Tohoku Math. J.
53 (2001), 37–54

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

YOSHITAKA ODAI AND HIROSHI SUZUKI

(Received November 27, 1998, revised July 10, 2000)

Abstract. For an extension of number fields, we define the group of relative units, and determine its rank when the extension is a Galois extension. For this purpose we need to determine all the finite groups of which every abelian subgroup is cyclic.

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

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

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 $\mathbf{Z}$. The statement (ii) of Theorem in [1] implies that $\operatorname{rank}_{\mathbf{Z}} \mathcal{E}_{L/K} = s_{L/K}\varphi([L : K])$ if L/K is cyclic, where φ is Euler's function and $s_{L/K}$ denotes the number of infinite prime spots of K which are unramified in L. Moreover, by using the statement (i) of the theorem, we easily see that $\operatorname{rank}_{\mathbf{Z}} \mathcal{E}_{L/K} = 0$ if L/K is non-cyclic abelian. Hence the rank is completely known when L/K is abelian. In this paper we determine the rank when L/K is a Galois extension.

For two finite groups A and B, we denote by $A \ltimes B$ a semi-direct product of A and B with A acting on B and by $A \times B$ the direct product of A and B. Let $\mathbf{Z}/n\mathbf{Z}$ denote the cyclic group of order n and D_n the dihedral group of order n. Let Q_n denote the generalized quaternion group of order n, where n is a power of 2 and $n \geq 8$. Let $SL(2, \boldsymbol{F}_q)$ denote the special linear group of degree 2 over the field $\boldsymbol{F}_q$ of q elements. Let H_p be the subgroup of $SL(2, \boldsymbol{F}_{p^2})$ defined by

$$H_p = \left\langle \begin{pmatrix} \sqrt{\omega} & 0 \\ 0 & \sqrt{\omega}^{-1} \end{pmatrix}, SL(2, \boldsymbol{F}_p) \right\rangle,$$

where p is an odd prime and ω is a generator of the multiplicative group of $\boldsymbol{F}_p$. Furthermore, let

$$H_{3,m} = \{(g, h) \in H_3 \times D_{2\cdot 3^m} \mid \phi(g) = \psi(h)\},$$

where $m \geq 1$ and ϕ (resp. ψ) is an epimorphism of H_3 (resp. $D_{2\cdot 3^m}$) to D_6.

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

DEFINITION. If a finite group G satisfies the conditions (1), (2) and (3-i) in Table 1, then G is said to be of Type i ($i = \mathrm{I}, \mathrm{II}, \ldots, \mathrm{VI}$).

TABLE 1

(1)	$G \cong (\mathfrak{G} \times C_1) \ltimes C_2$, where C_1 and C_2 are cyclic groups such that $(\lvert C_1\rvert, \lvert C_2\rvert) = (\lvert C_1\rvert \lvert C_2\rvert, \lvert\mathfrak{G}\rvert) = 1$.
(2)	Every element of prime order of $\mathfrak{G} \times C_1$ acts trivially on C_2.
(3-I)	$\mathfrak{G} \cong \{1\}$.
(3-II)	$\mathfrak{G} \cong Q_n$.
(3-III)	$\mathfrak{G} \cong \boldsymbol{Z}/3^m\boldsymbol{Z} \ltimes Q_8$ (non-direct) ($m \geq 1$).
(3-IV)	$\mathfrak{G} \cong H_{3,m}$ ($m \geq 1$).
(3-V)	$\mathfrak{G} \cong SL(2, \boldsymbol{F}_p)$ (p is a Fermat prime, $p \geq 5$).
(3-VI)	$\mathfrak{G} \cong H_p$ (p is a Fermat prime, $p \geq 5$).

Then we have the following theorem.

THEOREM. *Suppose that L/K is a Galois extension and denote by G the Galois group of L/K. Let φ be Euler's function and $s_{L/K}$ denote the number of infinite prime spots of K which are unramified in L. Then we have*

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

where

$$n_G = \begin{cases} \varphi(|G|) & \text{if } G \text{ is of Type I, II, III } (m \geq 2) \text{ or IV } (m \geq 2), \\ \dfrac{1}{2}\varphi(|G|) & \text{if } G \text{ is of Type III } (m = 1) \text{ or IV } (m = 1), \\ \dfrac{n_{SL(2,\boldsymbol{F}_p)}}{\varphi(|SL(2,\boldsymbol{F}_p)|)}\varphi(|G|) & \text{if } G \text{ is of Type V or VI}, \\ 0 & \text{otherwise}. \end{cases}$$

REMARK. If G is cyclic, then it is of Type I because an action of C_1 on C_2 may be trivial. In this case the Theorem implies that $\mathrm{rank}_{\boldsymbol{Z}}\mathcal{E}_{L/K} = s_{L/K}\varphi(|G|)$. If G is non-cyclic abelian, then it is not of any of Types I–VI (cf. Proposition 2). In this case, therefore, the Theorem implies that $\mathrm{rank}_{\boldsymbol{Z}}\mathcal{E}_{L/K} = 0$. Hence this is a generalization of the result in the abelian case.

This paper is organized as follows. In Section 1 an expression of n_G in terms of the group ring of G is obtained (Proposition 1). In Section 2 two simple sufficient conditions for $n_G = 0$ are given. Then they give a necessary condition for $n_G \neq 0$, which is equivalent to that G is of one of Types I–VI (Proposition 2). It seems remarkable that a modification of Proposition 2 determines all the finite groups of which every abelian subgroup is cyclic (Proposition 2′). In Section 3 we calculate n_G for G of each type and complete the proof of the Theorem. We also remark on $n_{SL(2,\boldsymbol{F}_p)}$ for Fermat primes $p \geq 5$.

1. Expression of n_G in terms of the group ring of G. For an infinite prime spot $\mathfrak{P}$ of a number field F, we denote by $F_{\mathfrak{P}}$ the completion of F with respect to $\mathfrak{P}$; namely, $F_{\mathfrak{P}}$ is the real number field $\boldsymbol{R}$ or the complex number field $\boldsymbol{C}$ according as $\mathfrak{P}$ is real or imaginary. We denote by $F_{\mathfrak{P}}^{\times}$ the multiplicative group of $F_{\mathfrak{P}}$ and define

$$[F]_{\mathfrak{P}} = F_{\mathfrak{P}}^{\times}/\{a \in F_{\mathfrak{P}}^{\times} \mid |a| = 1\},$$

where $|a|$ denotes the absolute value of a. Since $[F]_{\mathfrak{P}}$ is always isomorphic to $\boldsymbol{R}^{\times}/\{\pm 1\}$, it is regarded as an $\boldsymbol{R}$-module by exponentiation. For an infinite prime spot $\mathfrak{p}$ of a subfield of F, we define

$$[F]_{\mathfrak{p}} = \bigoplus_{\mathfrak{P}|\mathfrak{p}} [F]_{\mathfrak{P}},$$

where $\mathfrak{P}$ runs over the infinite prime spots of L above $\mathfrak{p}$. We denote by ∞ the infinite prime spot of the rational number field and consider a monomorphism

$$\Psi_F : E_F/W_F \ni \varepsilon \mapsto \bigoplus_{\mathfrak{P}|\infty} |\varepsilon_{\mathfrak{P}}|^{\nu_{\mathfrak{P}}} \in [F]_{\infty},$$

where $\varepsilon_{\mathfrak{P}}$ is the conjugate of ε corresponding to $\mathfrak{P}$, and $\nu_{\mathfrak{P}}$ is equal to 1 or 2 according as $\mathfrak{P}$ is real or imaginary.

Let $L \supsetneq K$ be an extension of number fields. For $K \subseteq M \subsetneq L$, we regard the relative norm mapping $N_{L/M}$ as a mapping of E_L/W_L to E_M/W_M. Then the definition of $\mathcal{E}_{L/K}$ implies that

$$\mathcal{E}_{L/K} = \bigcap_{K \subseteq M \subsetneq L} \mathrm{Ker}(N_{L/M} : E_L/W_L \to E_M/W_M),$$

where Ker $*$ denotes the kernel of $*$. We may also regard $N_{L/M}$ as a mapping of $[L]_{\infty}$ to $[M]_{\infty}$, namely,

$$N_{L/M} : [L]_{\infty} \ni \bigoplus_{\mathfrak{P}|\infty} x_{\mathfrak{P}} \mapsto \bigoplus_{\mathfrak{p}|\infty} (\Pi_{\mathfrak{P}|\mathfrak{p}} x_{\mathfrak{P}}) \in [M]_{\infty},$$

where $\mathfrak{p}$ runs over the infinite prime spots of M. Since

$$\Psi_M \circ (N_{L/M} : E_L/W_L \to E_M/W_M) = (N_{L/M} : [L]_{\infty} \to [M]_{\infty}) \circ \Psi_L,$$

we see that

$$\Psi_L(\mathrm{Ker}(N_{L/M} : E_L/W_L \to E_M/W_M)) \subset \mathrm{Ker}(N_{L/M} : [L]_{\infty} \to [M]_{\infty}).$$

By comparing the dimensions, we have

$$\mathrm{Ker}(N_{L/M} : E_L/W_L \to E_M/W_M) \otimes_{\boldsymbol{Z}} \boldsymbol{R} \cong \mathrm{Ker}(N_{L/M} : [L]_{\infty} \to [M]_{\infty}).$$

Moreover, $N_{L/M}$ can be regarded also as a mapping $[L]_{\mathfrak{p}}$ to $[M]_{\mathfrak{p}}$ for an infinite prime spot $\mathfrak{p}$ of K. Hence we have

$$\mathrm{Ker}(N_{L/M} : [L]_{\infty} \to [M]_{\infty}) = \bigoplus_{\mathfrak{p}|\infty} \mathrm{Ker}(N_{L/M} : [L]_{\mathfrak{p}} \to [M]_{\mathfrak{p}}),$$

where $\mathfrak{p}$ runs over the infinite prime spots of K. Consequently, we have the following lemma.

LEMMA 1.

$$\mathcal{E}_{L/K} \otimes_{\boldsymbol{Z}} \boldsymbol{R} \cong \bigoplus_{\mathfrak{p}|\infty} \left(\bigcap_{K \subseteq M \subsetneq L} \mathrm{Ker}(N_{L/M} : [L]_{\mathfrak{p}} \to [M]_{\mathfrak{p}}) \right),$$

where $\mathfrak{p}$ *runs over the infinite prime spots of* K.

For a finite group G we denote by $\boldsymbol{R}[G]$ the group ring of G over $\boldsymbol{R}$. 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. Then we have:

PROPOSITION 1. *Suppose that* L/K *is a Galois extension and denote by* G *the Galois group of* L/K. *Let* $s_{L/K}$ *denote the number of infinite prime spots of* K *which are unramified in* L. *Then*

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

where

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

PROOF. Lemma 1 says that

$$\mathrm{rank}_{\boldsymbol{Z}} \mathcal{E}_{L/K} = \sum_{\mathfrak{p}|\infty} \dim_{\boldsymbol{R}} \left(\bigcap_{K \subseteq M \subsetneq L} \mathrm{Ker}(N_{L/M} : [L]_{\mathfrak{p}} \to [M]_{\mathfrak{p}}) \right), \tag{1}$$

where $\mathfrak{p}$ runs over the infinite prime spots of K.

We first consider the case where $\mathfrak{p}$ ramifies in L. Let $\{\mathfrak{P}_i\}_{1 \le i \le |G|/2}$ be the infinite prime spots of L above $\mathfrak{p}$. We denote by M_i the decomposition field of $\mathfrak{P}_i$ and by $\mathfrak{p}_i$ the infinite prime spot of M_i below $\mathfrak{P}_i$. We note that $[L]_{\mathfrak{p}_i} = [L]_{\mathfrak{P}_i} = \boldsymbol{C}^{\times}/\{z \in \boldsymbol{C}^{\times} \mid |z| = 1\}$ and $[M_i]_{\mathfrak{p}_i} = \boldsymbol{R}^{\times}/\{\pm 1\}$. Since the norm mapping $N_{\boldsymbol{C}/\boldsymbol{R}} : \boldsymbol{C}^{\times}/\{z \in \boldsymbol{C}^{\times} \mid |z| = 1\} \to \boldsymbol{R}^{\times}/\{\pm 1\}$ is isomorphic, we have

$$\mathrm{Ker}(N_{L/M_i} : [L]_{\mathfrak{p}_i} \to [M_i]_{\mathfrak{p}_i}) = \{1\},$$

which implies that

$$[L]_{\mathfrak{p}_i} \cap \mathrm{Ker}(N_{L/M_i} : [L]_{\mathfrak{p}} \to [M_i]_{\mathfrak{p}}) = \{1\}.$$

Since $[L]_{\mathfrak{p}} = \bigoplus_i [L]_{\mathfrak{P}_i} = \bigoplus_i [L]_{\mathfrak{p}_i}$, we have

$$\bigcap_{K \subseteq M \subsetneq L} \mathrm{Ker}(N_{L/M} : [L]_{\mathfrak{p}} \to [M]_{\mathfrak{p}}) = \{1\}. \tag{2}$$

Secondly, we consider the case where $\mathfrak{p}$ is unramified in L. Let $\{\mathfrak{P}_i\}_{1 \le i \le |G|}$ be the infinite prime spots of L above $\mathfrak{p}$. We put $\mathfrak{P} = \mathfrak{P}_1$. Then we see that $\{\mathfrak{P}_i\}_{1 \le i \le |G|} = \{\mathfrak{P}^g\}_{g \in G}$ and that any element of $[L]_{\mathfrak{p}}$ is written in the form $\bigoplus_{g \in G} x_{\mathfrak{P}^g}$, where $x_{\mathfrak{P}^g} \in [L]_{\mathfrak{P}^g}$. If we consider the action of G on $[L]_{\mathfrak{p}}$ defined by

$$\left(\bigoplus_{g \in G} x_{\mathfrak{P}^g} \right)^h = \bigoplus_{g \in G} x_{\mathfrak{P}^{gh^{-1}}} \quad \text{for } h \in G ,$$

then we have a G-isomorphism of $[L]_{\mathfrak{p}}$ to the right G-module $\boldsymbol{R}[G]$:

$$\bigoplus_{g\in G} x_{\mathfrak{P}^g} \mapsto \sum_{g\in G} (\log |x_{\mathfrak{P}^g}|) g\,.$$

Therefore we know

$$\bigcap_{K\subseteq M\subsetneq L} \operatorname{Ker}(N_{L/M} : [L]_{\mathfrak{p}} \to [M]_{\mathfrak{p}}) \cong \bigcap_{\{1\}\neq H\subseteq G} \operatorname{Ker} \operatorname{Tr}_H\,. \tag{3}$$

Consequently, (1), (2) and (3) prove Proposition 1.

We know that $\boldsymbol{R}[G]$ is a Hilbert space with respect to the inner product $(\sum_{g\in G} a_g g, \sum_{g\in G} b_g g) = \sum_{g\in G} a_g b_g$. Since

$$\operatorname{Ker} \operatorname{Tr}_H = \left\{ \sum_{g\in G} a_g g \,\middle|\, \sum_{g\in C} a_g = 0 \text{ for any } C \in G/H \right\},$$

we have from the definition of orthogonal complement that

$$(\operatorname{Ker} \operatorname{Tr}_H)^{\perp} = \left\{ \sum_{g\in G} a_g g \,\middle|\, a_g = a_h \text{ if } g \in hH \right\} = (\operatorname{Tr}_H)_{\boldsymbol{R}[G]}\,,$$

where $(*)_{\boldsymbol{R}[G]}$ denotes the left ideal of $\boldsymbol{R}[G]$ generated by $*$. Hence

$$\left(\bigcap_{\{1\}\neq H\subseteq G} \operatorname{Ker} \operatorname{Tr}_H \right)^{\perp} = (\operatorname{Tr}_H \mid \{1\} \neq H \subseteq G)_{\boldsymbol{R}[G]}\,.$$

Therefore n_G is expressed as follows:

COROLLARY. *Let the assumptions and notation be as in* Proposition 1. *Then*

$$n_G = |G| - t_G\,,$$

where

$$t_G = \dim_{\boldsymbol{R}} (\operatorname{Tr}_H \mid \{1\} \neq H \subseteq G)_{\boldsymbol{R}[G]}\,.$$

2. Necessary condition for $n_G \neq 0$. We start with two simple examples, where the notation is as in the preceding section.

EXAMPLE 1. If a direct product $\boldsymbol{Z}/l\boldsymbol{Z} \times \boldsymbol{Z}/l\boldsymbol{Z}$ is contained in G for some prime l, then $1 \in (\operatorname{Tr}_H \mid \{1\} \neq H \subseteq G)_{\boldsymbol{R}[G]}$, because the equation

$$1 = -\frac{1}{l} \left(\operatorname{Tr}_{\boldsymbol{Z}/l\boldsymbol{Z}\times\boldsymbol{Z}/l\boldsymbol{Z}} - \sum_{\{1\}\neq H\subsetneq \boldsymbol{Z}/l\boldsymbol{Z}\times\boldsymbol{Z}/l\boldsymbol{Z}} \operatorname{Tr}_H \right)$$

holds. It implies that $t_G = |G|$ and $n_G = 0$.

EXAMPLE 2. If a non-direct semi-direct product $\mathbf{Z}/l_1\mathbf{Z} \ltimes \mathbf{Z}/l_2\mathbf{Z}$ is contained in G for a pair of primes l_1 and l_2, then $1 \in (\mathrm{Tr}_H \mid \{1\} \neq H \subseteq G)_{\boldsymbol{R}[G]}$, because the equation

$$1 = -\frac{1}{l_2}\left(\mathrm{Tr}_{\mathbf{Z}/l_1\mathbf{Z}\ltimes\mathbf{Z}/l_2\mathbf{Z}} - \sum_{\{1\}\neq H\subsetneq \mathbf{Z}/l_1\mathbf{Z}\ltimes\mathbf{Z}/l_2\mathbf{Z}} \mathrm{Tr}_H\right)$$

holds. It implies that $t_G = |G|$ and $n_G = 0$.

Now we are interested in finite groups which are different from the above examples. The following proposition is the most important part of the proof of the Theorem.

PROPOSITION 2. *For a finite group G the following two conditions are equivalent*:

(i) *G contains neither a direct product $\mathbf{Z}/l\mathbf{Z} \times \mathbf{Z}/l\mathbf{Z}$ for a prime l nor a non-direct semi-direct product $\mathbf{Z}/l_1\mathbf{Z} \ltimes \mathbf{Z}/l_2\mathbf{Z}$ for a pair of primes l_1 and l_2.*

(ii) *G is of one of Types* I–VI.

The rest of the section is devoted to the proof of Proposition 2.

2.1. Let the notation be as in Introduction. We prove three lemmas for the proof of Proposition 2. For a finite group G we denote by $Z(G)$ the center of G. For a prime l we denote by $S_l(G)$ a Sylow l-subgroup of G. We write $H \lhd G$ (resp. H char G) when H is a normal (resp. characteristic) subgroup of G.

LEMMA 2. *Let G be a finite group and H a normal subgroup of G. Suppose that $S_l(G/H) \lhd G/H$ for a prime l. If one of the following two conditions is satisfied, then $S_l(G) \lhd G$*:

(i) *The order of H is a power of l.*

(ii) *The order of H is not divisible by l and $H \subset Z(G)$.*

PROOF. Since $S_l(G)H/H$ is a Sylow l-subgroup of G/H, our assumption implies that $S_l(G)H/H \lhd G/H$, which is equivalent to $S_l(G)H \lhd G$. Since the condition (i) implies that $S_l(G) = S_l(G)H$ and (ii) implies that $S_l(G)$ char $S_l(G)H$, we have $S_l(G) \lhd G$.

For a finite group G we denote by Aut G (resp. Inn G) the group of automorphisms (resp. inner automorphisms) of G.

LEMMA 3. *Let*

$$1 \to A \to B \to C \times D \to 1$$

be an exact sequence of finite groups. Suppose that $(|A|\,|C|, |D|) = 1$. If one of the following two conditions is satisfied, then $B \cong B' \times D$, where

$$1 \to A \to B' \to C \to 1$$

is an exact sequence:

(i) $A \subset Z(B)$.

(ii) $(|\mathrm{Aut}\, A|, |D|) = 1$.

PROOF. The exact sequence $1 \to A \to B \to C \times D \to 1$ gives an exact sequence $1 \to A \to B_1 \to D \to 1$, where B_1 is the inverse image of D. Since $(|A|, |D|) = 1$, the condition

(i) or (ii) implies that $B_1 \cong A \times D$ and that B_1 has a characteristic subgroup isomorphic to D. It implies that B has a normal subgroup isomorphic to D. Since $(|B/D|, |D|) = (|A|\,|C|, |D|) = 1$, we have $B \cong B' \ltimes D$, where $B' \cong B/D$. By restricting the exact sequence $1 \to A \to B \to C \times D \to 1$ to B', we have an exact sequence $1 \to A \to B' \to C \to 1$. Two exact sequences $1 \to A \to B' \to C \to 1$ and $1 \to A \to B_1 \to D \to 1$ imply that the action of B' on B_1 is trivial modulo A, because that of C on D is trivial. In particular, for $b \in B'$ and $d \in D \subset B_1$, there exists $a \in A$ such that $b^{-1}db = da$. Since $(|A|, |D|) = 1$, the condition (i) or (ii) implies that (the order of da)=(the order of d)$\times$(the order of a). Since $b^{-1}db$ has the same order as d, we have $a = 1$. It implies that $B \cong B' \times D$.

We denote by $PGL(2, \boldsymbol{F}_p)$ (resp. $PSL(2, \boldsymbol{F}_p)$) the projective general (resp. special) linear group of degree 2 over $\boldsymbol{F}_p$. For a finite group G we denote by G^c the commutator subgroup of G.

LEMMA 4. *Let*

$$1 \to \mathbf{Z}/2\mathbf{Z} \to A \to B \to 1$$

be an exact sequence of finite groups. Suppose that a direct product $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ *is not contained in A. Let p be an odd prime.*

(i) *If* $B \cong PSL(2, \boldsymbol{F}_p)$, *then* $A \cong SL(2, \boldsymbol{F}_p)$.

(ii) *If* $B \cong PGL(2, \boldsymbol{F}_p)$, *then* $A \cong H_p$.

PROOF. The image of $\mathbf{Z}/2\mathbf{Z}$ is contained in $Z(A)$, because it is normal. Then the above assumption is equivalent to that A has a unique subgroup of order 2, which we denote by Z. We have an exact sequence $1 \to Z \to A \to B \to 1$.

(i) If $p > 3$, then we know that $PSL(2, \boldsymbol{F}_p)$ is a non-abelian simple group (Corollary to (9.10), Chapter 1, [2]). The order of A^c is divisible by that of $PSL(2, \boldsymbol{F}_p)^c = PSL(2, \boldsymbol{F}_p)$, and hence is even. Then the uniqueness of Z implies $Z \subset A^c$. Therefore the restriction of the above exact sequence to A^c induces $A^c = A$. The statement (3) of Theorem 9.18 in Chapter 2 of [2] implies that the central extension A is irreducible. Since the multiplier of $SL(2, \boldsymbol{F}_p)$ is trivial (Example 2, Section 9, Chapter 2, [2]), the statement (6) of the theorem implies that the multiplier of $PSL(2, \boldsymbol{F}_p)$ is of order 2. Then we know that the central extension A is primitive (Definition 9.10, Chapter 2, [2]). Hence the statement (5) of the theorem implies that A is uniquely determined. Since $SL(2, \boldsymbol{F}_p)$ clearly satisfies the condition on A, we have $A \cong SL(2, \boldsymbol{F}_p)$. If $p = 3$, we know that $PSL(2, \boldsymbol{F}_3) \cong \mathbf{Z}/3\mathbf{Z} \ltimes (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})$ (non-direct). Since Lemma 2 implies $S_2(A) \lhd A$ and the assumption of the lemma implies $S_2(A) \cong Q_8$, we have $A \cong \mathbf{Z}/3\mathbf{Z} \ltimes Q_8$ (non-direct) $\cong SL(2, \boldsymbol{F}_3)$.

(ii) The exact sequence $1 \to Z \to A \to PGL(2, \boldsymbol{F}_p) \to 1$ gives an exact sequence $1 \to Z \to A_1 \to PSL(2, \boldsymbol{F}_p) \to 1$, where A_1 is a subgroup of A of index 2 defined as the inverse image of $PSL(2, \boldsymbol{F}_p)$. Then A is generated by A_1 and an element a which does not belong to A_1. Since (i) implies $A_1 \cong SL(2, \boldsymbol{F}_p)$, two elements a_1 and a_2 of order p generate A_1. For example, we can take

$$a_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

We note that $a^{-1}a_i a$ is determined up to an element of Z. Since $Z \subset Z(A)$ and $(|Z|, p) = 1$, by considering the order, we see that $a^{-1}a_i a$ is uniquely determined and that A is uniquely determined. On the other hand, it is easily proved that H_p has a unique subgroup Z of order 2 such that $H_p/Z \cong PGL(2, \boldsymbol{F}_p)$, namely,

$$Z = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle .$$

Therefore we have $A \cong H_p$.

COROLLARY. *For a prime $p > 3$,*

$$H_p^c = SL(2, \boldsymbol{F}_p)^c = SL(2, \boldsymbol{F}_p) .$$

PROOF. The identity $SL(2, \boldsymbol{F}_p)^c = SL(2, \boldsymbol{F}_p)$ has been seen in the proof of (i) of Lemma 4. Since $H_p/SL(2, \boldsymbol{F}_p) \cong \boldsymbol{Z}/2\boldsymbol{Z}$, we have $H_p^c \subset SL(2, \boldsymbol{F}_p)$, which implies $H_p^c = SL(2, \boldsymbol{F}_p)$.

2.2. We suppose that a finite group G satisfies the condition (i) of Proposition 2. Since any direct product $\boldsymbol{Z}/l\boldsymbol{Z} \times \boldsymbol{Z}/l\boldsymbol{Z}$ for a prime l is not contained in G, every abelian subgroup of G is cyclic. Then the statement (4.4) in Chapter 4 of [2] implies that $S_l(G)$ is cyclic or isomorphic to Q_n. Moreover, if A is a subgroup or a quotient group of G, then $S_l(A)$ is cyclic for any odd prime l. Similarly, if A is a subgroup of G, then $S_2(A)$ is cyclic or isomorphic to Q_n. In this section we denote by F the Fitting subgroup (i.e., the maximal nilpotent normal subgroup) of G. Since F is nilpotent, it is a direct product of its Sylow subgroups (Theorem 2.12, Chapter 4, [2]). For a natural number n, we put $F_n = \prod_{(l,n)=1} S_l(F)$. Then we can write $F = S_2(F) \times F_2$. Since $S_l(F)$ is cyclic for each odd prime l, we see that F_2 is cyclic, and hence $Z(F) = Z(S_2(F)) \times F_2$.

By inner automorphisms of G, we obtain a homomorphism of G to $\operatorname{Aut} F$. If G is solvable, then the kernel of the homomorphism is equal to $Z(F)$ (Corollary to Theorem 2.18, Chapter 4, [2]). Therefore we can regard the homomorphism as a monomorphism of $G/Z(F)$ to $\operatorname{Aut} F$. Since $(|S_2(F)|, |F_2|) = 1$, we have $\operatorname{Aut} F = \operatorname{Aut} S_2(F) \times \operatorname{Aut} F_2$, where $\operatorname{Aut} F_2$ is abelian because F_2 is cyclic. Now we define a homomorphism

$$\Phi : G/Z(F) \hookrightarrow \operatorname{Aut} F \xrightarrow{\text{projection}} \operatorname{Aut} S_2(F) .$$

We denote by $\operatorname{Im}\Phi$ (resp. $\operatorname{Ker}\Phi$) the image (resp. kernel) of Φ. Then the above monomorphism implies $G/Z(F) \hookrightarrow \operatorname{Im}\Phi \times \operatorname{Aut} F_2$.

The case where G is solvable and $\operatorname{Im}\Phi$ is a 2-group is treated in Section 2.3. The case where G is solvable and $\operatorname{Im}\Phi$ is not a 2-group is treated in Section 2.4. The case where G is non-solvable is treated in Section 2.5.

2.3. We suppose that a finite solvable group G satisfies the condition (i) of Proposition 2 and that $\operatorname{Im}\Phi$ is a 2-group. Since both $\operatorname{Im}\Phi$ and $\operatorname{Aut} F_2$ are nilpotent, so is $\operatorname{Im}\Phi \times \operatorname{Aut} F_2$. Since $G/Z(F) \hookrightarrow \operatorname{Im}\Phi \times \operatorname{Aut} F_2$, we see that $G/Z(F)$ is nilpotent.

Since $\operatorname{Im}\Phi$ is a 2-group, the number of G-conjugates of a subgroup of $S_2(F)$ is a power of 2. On the other hand, the number of subgroups of $Z(S_2(F))$ of index 2 is odd

because $Z(S_2(F))$ is an abelian 2-group. Therefore there exists a G-invariant subgroup E_1 of $Z(S_2(F))$ of index 2. Moreover we can prove recursively that there exists a series of G-invariant subgroups

$$Z(S_2(F)) = E_0 \supset E_1 \supset E_2 \supset \cdots \supset E_{t-1} \supset E_t = \{1\},$$

where the index of E_i in E_{i-1} is 2. Then $G/(E_i \times F)$ is an extension of $G/(E_{i-1} \times F)$ by $\boldsymbol{Z}/2\boldsymbol{Z}$, which is automatically central. Therefore the fact that $G/Z(F) \cong G/(E_0 \times F_2)$ is nilpotent implies that $G/F_2 \cong G/(E_t \times F_2)$ is nilpotent.

We put $k = |G/F_2|$. Then we have the following lemma.

LEMMA 5.

$$1 \to F_2/F_{2k} \to G/F_{2k} \to G/F_2 \to 1$$

is a central extension

PROOF. Since F_2 is abelian, an action of G/F_{2k} on F_2/F_{2k} is determined by that of G/F_2 on F_2/F_{2k}. Since $F_2/F_{2k} \cong \prod_l S_l(F)$, where l runs over the odd prime divisors of k, it suffices to show that G/F_2 acts trivially on $S_l(F)$ for all those l. Since G/F_2 is nilpotent and $S_l(G/F_2)$ is cyclic, we have $S_l(G/F_2) \subset Z(G/F_2)$ and that the homomorphism of G/F_2 to $\mathrm{Aut}\, S_l(G/F_2)$ induced by inner automorphisms is trivial. Since $S_l(G/F_2) \lhd G/F_2$ and F_2/F_{2l} is an l-group, Lemma 2 implies that $S_l(G/F_{2l}) \lhd G/F_{2l}$. We denote by μ the homomorphism of G/F_{2l} to $\mathrm{Aut}\, S_l(G/F_{2l})$ induced by inner automorphisms and by ν the epimorphism of $\mathrm{Aut}\, S_l(G/F_{2l})$ to $\mathrm{Aut}\, S_l(G/F_2)$ induced by considering modulo F_2/F_{2l}. Then the following diagram is commutative.

$$\begin{array}{ccc} G/F_{2l} & \xrightarrow{\mu} & \mathrm{Aut}\, S_l(G/F_{2l}) \\ \downarrow & & \downarrow \nu \\ G/F_2 & \xrightarrow{\text{trivial}} & \mathrm{Aut}\, S_l(G/F_2) \end{array}$$

It implies that the image of μ is contained in the kernel of ν. Since both $S_l(G/F_{2l})$ and $S_l(G/F_2)$ are nontrivial cyclic l-groups and ν is surjective, the order of the kernel of ν is a power of l. Hence the order of the image of μ is a power of l. On the other hand, since $S_l(G/F_{2l})$ is abelian, we can regard μ as a homomorphism of $(G/F_{2l})/S_l(G/F_{2l})$ to $\mathrm{Aut}\, S_l(G/F_{2l})$. Since the order of $(G/F_{2l})/S_l(G/F_{2l})$ is prime to l, so is the order of the image of μ. Consequently, μ is trivial and G/F_{2l} acts trivially on $S_l(G/F_{2l})$. In particular, G/F_{2l} acts trivially on $F_2/F_{2l} \subset S_l(G/F_{2l})$. Then G/F_2 acts trivially on F_2/F_{2l} because F_2/F_{2l} is abelian. Therefore the fact $F_2/F_{2l} \cong S_l(F)$ completes the proof.

Since G/F_2 is nilpotent, Lemma 5 implies that G/F_{2k} is nilpotent. Since $S_l(G/F_{2k})$ is cyclic for every odd prime l and $S_2(G/F_{2k}) \cong S_2(G)$, we have

$$G/F_{2k} \cong S_2(G) \times C,$$

where C is a cyclic group of odd order. Since both $|G/F_2|(=k)$ and $|F_2/F_{2k}|$ are prime to $|F_{2k}|$, so is $|G/F_{2k}|$. Then we have

$$G \cong G/F_{2k} \ltimes F_{2k} \cong (S_2(G) \times C) \ltimes F_{2k},$$

where C and F_{2k} are cyclic groups of odd order such that $(|C|, |F_{2k}|) = 1$. Let x be an element of prime order l_1 of G/F_{2k}. If x acts nontrivially on F_{2k}, then it acts nontrivially on $S_{l_2}(F_{2k}) \cong \mathbf{Z}/l_2{}^n\mathbf{Z}$ for some prime divisor l_2 of $|F_{2k}|$. Since the order of the kernel of an epimorphism of $\mathrm{Aut}\,\mathbf{Z}/l_2{}^n\mathbf{Z}$ to $\mathrm{Aut}\,\mathbf{Z}/l_2\mathbf{Z}$ is a power of l_2 and is prime to the order l_1 of x, we have that x acts nontrivially on $\mathbf{Z}/l_2\mathbf{Z}$. It implies that a non-direct semi-direct product $\mathbf{Z}/l_1\mathbf{Z} \ltimes \mathbf{Z}/l_2\mathbf{Z}$ is contained in G, which contradicts the condition (i) of Proposition 2. Consequently, any element of prime order of G/F_{2k} acts trivially on F_{2k}. In the case where $S_2(G)$ is cyclic, by putting $\mathfrak{G} = \{1\}$, $C_1 = S_2(G) \times C$ and $C_2 = F_{2k}$, we see that G is of Type I. In the case where $S_2(G) \cong Q_n$, by putting $\mathfrak{G} = S_2(G)$, $C_1 = C$ and $C_2 = F_{2k}$, we see that G is of Type II.

We summarize the result of this subsection.

PROPOSITION 3. *Let G be a finite group satisfying the condition* (i) *of Proposition* 2. *If G is solvable and* $\mathrm{Im}\,\Phi$ *is a* 2*-group, then G is of Type* I *or* II.

2.4. We suppose that a finite solvable group G satisfies the condition (i) of Proposition 2 and that $\mathrm{Im}\,\Phi$ is not a 2-group. Then $\mathrm{Aut}\,S_2(F)$ is not a 2-group. Since $S_2(F)$ is cyclic or isomorphic to Q_n, we conclude that $S_2(F) \cong Q_8$ and $\mathrm{Aut}\,S_2(F) \cong \mathfrak{S}_4$, where $\mathfrak{S}_4$ denotes the symmetric group of degree 4. Since $S_2(F)$ char $F \lhd G$, we have $S_2(F) \lhd S_2(G)$ and $S_2(G) \cong Q_8$ or Q_{16}. Then, by noting that $\mathrm{Inn}\,S_2(F) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \subset \mathrm{Im}\,\Phi$, we easily obtain $\mathrm{Im}\,\Phi \cong \mathfrak{A}_4$ or $\mathfrak{S}_4$ according as $S_2(G) \cong Q_8$ or Q_{16}, where $\mathfrak{A}_4$ denotes the alternating group of degree 4. On the other hand, $\mathrm{Ker}\,\Phi$ is abelian because $\mathrm{Ker}\,\Phi \hookrightarrow \{1\} \times \mathrm{Aut}\,F_2$. Since $S_2(Z(F)) = Z(S_2(F)) \cong Z(Q_8) \cong \mathbf{Z}/2\mathbf{Z}$, we have $|S_2(G/Z(F))| = 4$ or 8 according as $S_2(G) \cong Q_8$ or Q_{16}. It implies that $|S_2(G/Z(F))| = |S_2(\mathrm{Im}\,\Phi)|$ and that $|\mathrm{Ker}\,\Phi|$ is odd. Then $\mathrm{Ker}\,\Phi$ is a cyclic group of odd order because $S_l(\mathrm{Ker}\,\Phi)$ is cyclic for every odd prime l. Therefore we can write $\mathrm{Ker}\,\Phi \cong S_3(\mathrm{Ker}\,\Phi) \times C$, where C is a cyclic group such that $(|C|, 6) = 1$. We put $X = (G/Z(F))/C$. Then $G/Z(F) \cong X \ltimes C$ because a prime divisor of $|X| = |\mathrm{Im}\,\Phi|\,|\mathrm{Ker}\,\Phi|/|C| = |\mathrm{Im}\,\Phi|\,|S_3(\mathrm{Ker}\,\Phi)|$ is 2 or 3. Since $G/Z(F) \hookrightarrow \mathrm{Im}\,\Phi \times \mathrm{Aut}\,F_2$ and $\mathrm{Ker}\,\Phi \hookrightarrow \{1\} \times \mathrm{Aut}\,F_2$, we see that $G/Z(F)$ acts trivially on $\mathrm{Ker}\,\Phi$ and that $G/Z(F) \cong X \times C$.

We would like to determine X. Since $G/Z(F)$ acts trivially on $\mathrm{Ker}\,\Phi$, X acts trivially on $S_3(\mathrm{Ker}\,\Phi)$. Then we have a central extension.

$$1 \to S_3(\mathrm{Ker}\,\Phi) \to X \to \mathrm{Im}\,\Phi \to 1. \tag{4}$$

We can write $S_3(X) \cong \mathbf{Z}/3^{m'}\mathbf{Z}$ for a natural number m'. If $S_2(G) \cong Q_8$, then $\mathrm{Im}\,\Phi \cong \mathfrak{A}_4$. Since $S_2(\mathfrak{A}_4) \lhd \mathfrak{A}_4$ and (4) is central, Lemma 2 implies that $S_2(X) \lhd X$. Since the order of $X/S_2(X)$ is a power of 3, we have $X/S_2(X) \cong S_3(X)$ and $X \cong S_3(X) \ltimes S_2(X)$.

Since $S_2(X) \cong S_2(\mathfrak{A}_4) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, we have $X \cong \mathbf{Z}/3^{m'}\mathbf{Z} \ltimes (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})$ (non-direct). If $S_2(G) \cong Q_{16}$, then $\operatorname{Im}\Phi \cong \mathfrak{S}_4$. The central extension (4) gives a central extension $1 \to S_3(\operatorname{Ker}\Phi) \to X_1 \to \operatorname{Inn} S_2(F) \to 1$, where X_1 is a normal subgroup of X defined as the inverse image of $\operatorname{Inn} S_2(F)$. Since $\operatorname{Inn} S_2(F) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, we have $X_1 \cong S_3(\operatorname{Ker}\Phi) \times (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})$. We put $X' = X/(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})$. Then $X'/S_3(\operatorname{Ker}\Phi) \cong X/X_1 \cong \operatorname{Im}\Phi/\operatorname{Inn} S_2(F) \cong D_6$. Since $S_3(D_6) \lhd D_6$, Lemma 2 implies that $S_3(X') \lhd X'$. The image of $X' \to \operatorname{Aut} S_3(X') \cong \operatorname{Aut}\mathbf{Z}/3^{m'}\mathbf{Z}$ is of even order, because the image of $D_6 \to \operatorname{Aut} S_3(D_6)$ is of order 2. On the other hand, since X acts trivially on $S_3(\operatorname{Ker}\Phi) \cong \mathbf{Z}/3^{m'-1}\mathbf{Z}$, so does X'. We know that the kernel of an epimorphism of $\operatorname{Aut}\mathbf{Z}/3^{m'}\mathbf{Z}$ to $\operatorname{Aut}\mathbf{Z}/3^{m'-1}\mathbf{Z}$ is of even order only if $m' = 1$. It implies that $S_3(\operatorname{Ker}\Phi)$ is trivial. Hence we have from (4) that $X \cong \mathfrak{S}_4$. Now we have

$$G/Z(F) \cong X \times C\,,$$

where

$$X \cong \begin{cases} \mathbf{Z}/3^{m'}\mathbf{Z} \ltimes (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \text{ (non-direct)} & \text{if } S_2(G) \cong Q_8\,, \\ \mathfrak{S}_4 & \text{if } S_2(G) \cong Q_{16}\,, \end{cases}$$

and C is a cyclic group such that $(|C|, 6) = 1$.

Since $Z(S_2(F)) \cong Z(Q_8) \cong \mathbf{Z}/2\mathbf{Z}$, we have a central extension $1 \to \mathbf{Z}/2\mathbf{Z} \to G/F_2 \to G/Z(F) \to 1$. Since $(|C|, 6) = 1$, Lemma 3 implies that $G/F_2 \cong Y \times C$ and that

$$1 \to \mathbf{Z}/2\mathbf{Z} \to Y \to X \to 1$$

is a central extension. If $S_2(G) \cong Q_8$, then we have proved that $S_2(X) \lhd X$. Hence Lemma 2 implies that $S_2(Y) \lhd Y$. Since the order of $Y/S_2(Y)$ is a power of 3, we have $Y/S_2(Y) \cong S_3(Y)$ and $Y \cong S_3(Y) \ltimes S_2(Y)$. Since $S_2(Y) \cong S_2(G) \cong Q_8$, we have $Y \cong \mathbf{Z}/3^{m'}\mathbf{Z} \ltimes Q_8$ (non-direct). If $S_2(G) \cong Q_{16}$, then $X \cong \mathfrak{S}_4 \cong PGL(2, \boldsymbol{F}_3)$. Since $S_2(Y) \cong S_2(G) \cong Q_{16}$, Lemma 4 implies $Y \cong H_3$. Now we have

$$G/F_2 \cong Y \times C\,,$$

where

$$Y \cong \begin{cases} \mathbf{Z}/3^{m'}\mathbf{Z} \ltimes Q_8 \text{ (non-direct)} & \text{if } S_2(G) \cong Q_8\,, \\ H_3 & \text{if } S_2(G) \cong Q_{16}\,, \end{cases}$$

and C is as above.

Since $F_2 = S_3(F) \times F_6$, we have an exact sequence $1 \to S_3(F) \to G/F_6 \to G/F_2 \to 1$. Since $S_3(F)$ is cyclic, a prime divisor of $|\operatorname{Aut} S_3(F)|$ is 2 or 3. Since $(|C|, 6) = 1$, Lemma 3 implies that $G/F_6 \cong U \times C$ and that

$$1 \to S_3(F) \to U \to Y \to 1 \tag{5}$$

is an exact sequence. We can write $S_3(U) \cong \mathbf{Z}/3^m\mathbf{Z}$ for a natural number m. Since $S_3(F)$ is cyclic, the action of U on $S_3(F)$ is determined by that of Y on $S_3(F)$. If $S_2(G) \cong Q_8$, then $Y \cong S_3(Y) \ltimes Q_8$ (non-direct). Clearly $S_3(Y)$ acts tribially on $S_3(F)$ because a cyclic group $S_3(U)$ acts trivially on its subgroup $S_3(F)$. On the other hand, since $\operatorname{Aut} S_3(F)$ is abelian, we see that the kernel of $Y \to \operatorname{Aut} S_3(F)$ contains $Y^c \cong Q_8$. It implies that Y acts

trivially on $S_3(F)$ and that (5) is a central extension. Since $S_2(Y) \lhd Y$, Lemma 2 implies that $S_2(U) \lhd U$. Since the order of $U/S_2(U)$ is a power of 3, we have $U/S_2(U) \cong S_3(U)$ and $U \cong S_3(U) \ltimes S_2(U) \cong \boldsymbol{Z}/3^m\boldsymbol{Z} \ltimes Q_8$ (non-direct). If $S_2(G) \cong Q_{16}$, then $Y \cong H_3$. We note that $H_3 \supset SL(2, \boldsymbol{F}_3) \cong \boldsymbol{Z}/3\boldsymbol{Z} \ltimes Q_8$ (non-direct). As noted in the proof of Lemma 4, H_3 is generated by $SL(2, \boldsymbol{F}_3)$ and an element a which does not belong to $SL(2, \boldsymbol{F}_3)$. Since $S_2(H_3) \cong S_2(G) \cong Q_{16}$, we can take a so that $a^{-1}Q_8a \subset Q_8$. It implies that $Q_8 \lhd H_3$. Then the exact sequence (5) gives an exact sequence $1 \to S_3(F) \to U_1 \to Q_8 \to 1$, where U_1 is a normal subgroup of U defined as the inverse image of Q_8. Since the kernel of $H_3 \to \operatorname{Aut} S_3(F)$ contains H_3^c and $H_3^c \supset SL(2, \boldsymbol{F}_3)^c \cong Q_8$, we see that $U_1 \cong Q_8 \times S_3(F)$ and that Q_8 char U_1. Therefore we have $Q_8 \lhd U$. Since U/Q_8 is of order $2 \cdot 3^m$ and has a cyclic Sylow 3-subgroup, we obtain an exact sequence $1 \to Q_8 \to U \to D_{2\cdot 3^m} \to 1$. By this exact sequence and the exact sequence (5), we can define a monomorphism $U \to H_3 \times D_{2\cdot 3^m}$. Then it is easily proved that $U \cong H_{3,m}$. Now we have

$$G/F_6 \cong U \times C\,,$$

where

$$U \cong \begin{cases} \boldsymbol{Z}/3^m\boldsymbol{Z} \ltimes Q_8 \text{ (non-direct)} & \text{if } S_2(G) \cong Q_8\,, \\ H_{3,m} & \text{if } S_2(G) \cong Q_{16}\,, \end{cases}$$

and C is as above.

We put $k = |G/F_6|$. Since a prime divisor of $|U|$ is 2 or 3, we know that $S_l(G/F_6) \subset Z(G/F_6)$ for a prime $l > 3$. Therefore we can use the same argument as in the proof of Lemma 5 and prove that $1 \to F_6/F_{6k} \to G/F_{6k} \to G/F_6 \to 1$ is a central extension. Since $(|F_6/F_{6k}|, 6) = (|C|, 6) = 1$, Lemma 3 implies that $G/F_{6k} \cong U \times C_1$ and that $1 \to F_6/F_{6k} \to C_1 \to C \to 1$ is a central extension. It implies that C_1 is nilpotent and that $(|C_1|, 6) = 1$. Moreover C_1 is cyclic because every Sylow subgroup of C_1 is cyclic. Now we have

$$G/F_{6k} \cong U \times C_1\,,$$

where U is as above and C_1 is a cyclic group such that $(|C_1|, 6) = 1$. Since both $|G/F_6|(= k)$ and $|F_6/F_{6k}|$ are prime to $|F_{6k}|$, so is $|G/F_{6k}|$. Then we have

$$G \cong G/F_{6k} \ltimes F_{6k} \cong (U \times C_1) \ltimes F_{6k}\,.$$

We note that C_1 and F_{6k} are cyclic groups such that $(|C_1|, |F_{6k}|) = (|C_1|\,|F_{6k}|, 6) = 1$. Since no non-direct semi-direct product $\boldsymbol{Z}/l_1\boldsymbol{Z} \ltimes \boldsymbol{Z}/l_2\boldsymbol{Z}$ is contained in G for any pair of primes l_1 and l_2, the same argument as in the preceding subsection implies that each element of prime order of G/F_{6k} acts trivially on F_{6k}. By putting $\mathfrak{G} = U$ and $C_2 = F_{6k}$, we now know that G is of Type III or IV according as $S_2(G) \cong Q_8$ or Q_{16}.

We summarize the result of this subsection.

PROPOSITION 4. *Let G be a finite group satisfying the condition* (i) *of Proposition* 2. *If G is solvable and* Im Φ *is not a* 2*-group, then G is of Type* III *or* IV.

2.5. We suppose that a finite non-solvable group G satisfies the condition (i) of Proposition 2. Then G is of even order (Theorem 3.1, Chapter 6, [2]). If $S_2(G)$ is cyclic, then

Corollary 1 to Theorem 2.10 in Chapter 5 of [2] implies that there exists a normal subgroup N of G such that $G/N \cong S_2(G)$. Since N is of odd order, it is solvable and so is G, which is a contradiction. Therefore we have $S_2(G) \cong Q_n$. We denote by O the maximal normal subgroup of G of odd order. Then Theorem 8.7 in Chapter 6 of [2] implies that G has a normal subgroup G_0 of odd index such that $G_0 \supset O$ and

$$1 \to \boldsymbol{Z}/2\boldsymbol{Z} \to G_0/O \to V \to 1$$

is a central extension, where $V \cong PSL(2, \boldsymbol{F}_q)$, $PGL(2, \boldsymbol{F}_q)$ or $\mathfrak{A}_7$ (the alternating group of degree 7) and q is an odd prime power and bigger than 3. Since we know that $PGL(2, \boldsymbol{F}_{p^2}) \supset PSL(2, \boldsymbol{F}_{p^2}) \supset \boldsymbol{F}_{p^2}(\text{additive}) \cong \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z}$ for a prime p and that $\mathfrak{A}_7 \supset \boldsymbol{Z}/3\boldsymbol{Z} \times \boldsymbol{Z}/3\boldsymbol{Z}$, we must have $V \cong PSL(2, \boldsymbol{F}_p)$ or $PGL(2, \boldsymbol{F}_p)$, where p is a prime bigger than 3. Since $S_2(G_0/O) \subset S_2(G/O) \cong S_2(G) \cong Q_n$, a direct product $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$ is not contained in G_0/O. Therefore Lemma 4 implies that

$$G_0/O \cong SL(2, \boldsymbol{F}_p) \quad \text{or} \quad H_p\,,$$

where p is a prime bigger than 3.

We suppose that $G_0 \neq G$. Since G/G_0 is of odd order, it is solvable. Since each Sylow subgroup of G/G_0 is cyclic, the same argument as in the preceding subsections implies that G/G_0 is of Type I, II, III or IV. (Here we do not know whether the condition (2) in Table 1 is satisfied or not, because we do not know whether any non-direct semi-direct product $\boldsymbol{Z}/l_1\boldsymbol{Z} \ltimes \boldsymbol{Z}/l_2\boldsymbol{Z}$ is contained in G/G_0 for any pair of primes l_1 and l_2.) Moreover, since G/G_0 is of odd order, we see that G/G_0 is of Type I. Therefore G/G_0 has a normal subgroup N/G_0 of odd prime order. We denote by l the order of N/G_0. Since $G_0/O \lhd N/O$, both $(G_0/O)^c$ and $Z((G_0/O)^c)$ are normal subgroups of N/O. We denote by ρ the homomorphism of N/O to $\mathrm{Aut}((G_0/O)^c/Z((G_0/O)^c))$ which assigns restrictions of inner automorphisms. Since Corollary to Lemma 4 implies that $(G_0/O)^c \cong SL(2, \boldsymbol{F}_p)$, we can regard ρ as a homomorphism of N/O to $\mathrm{Aut}\, PSL(2, \boldsymbol{F}_p)$. We denote by $\mathrm{Ker}\,\rho$ (resp. $\mathrm{Im}\,\rho$) the kernel (resp. image) of ρ. We note that $\mathrm{Ker}\,\rho \cap G_0/O$ is a normal subgroup of G_0/O and contains $Z((G_0/O)^c) \cong \boldsymbol{Z}/2\boldsymbol{Z}$. Since $PSL(2, \boldsymbol{F}_p)$ is simple and $PGL(2, \boldsymbol{F}_p)$ has only 3 normal subgroups $\{1\}$, $PSL(2, \boldsymbol{F}_p)$ and $PGL(2, \boldsymbol{F}_p)$ (Theorem 9.9, Chapter 1, [2]), Lemma 4 implies that $\mathrm{Ker}\,\rho \cap G_0/O \cong \boldsymbol{Z}/2\boldsymbol{Z}$, $SL(2, \boldsymbol{F}_p)$ or H_p. Since $SL(2, \boldsymbol{F}_p)$ acts nontrivially on $PSL(2, \boldsymbol{F}_p)$, we see that $\mathrm{Ker}\,\rho \cap G_0/O \cong \boldsymbol{Z}/2\boldsymbol{Z}$. Hence $\mathrm{Im}\,\rho \supset \rho(G_0/O) \cong (G_0/O)/(\mathrm{Ker}\,\rho \cap G_0/O)$, which implies that $|G_0/O|$ divides $2|\mathrm{Im}\,\rho|$. Since $\mathrm{Im}\,\rho \subset \mathrm{Aut}\, PSL(2, \boldsymbol{F}_p) \cong PGL(2, \boldsymbol{F}_p)$ ((8.8), Chapter 6, [2]), we see that $|\mathrm{Im}\,\rho|$ divides $|G_0/O|$. Therefore $|G_0/O|/|\mathrm{Im}\,\rho| = 1$ or 2. Since $|\mathrm{Ker}\,\rho|$ is even and $|\mathrm{Ker}\,\rho| = |N/O|/|\mathrm{Im}\,\rho| = l \cdot |G_0/O|/|\mathrm{Im}\,\rho|$, we see that $|\mathrm{Ker}\,\rho| = 2l$. It implies that $\mathrm{Ker}\,\rho \cong \boldsymbol{Z}/l\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$, because $\mathrm{Ker}\,\rho \rhd \mathrm{Ker}\,\rho \cap G_0/O \cong \boldsymbol{Z}/2\boldsymbol{Z}$. Then $S_l(\mathrm{Ker}\,\rho) \lhd N/O$. Since $\mathrm{Ker}\,\rho \cap G_0/O \cong \boldsymbol{Z}/2\boldsymbol{Z}$ implies that $S_l(\mathrm{Ker}\,\rho) \cap G_0/O \cong \{1\}$, we conclude that $N/O \cong S_l(\mathrm{Ker}\,\rho) \times G_0/O \cong \boldsymbol{Z}/l\boldsymbol{Z} \times G_0/O$. Since $S_l(N/O)$ is cyclic, the order of G_0/O is not divisible by l. It implies that N/O has a characteristic subgroup of order l and that G/O has a normal subgroup of order l, a contradiction to the definition of O. Therefore we have

proved that $G_0 = G$, which implies that

$$G/O \cong SL(2, \boldsymbol{F}_p) \quad \text{or} \quad H_p ,$$

where p is a prime bigger than 3.

Since O is of odd order and any Sylow subgroup of O is cyclic, we have shown above that O is of Type I; namely, $O \cong C_1 \ltimes C_2$, where C_1 and C_2 are cyclic groups such that $(|C_1|, |C_2|) = 1$. If $S_l(C_1)$ acts trivially on C_2 for a prime divisor l of $|C_1|$, we can replace C_1 (resp. C_2) by a subgroup isomorphic to $C_1/S_l(C_1)$ (resp. $C_2 \times S_l(C_1)$). Therefore we may assume that every nontrivial Sylow subgroup of C_1 acts nontrivially on C_2. We examine the exact sequence

$$1 \to C_1 \to G/C_2 \to G/O \to 1 . \tag{6}$$

Since C_1 is cyclic, an action of G/C_2 on C_1 is determined by that of G/O on C_1. We denote by σ the homomorphism of G/O to $\operatorname{Aut} C_1$ induced by inner automorphisms. Then, since $\operatorname{Aut} C_1$ is abelian, the kernel of σ contains $(G/O)^c \cong SL(2, \boldsymbol{F}_p)$, which implies that the index of the kernel of σ in G/O is 1 or 2. We suppose that there exists an element y of G/O which acts nontrivially on C_1. Then y acts nontrivially on $S_{l_1}(C_1)$ for a prime l_1. We denote by x a generator of $S_{l_1}(C_1)$. Then $y^{-1}xy = x^{-1}$ because the order of $\sigma(y)$ is 2. It is assumed that x acts nontrivially on $S_{l_2}(C_2)$ for a prime l_2. Here we may regard x and y as elements of G/C_2. We denote by τ the homomorphism of G/C_2 to $\operatorname{Aut} S_{l_2}(C_2)$ induced by inner automorphisms. Since $\operatorname{Aut} S_{l_2}(C_2)$ is abelian, we have $\tau(x) = \tau(y^{-1}xy) = \tau(x^{-1})$. Since $\tau(x)$ is not trivial, it implies that the order of $\tau(x)$ is 2, which contradicts the fact that O is of odd order. Therefore G/O acts trivially on C_1 and (6) is a central extension. It gives a central extension $1 \to C_1 \to G_1 \to SL(2, \boldsymbol{F}_p) \to 1$, where G_1 is a normal subgroup of G/C_2 defined as the inverse image of $SL(2, \boldsymbol{F}_p)$. Since we know that any central extension of $SL(2, \boldsymbol{F}_p)$ splits (Section 9, Chapter 2, [2]), we conclude that $G_1 \cong SL(2, \boldsymbol{F}_p) \times C_1$. Since any Sylow subgroup of G_1 has to be cyclic or isomorphic to Q_n, we have $(|SL(2, \boldsymbol{F}_p)|, |C_1|) = 1$ and $(|G/O|, |C_1|) = 1$. Therefore the central extension (6) implies that

$$G/C_2 \cong G/O \times C_1 .$$

An exact sequence $1 \to C_2 \to G \to G/C_2 \to 1$ gives an exact sequence $1 \to C_2 \to G_2 \to SL(2, \boldsymbol{F}_p) \to 1$, where G_2 is a subgroup of G defined as the inverse image of $SL(2, \boldsymbol{F}_p)$. Since C_2 is cyclic, an action of G_2 on C_2 is determined by that of $SL(2, \boldsymbol{F}_p)$ on C_2. It is trivial because $\operatorname{Aut} C_2$ is abelian and $SL(2, \boldsymbol{F}_p)^c = SL(2, \boldsymbol{F}_p)$. Hence $1 \to C_2 \to G_2 \to SL(2, \boldsymbol{F}_p) \to 1$ is a central extension and splits, namely, $G_2 \cong SL(2, \boldsymbol{F}_p) \times C_2$. Since any Sylow subgroup of G_2 has to be cyclic or isomorphic to Q_n, we have $(|SL(2, \boldsymbol{F}_p)|, |C_2|) = 1$ and $(|G/C_2|, |C_2|) = 1$. Therefore we have

$$G \cong G/C_2 \ltimes C_2 \cong (G/O \times C_1) \ltimes C_2 .$$

We note that C_1 and C_2 are cyclic groups such that $(|C_1|, |C_2|) = (|C_1||C_2|, |G/O|) = 1$. Since no non-direct semi-direct product $\boldsymbol{Z}/l_1\boldsymbol{Z} \ltimes \boldsymbol{Z}/l_2\boldsymbol{Z}$ is contained in G for any pair of

primes l_1 and l_2, the same argument as in the preceding subsections implies that every element of prime order of G/C_2 acts trivially on C_2. If there exists an odd prime l dividing $p-1$, then

$$SL(2, \boldsymbol{F}_p) \supset \left\langle \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \cong \mathbf{Z}/l\mathbf{Z} \ltimes \mathbf{Z}/p\mathbf{Z} \text{ (non-direct)},$$

where α is an element of the multiplicative group of $\boldsymbol{F}_p$ of order l. It contradicts the condition (i) of Proposition 2. Therefore p is a Fermat prime. By putting $\mathfrak{G} = G/O$, we know that G is of Type V or VI.

We summarize the result of this subsection.

PROPOSITION 5. *Let G be a finite group satisying the condition* (i) *of Proposition* 2. *If G is non-solvable, then G is of Type* V *or* VI.

2.6. Combining Propositions 3, 4 and 5, we see that the condition (ii) follows from the condition (i) in Proposition 2. To prove the converse, we suppose that G is a finite group satisfying the condition (ii), namely, that G is of one of Types I–VI. Clearly, Q_n has a unique element of order 2. As noted in the proof of Lemma 4, both $SL(2, \boldsymbol{F}_p)$ and H_p have the same property. Then it is also proved that $H_{3,m}$ has the same property. Consequently, the number of elements of order 2 of $\mathfrak{G} \times C_1$ is at most one. It implies that no direct product $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ is contained in G. Moreover, no non-direct semi-direct product $\mathbf{Z}/2\mathbf{Z} \ltimes \mathbf{Z}/l\mathbf{Z}$ is contained in G for any prime l, because every element of prime order of $\mathfrak{G} \times C_1$ acts trivially on C_2. On the other hand, since all subgroups of $SL(2, \boldsymbol{F}_p)$ are obtained in Theorem 6.17 in Chapter 3 of [2], we see that every subgroup of odd order of $SL(2, \boldsymbol{F}_p)$ is cyclic if p is a Fermat prime. Then H_p has the same property because each subgroup of odd order of H_p is contained in $SL(2, \boldsymbol{F}_p)$. It is also proved that $H_{3,m}$ has the same property. Consequently, every subgroup of odd order of $\mathfrak{G} \times C_1$ is cyclic. It implies that no direct product $\mathbf{Z}/l\mathbf{Z} \times \mathbf{Z}/l\mathbf{Z}$ is contained in G for any odd prime l. Moreover, no non-direct semi-direct product $\mathbf{Z}/l_1\mathbf{Z} \ltimes \mathbf{Z}/l_2\mathbf{Z}$ is contained in G for any pair of odd primes l_1 and l_2, because every element of prime order of $\mathfrak{G} \times C_1$ acts trivially on C_2. Now we have proved that the condition (i) follows from the condition (ii). The proof of Proposition 2 is complete.

REMARK. As noted above, the condition that no non-direct semi-direct product $\mathbf{Z}/l_1\mathbf{Z} \ltimes \mathbf{Z}/l_2\mathbf{Z}$ is contained in G for any pair of primes l_1 and l_2 follows from two conditions that every element of prime order of $\mathfrak{G} \times C_1$ acts trivially on C_2 and that p is a Fermat prime. As was shown in the preceding subsection, the converse is also true. Therefore we can state a modification of Proposition 2.

PROPOSITION 2′. *For a finite group G the following two conditions are equivalent*:

(i) *Every abelian subgroup of G is cyclic.*

(ii) *G satisfies the conditions* (1) *and one of* (3-I)–(3-VI) *in Table* 1. (*A prime p is not necessarily "Fermat".*)

3. Calculation of n_G. Proposition 2 implies that it is sufficient for the proof of the Theorem to calculate n_G for the finite groups G of Types I–VI. We carry out the calculation in this section. We start with some simple examples, where the notation is as in Section 1.

EXAMPLE 3. If G is a cyclic group of prime order l, then $(\mathrm{Tr}_H \mid \{1\} \neq H \subseteq G)_{\boldsymbol{R}[G]} = (\mathrm{Tr}_G)_{\boldsymbol{R}[G]}$. It implies that $t_G = 1$ and $n_G = l - 1 = \varphi(|G|)$.

For two subgroups H_1 and H_2 of G, it is clear that $\mathrm{Ker}\,\mathrm{Tr}_{H_1} \subset \mathrm{Ker}\,\mathrm{Tr}_{H_2}$ if $H_1 \subset H_2$. Hence it suffices to consider only minimal subgroups H of G in the definition of n_G in Proposition 1. Therefore we have the following lemma.

LEMMA 6. *Let G_0 be a subgroup of G such that the set of minimal subgroups of G_0 is equal to that of G. Then*

$$n_G = [G : G_0] n_{G_0},$$

where $[G : G_0]$ denotes the index of G_0 in G.

PROOF. The assumption implies that

$$\bigcap_{\{1\}\neq H\subseteq G} \mathrm{Ker}\,\mathrm{Tr}_H = \bigcap_{\{1\}\neq H\subseteq G_0} \mathrm{Ker}\,\mathrm{Tr}_H$$
$$= \bigoplus_g g \cdot \left(\bigcap_{\{1\}\neq H\subseteq G_0} \mathrm{Ker}(\mathrm{Tr}_H : \boldsymbol{R}[G_0] \to \boldsymbol{R}[G_0]) \right),$$

where g runs over a complete system of representatives of left cosets of G_0 in G. Hence $n_G = [G : G_0] n_{G_0}$.

EXAMPLE 4. If G is a cyclic group of prime power order l^m, then we can take the subgroup of order l as G_0. Hence Lemma 6 and Example 3 imply that $n_G = l^{m-1}(l-1) = \varphi(|G|)$.

LEMMA 7. *If $G = G_1 \times G_2$ and $(|G_1|, |G_2|) = 1$, then*

$$n_G = n_{G_1} n_{G_2}.$$

PROOF. Under the assumption every subgroup H of G is written in the form $H_1 \times H_2$, where H_i is a subgroup of G_i. Then a minimal subgroup of G is either that of G_1 or of G_2. Because $\boldsymbol{R}[G]$ is naturally isomorphic to a tensor product $\boldsymbol{R}[G_1] \otimes_{\boldsymbol{R}} \boldsymbol{R}[G_2]$ as a right $\boldsymbol{R}[G]$-module, we see that

$$\bigcap_{\{1\}\neq H\subseteq G} \mathrm{Ker}\,\mathrm{Tr}_H = \left(\bigcap_{\{1\}\neq H\subseteq G_1} \mathrm{Ker}\,\mathrm{Tr}_H \right) \cap \left(\bigcap_{\{1\}\neq H\subseteq G_2} \mathrm{Ker}\,\mathrm{Tr}_H \right)$$
$$\cong \bigcap_{\{1\}\neq H\subseteq G_1} \mathrm{Ker}(\mathrm{Tr}_H : \boldsymbol{R}[G_1] \to \boldsymbol{R}[G_1])$$
$$\otimes_{\boldsymbol{R}} \bigcap_{\{1\}\neq H\subseteq G_2} \mathrm{Ker}(\mathrm{Tr}_H : \boldsymbol{R}[G_2] \to \boldsymbol{R}[G_2]).$$

Hence $n_G = n_{G_1} n_{G_2}$.

EXAMPLE 5. If G is a cyclic group, then Lemma 7 and Example 4 imply that $n_G = \varphi(|G|)$.

Now we can calculate n_G for G of Types I–VI by using Lemmas 6 and 7 and Example 5. From now on, let G_0 be the subgroup of G generated by all of the elements of prime order.

Then G_0 satisfies the assumption of Lemma 6. We also remark that $[G : G_0]\varphi(|G_0|) = \varphi(|G|)$, because the set of prime divisors of $|G_0|$ is equal to that of $|G|$. The conditions (1) and (2) in Table 1 imply that every element of prime order of G belongs to $\mathfrak{G}$, C_1 or C_2 and that

$$G_0 \cong \mathfrak{G}_0 \times (C_1)_0 \times (C_2)_0 .$$

We calculate $\mathfrak{G}_0$ for each type.

Type I: $\mathfrak{G} \cong \{1\}$. $\mathfrak{G}_0 \cong \{1\}$.

Type II: $\mathfrak{G} \cong Q_n$. $\mathfrak{G}_0 \cong \boldsymbol{Z}/2\boldsymbol{Z}$.

Type III: $\mathfrak{G} \cong \boldsymbol{Z}/3^m\boldsymbol{Z} \ltimes Q_8$ (non-direct). If $m \geq 2$, then every element of order 3 of $\boldsymbol{Z}/3^m\boldsymbol{Z}$ belongs to the kernel of $(\boldsymbol{Z}/3^m\boldsymbol{Z} \to \operatorname{Aut} Q_8 \cong \mathfrak{S}_4)$. Hence we have $\mathfrak{G}_0 \cong \boldsymbol{Z}/3\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z} \cong \boldsymbol{Z}/6\boldsymbol{Z}$. If $m = 1$, then $\mathfrak{G} \cong \boldsymbol{Z}/3\boldsymbol{Z} \ltimes Q_8$ (non-direct) $\cong SL(2, \boldsymbol{F}_3)$. Since $SL(2, \boldsymbol{F}_3)_0 = SL(2, \boldsymbol{F}_3)$, we have $\mathfrak{G}_0 \cong SL(2, \boldsymbol{F}_3)$.

Type IV: $\mathfrak{G} \cong H_{3,m}$. If $m \geq 2$, then the definition of $H_{3,m}$ implies that $H_{3,m}$ has a unique subgroup of order 3 (because so dose $D_{2\cdot 3^m}$). As was noted in Section 2.6, $H_{3,m}$ has a unique subgroup of order 2. Hence we have $\mathfrak{G}_0 \cong \boldsymbol{Z}/3\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z} \cong \boldsymbol{Z}/6\boldsymbol{Z}$. If $m = 1$, then $\mathfrak{G} \cong H_{3,m} = H_3$. Since $SL(2, \boldsymbol{F}_3)_0 = SL(2, \boldsymbol{F}_3)$, we have $(H_3)_0 \supset SL(2, \boldsymbol{F}_3)$. Since every element of prime order of H_3 belongs to $SL(2, \boldsymbol{F}_3)$, we have $\mathfrak{G}_0 \cong SL(2, \boldsymbol{F}_3)$.

Type V: $\mathfrak{G} \cong SL(2, \boldsymbol{F}_p)$. Since $SL(2, \boldsymbol{F}_p)_0 = SL(2, \boldsymbol{F}_p)$, we have $\mathfrak{G}_0 \cong SL(2, \boldsymbol{F}_p)$.

Type VI: $\mathfrak{G} \cong H_p$. Since $SL(2, \boldsymbol{F}_p)_0 = SL(2, \boldsymbol{F}_p)$, we have $(H_p)_0 \supset SL(2, \boldsymbol{F}_p)$. Since every element of prime order of H_p belongs to $SL(2, \boldsymbol{F}_p)$, we have $\mathfrak{G}_0 \cong SL(2, \boldsymbol{F}_p)$.

Therefore we have the following consequence. For Types I, II, III ($m \geq 2$) and IV ($m \geq 2$), G_0 is cyclic. Lemma 6 and Example 5 imply that

$$n_G = [G : G_0]\varphi(|G_0|) = \varphi(|G|) .$$

For Types III ($m = 1$) and IV ($m = 1$), we have $G_0 \cong SL(2, \boldsymbol{F}_3) \times C$, where C is a cyclic group and $(|SL(2, \boldsymbol{F}_3)|, |C|) = 1$. Lemmas 6 and 7 and Example 5 imply that

$$\begin{aligned} n_G &= [G : G_0] n_{SL(2,\boldsymbol{F}_3)} \varphi(|C|) \\ &= [G : G_0] n_{SL(2,\boldsymbol{F}_3)} \frac{\varphi(|G_0|)}{\varphi(|SL(2, \boldsymbol{F}_3)|)} \\ &= \frac{n_{SL(2,\boldsymbol{F}_3)}}{\varphi(|SL(2, \boldsymbol{F}_3)|)} \varphi(|G|) . \end{aligned}$$

By using computer, we obtain that $n_{SL(2,\boldsymbol{F}_3)} = 4$. Since $\varphi(|SL(2, \boldsymbol{F}_3)|) = 8$, we have

$$n_G = \frac{1}{2}\varphi(|G|) .$$

For Types V and VI, we have $G_0 \cong SL(2, \boldsymbol{F}_p) \times C$, where C is a cyclic group and $(|SL(2, \boldsymbol{F}_p)|, |C|) = 1$. Lemmas 6 and 7 and Example 5 imply that

$$n_G = \frac{n_{SL(2,\boldsymbol{F}_p)}}{\varphi(|SL(2, \boldsymbol{F}_p)|)} \varphi(|G|) ,$$

as above. The proof of the Theorem is complete.

REMARK. We have proven that the calculation of $n_{SL(2,\boldsymbol{F}_p)}$ for every Fermat prime p completes the calculation of n_G for every finite group G. For example, by using computer, we obtain $n_{SL(2,\boldsymbol{F}_5)} = 8$. Since $\varphi(|SL(2, \boldsymbol{F}_5)|) = 32$, we then have

$$n_G = \frac{1}{4}\varphi(|G|) \quad \text{if } G \text{ is of Type V } (p = 5) \text{ or VI } (p = 5)\,.$$

We do not yet calculate $n_{SL(2,\boldsymbol{F}_p)}$ for Fermat primes $p \geq 17$.

REFERENCES

[1] Y. ODAI, On the group of units of an abelian extension of an algebraic number field, Proc. Japan Acad. Ser. A 64 (1988), 304–306.

[2] M. SUZUKI, Group theory I, II, Grundlehren Math. Wiss. 247, 248, Springer-Verlag, Berlin-Heidelberg-New York, 1982, 1986.

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

GRADUATE SCHOOL OF MATHEMATICS
NAGOYA UNIVERSITY
NAGOYA 464-8602
JAPAN