfrak{T}_G$ the left ideal of $\boldsymbol{R}[G]$ generated by $\{\mathrm{Tr}_H \mid \{1\} \neq H \subseteq G\}$. Then $\mathfrak{T}_G$ is a two-sided ideal because $\mathrm{Tr}_H \cdot g = g \cdot \mathrm{Tr}_{g^{-1}Hg}$ for $g \in G$. Furthermore, we have:

LEMMA 1 (Corollary to Proposition 1 of [2]).

$$n_G = |G| - \dim_{\boldsymbol{R}} \mathfrak{T}_G .$$

The following fact about conjugate classes of $SL(2, \boldsymbol{F}_p)$ is well known (e.g. Section 1 of Part I of [1]).

LEMMA 2. *Let p be an odd prime. For an element α of $\boldsymbol{F}_p$, we denote by $C(\alpha)$ the set of elements of $SL(2, \boldsymbol{F}_p)$ of trace α. If $\alpha \neq \pm 2$, then $C(\alpha)$ is a conjugate class of $SL(2, \boldsymbol{F}_p)$ and contains $p(p+1)$ or $p(p-1)$ elements according as $\alpha^2 - 4$ is a square or not in $\boldsymbol{F}_p$.*

When p is a Fermat prime bigger than 5, we can write $p = 2^{2^m}+1$ with $m \geq 2$. It implies p is congruent to 2 modulo 3, 1 modulo 4, and 2 modulo 5. Then the following calculation of Legendre's symbols is obtained:

$$\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1 , \quad \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1 .$$

Therefore we have:

LEMMA 3. *Let p be a Fermat prime bigger than 5. Then neither -3 nor 5 is a square in $\boldsymbol{F}_p$.*

3. Poof of the Theorem. Let G be $SL(2, \boldsymbol{F}_p)$ and p a Fermat prime bigger than 5. We denote by T the subgroup of G generated by

$$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} .$$

Then we have

$$\mathrm{Tr}_T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} .$$

Because the second and third terms are of trace -1 and $(-1)^2 - 4 = -3$ is not a square in $\boldsymbol{F}_p$, Lemma 2 implies

$$\frac{1}{|G|} \sum_{g \in G} g^{-1} (\mathrm{Tr}_T) g = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{2}{p(p-1)} \sum_{a \in C(-1)} a . \tag{1}$$

Because Lemma 3 implies -15 is a square in $\boldsymbol{F}_p$, we denote by $\sqrt{-15}$ a square root of -15. Then the matrix

$$g_0 = \begin{pmatrix} \frac{1+\sqrt{-15}}{4} & \frac{3+\sqrt{-15}}{4} \\ 0 & \frac{1-\sqrt{-15}}{4} \end{pmatrix}$$

is an element of G and we have

$$g_0\mathrm{Tr}_T = \begin{pmatrix} \frac{1+\sqrt{-15}}{4} & \frac{3+\sqrt{-15}}{4} \\ 0 & \frac{1-\sqrt{-15}}{4} \end{pmatrix} + \begin{pmatrix} \frac{1}{2} & -\frac{1+\sqrt{-15}}{4} \\ \frac{1-\sqrt{-15}}{4} & 0 \end{pmatrix}$$

$$+ \begin{pmatrix} -\frac{3+\sqrt{-15}}{4} & -\frac{1}{2} \\ -\frac{1-\sqrt{-15}}{4} & -\frac{1-\sqrt{-15}}{4} \end{pmatrix} .$$

The first and second terms are of trace $1/2$ and the third term is of trace -1. Because $(1/2)^2 - 4 = -15/4$ is a square in $\boldsymbol{F}_p$, Lemma 2 implies

$$\text{(2)} \qquad \frac{1}{|G|}\sum_{g\in G} g^{-1}(g_0\mathrm{Tr}_T)g = \frac{2}{p(p+1)}\sum_{a\in C(1/2)} a + \frac{1}{p(p-1)}\sum_{a\in C(-1)} a .$$

We denote by P the subgroup of G generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} .$$

Then we have

$$g_0\mathrm{Tr}_P = \sum_{\alpha\in \boldsymbol{F}_p} \begin{pmatrix} \frac{1+\sqrt{-15}}{4} & \alpha \\ 0 & \frac{1-\sqrt{-15}}{4} \end{pmatrix} .$$

Because all terms are of trace $1/2$, Lemma 2 implies

$$\text{(3)} \qquad \frac{1}{|G|}\sum_{g\in G} g^{-1}(g_0\mathrm{Tr}_P)g = \frac{1}{(p+1)}\sum_{a\in C(1/2)} a .$$

Now we put

$$x_0 = \mathrm{Tr}_T - 2g_0\mathrm{Tr}_T + \frac{4}{p} g_0\mathrm{Tr}_P ,$$

which is an element of $\mathfrak{T}_G$. Then (1), (2) and (3) imply

$$\frac{1}{|G|}\sum_{g\in G} g^{-1}x_0 g = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} .$$

Because the left side is an element of the two-sided ideal $\mathfrak{T}_G$, so is the right side. It implies $\mathfrak{T}_G = \boldsymbol{R}[G]$. Therefore we see from Lemma 1 that $n_G = 0$. The proof of the Theorem is complete.

REFERENCES

[1] H. E. JORDAN, Group-characters of various types of linear groups, Amer. J. Math. 29 (1907), 387–405.

[2] Y. ODAI AND H. SUZUKI, The rank of the group of relative units of a Galois extension, Tohoku Math. J. 53 (2001), 37–54.

FACULTY OF HUMANITIES AND SOCIAL SCIENCES
IWATE UNIVERSITY
MORIOKA 020–8550
JAPAN

GRADUATE SCHOOL OF MATHEMATICS
NAGOYA UNIVERSITY
NAGOYA 464–8602
JAPAN