Y. Kitaoka
Nagoya Math. J.
Vol. 146 (1997), 131–148

FINITE ARITHMETIC SUBGROUPS OF GL_n, V

YOSHIYUKI KITAOKA

Abstract. Let K be a finite Galois extension of the rational number field $\mathbf{Q}$ and G a $Gal(K/\mathbf{Q})$-stable finite subgroup of $GL_n(O_K)$. We have shown that G is of A-type in several cases under some restrictions on K. In this paper, we show that it is true for $n = 2$ without any restrictions on K.

Let K be a finite Galois extension of the rational number field $\mathbf{Q}$ with Galois group Γ and let G be a Γ-stable finite subgroup of $GL_n(O_K)$. Here O_K stands for the ring of integers in K and we define the action of $\sigma \in \Gamma$ on $g = (g_{ij}) \in GL_n(O_K)$ by $\sigma(g) := (\sigma(g_{ij}))$. G being Γ-stable means that $\sigma(g) \in G$ for every $\sigma \in \Gamma$ and every $g \in G$. To state the property of such a group, we introduce the notion of A-type. Let H be a subgroup of $GL_n(O_K)$. We denote by $L = \mathbf{Z}[e_1, \ldots, e_n]$ a free module over $\mathbf{Z}$ and we make $h = (h_{ij}) \in H$ act on $O_K L$ by $h(e_i) = \sum_{j=1}^{n} h_{ij} e_j$. If there exists a decomposition $L = \oplus_{i=1}^{k} L_i$ such that for every $h \in H$, we can take roots of unity $\epsilon_i(h)$ $(1 \le i \le k)$ and a permutation $s(h)$ so that $\epsilon_i(h) h L_i = L_{s(h)(i)}$ for $i = 1, 2, \ldots, k$, then we say that H is of A-type.

We have shown in [4] that if Γ is nilpotent, then G is of A-type. The aim of this paper is to show the following

THEOREM. *Let K be a finite Galois extension of the rational number field $\mathbf{Q}$ with Galois group Γ and let G be a Γ-stable finite subgroup of $GL_2(O_K)$. Then G is of A-type.*

Through this paper, algebraic number fields are finite over the rational number field $\mathbf{Q}$. For an algebraic number field K, we denote the ring of integers in K by O_K. When K is the rational number field $\mathbf{Q}$, we use $\mathbf{Z}$ instead of $O_{\mathbf{Q}}$, as usual. An algebraic number field is called abelian if it is a Galois extension over $\mathbf{Q}$ with abelian Galois group. Let K be an algebraic number field and $\mathfrak{p}$ an integral ideal of K, and let G be a subgroup of $GL_n(O_K)$. Then we set

$$G(\mathfrak{p}) := \{g \in G \mid g \equiv 1_n \bmod \mathfrak{p}\},$$

Received June 5, 1995.

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

where 1_n stands for the identity matrix of size n. For elements g, h in a group, we set

$$[g, h] := ghg^{-1}h^{-1}.$$

§1.

In this section, we give the proof of the theorem except the proof of Lemma 1.6, which is given in the succeeding sections.

LEMMA 1.1. (Theorem 1 in [3]) *Let K be an abelian extension of $\mathbf{Q}$ with Galois group Γ. Then a Γ-stable finite subgroup of $GL_n(O_K)$ is of A-type.*

LEMMA 1.2. (Lemma 3 in [3]) *Let $K/\mathbf{Q}$ be a Galois extension with Galois group Γ and G a Γ-stable finite subgroup of $GL_n(O_K)$. Let Γ' be the commutator subgroup of Γ and K' the maximal abelian subfield of K corresponding to Γ'. Suppose the following conditions:*

1. *If a proper subfield F of K is a Galois extension of $\mathbf{Q}$, then $G \cap GL_n(F) \subset GL_n(K')$.*
2. *At least two rational primes ramify in K.*

Then G is of A-type.

We prove the theorem by induction on $[K : \mathbf{Q}]$. By virtue of Lemmas 1.1, 1.2, we may assume that the number of prime numbers ramified in K is one.

LEMMA 1.3. *Let K be an algebraic number field and suppose that $g \in GL_n(O_K)$ is of finite order and $g \equiv 1_n \bmod \mathfrak{p}$ for a prime ideal $\mathfrak{p}$ of K. Then the order of g is a power of the prime number p which lies below $\mathfrak{p}$.*

Proof. Let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$ and π a prime element of $K_\mathfrak{p}$. Suppose that the order of g is divided by a prime number q different from p. Let h be a power of g whose order is q. We write $h = 1_n + \pi^r A$, where A is an integral matrix and $\pi^{-1}A$ is not integral. Then we have

$$1_n = h^q = 1_n + \sum_{k=1}^{q} \binom{q}{k} (\pi^r A)^k,$$

and hence

$$q\pi^r A \equiv 0 \bmod \pi^{2r}.$$

Since $q \not\equiv 0 \bmod \pi$, $A \not\equiv 0 \bmod \pi$ and $r > 0$, it is a contradiction. □

LEMMA 1.4. (Lemma 1 in [4]) *Let F be an abelian extension of $\mathbf{Q}$ with Galois group Γ, and $\mathfrak{p}$ a prime ideal. Let G be a Γ-stable finite subgroup of $GL_n(O_F)$. Then there exists an integral matrix $T \in GL_n(\mathbf{Z})$ such that $\{TgT^{-1} \mid g \in G, g \equiv 1_n \bmod \mathfrak{p}\}$ consists of diagonal matrices.*

LEMMA 1.5. *Let K be a Galois extension of $\mathbf{Q}$ with Galois group Γ, and let G be a Γ-stable commutative finite subgroup of $GL_2(O_K)$. Then G is contained in $GL_2(K')$, where K' is the maximal abelian subfield of K.*

Proof. If G consists of scalar matrices, the assertion is clear, and hence we assume that G contains a non-scalar matrix. Let m be the exponent of G and it is obvious that we have only to prove the assertion for $K(1^{1/m})$ instead of K. So we may assume $1^{1/m} \in K$; then there is a matrix $T \in GL_2(K)$ so that $T^{-1}GT$ consists of diagonal matrices. Take any non-scalar element $g \in G$ and put

$$g = T \begin{pmatrix} \zeta_1 & 0 \\ 0 & \zeta_2 \end{pmatrix} T^{-1}.$$

Take $\sigma \in \Gamma$ and set

$$u := T^{-1}\sigma(T) = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix};$$

then $\sigma(g) \in G$ implies $u \begin{pmatrix} \sigma(\zeta_1) & 0 \\ 0 & \sigma(\zeta_2) \end{pmatrix} = \begin{pmatrix} \eta_1 & 0 \\ 0 & \eta_2 \end{pmatrix} u$ for some roots of unity η_1, η_2, and hence $u_1\sigma(\zeta_1) = u_1\eta_1$, $u_2\sigma(\zeta_2) = u_2\eta_1$, $u_3\sigma(\zeta_1) = u_3\eta_2$ and $u_4\sigma(\zeta_2) = u_4\eta_2$. Suppose $u_1u_2 \neq 0$; then we have $\sigma(\zeta_1) = \eta_1$ and $\sigma(\zeta_2) = \eta_1$, which contradict $\zeta_1 \neq \zeta_2$. Thus we have $u_1u_2 = 0$. Suppose $u_3u_4 \neq 0$; then we have $\sigma(\zeta_1) = \eta_2$ and $\sigma(\zeta_2) = \eta_2$, which are the contradiction, similarly. Thus we have $u_1u_2 = u_3u_4 = 0$ and hence

$$T^{-1}\sigma(T) = u = \begin{pmatrix} u_1 & 0 \\ 0 & u_4 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & u_2 \\ u_3 & 0 \end{pmatrix}.$$

By setting

$$\Gamma_0 := \left\{ \sigma \in \Gamma \;\middle|\; \sigma(T) = T \begin{pmatrix} u_1 & 0 \\ 0 & u_4 \end{pmatrix} \text{ for some } u_1, u_4 \in K \right\},$$

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

the index $[\Gamma : \Gamma_0]$ is at most 2 and Γ_0 contains the commutator subgroup of Γ. Let F be the subfield corresponding to Γ_0; then $F \subset K'$. Set

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We divide the proof into the three cases.

(i) The case of $c = 0$.

For $\sigma \in \Gamma_0$, we have

$$\begin{pmatrix} \sigma(a) & \sigma(b) \\ 0 & \sigma(d) \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} u_1 & 0 \\ 0 & u_4 \end{pmatrix},$$

and so $\sigma(b/d) = b/d$. Hence $t := b/d$ is in the field F. Then we have, for roots of unity γ_1, γ_2,

$$\begin{aligned} T \begin{pmatrix} \gamma_1 & 0 \\ 0 & \gamma_2 \end{pmatrix} T^{-1} &= \begin{pmatrix} a & dt \\ 0 & d \end{pmatrix} \begin{pmatrix} \gamma_1 & 0 \\ 0 & \gamma_2 \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}t \\ 0 & d^{-1} \end{pmatrix} \\ &= \begin{pmatrix} a\gamma_1 & dt\gamma_2 \\ 0 & d\gamma_2 \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}t \\ 0 & d^{-1} \end{pmatrix} \\ &= \begin{pmatrix} \gamma_1 & (\gamma_2 - \gamma_1)t \\ 0 & \gamma_2 \end{pmatrix} \in GL_2(K'). \end{aligned}$$

Thus G is in $GL_2(K')$.

(ii) The case of $d = 0$.

For $\sigma \in \Gamma_0$, we have

$$\begin{pmatrix} \sigma(a) & \sigma(b) \\ \sigma(c) & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \begin{pmatrix} u_1 & 0 \\ 0 & u_4 \end{pmatrix},$$

and so $\sigma(a/c) = a/c$ and hence $t := a/c$ belongs to F. Then we have, for roots of unity γ_1, γ_2,

$$\begin{aligned} T \begin{pmatrix} \gamma_1 & 0 \\ 0 & \gamma_2 \end{pmatrix} T^{-1} &= \begin{pmatrix} ct & b \\ c & 0 \end{pmatrix} \begin{pmatrix} \gamma_1 & 0 \\ 0 & \gamma_2 \end{pmatrix} \begin{pmatrix} 0 & c^{-1} \\ b^{-1} & -b^{-1}t \end{pmatrix} \\ &= \begin{pmatrix} ct\gamma_1 & b\gamma_2 \\ c\gamma_1 & 0 \end{pmatrix} \begin{pmatrix} 0 & c^{-1} \\ b^{-1} & -b^{-1}t \end{pmatrix} \\ &= \begin{pmatrix} \gamma_2 & (\gamma_1 - \gamma_2)t \\ 0 & \gamma_1 \end{pmatrix} \in GL_2(K'). \end{aligned}$$

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

Hence G is contained in $GL_2(K')$.

(iii) The case of $cd \neq 0$.

For $\sigma \in \Gamma_0$, we have

$$\begin{pmatrix} \sigma(a) & \sigma(b) \\ \sigma(c) & \sigma(d) \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u_1 & 0 \\ 0 & u_4 \end{pmatrix},$$

and so $\sigma(a/c) = a/c$, $\sigma(b/d) = b/d$ and hence $t_1 := a/c$, $t_2 := b/d$ are in F. Then we have, for roots of unity γ_1, γ_2,

$$\begin{aligned} T \begin{pmatrix} \gamma_1 & 0 \\ 0 & \gamma_2 \end{pmatrix} T^{-1} &= \begin{pmatrix} ct_1 & dt_2 \\ c & d \end{pmatrix} \begin{pmatrix} \gamma_1 & 0 \\ 0 & \gamma_2 \end{pmatrix} \begin{pmatrix} ct_1 & dt_2 \\ c & d \end{pmatrix}^{-1} \\ &= \begin{pmatrix} t_1 & t_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} \gamma_1 & 0 \\ 0 & \gamma_2 \end{pmatrix} \left(\begin{pmatrix} t_1 & t_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \right)^{-1} \\ &= \begin{pmatrix} t_1 & t_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \gamma_1 & 0 \\ 0 & \gamma_2 \end{pmatrix} \begin{pmatrix} t_1 & t_2 \\ 1 & 1 \end{pmatrix}^{-1} \in GL_2(K'). \end{aligned}$$

Thus we have shown $G \subset GL_2(K')$.

LEMMA 1.6. *Let p be a prime number and let K be a Galois extension of $\mathbf{Q}$ with Galois group Γ where p is the only rational prime number ramified in K, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ be all the prime ideals in K lying above p. Let G be a Γ-stable finite subgroup of $GL_2(O_K)$. Then the subgroup of G generated by $G(\mathfrak{p}_1), \ldots, G(\mathfrak{p}_g)$ is commutative.*

The proof for an odd prime p (resp. 2) is given in the second (resp. third) section.

LEMMA 1.7. *Let p be a prime number, and K a Galois extension of $\mathbf{Q}$ with Galois group Γ where p is the only prime number ramified in K, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ be the prime ideals in K lying above p. Let G be a Γ-stable finite subgroup of $GL_2(O_K)$. Then we have $G(\mathfrak{p}_1) = \cdots = G(\mathfrak{p}_g) \subset GL_2(K')$, where K' is the maximal abelian subfield of K.*

Proof. By Lemma 1.6, the subgroup H generated by $G(\mathfrak{p}_1), \ldots, G(\mathfrak{p}_g)$ is an abelian Γ-stable subgroup of $GL_2(O_K)$. By Lemma 1.5, H is contained in $GL_2(K')$. Let $\mathfrak{p}$ be the unique prime ideal of K' lying above p;

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

then $G(\mathfrak{p}_i) \subset (G \cap GL_2(K'))(\mathfrak{p})$ follows from the fact $\mathfrak{p}_i \cap K' = \mathfrak{p}$. The inclusion $(G \cap GL_2(K'))(\mathfrak{p}) \subset G(\mathfrak{p}_i)$ is obvious and so we have $G(\mathfrak{p}_i) = (G \cap GL_2(K'))(\mathfrak{p})$. □

LEMMA 1.8. *Let p be a prime number and K a Galois extension of $\mathbf{Q}$ with Galois group Γ. We suppose that p is the only prime number that ramifies in K, and let $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ be the prime ideals of K lying above p. Let G be a Γ-stable finite subgroup of $GL_n(O_K)$ and suppose that $G(\mathfrak{p}_1) = \cdots = G(\mathfrak{p}_g)$ is in $GL_n(K')$ where K' is the maximal abelian subfield of K. Then G is of A-type.*

Proof. Let $g \in G$ and set $A_\sigma := \sigma(g)g^{-1}$ for $\sigma \in \Gamma$; we have, for $\sigma, \mu \in \Gamma$

$$A_{\mu\sigma}g = \mu\sigma(g) = \mu(A_\sigma g) = \mu(A_\sigma)A_\mu g$$

and hence $A_{\mu\sigma} = \mu(A_\sigma)A_\mu$. Since K' is abelian over $\mathbf{Q}$, the prime ideal $\mathfrak{p}$ in K' lying above p is uniquely determined and $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ lie above $\mathfrak{p}$. By the assumption $G(\mathfrak{p}_1) = \cdots = G(\mathfrak{p}_g) \subset GL_n(K')$, we have $G(\mathfrak{p}_1) \subset (G \cap GL_n(K'))(\mathfrak{p})$. Therefore, by Lemma 1.4, there exists a matrix $T \in GL_n(\mathbf{Z})$ such that $\{TgT^{-1} \mid g \in G(\mathfrak{p}_1)\}$ consists of diagonal matrices. Considering TGT^{-1} instead of G, we may assume that $G(\mathfrak{p}_1)$ and hence all $G(\mathfrak{p}_i)$ consist of diagonal matrices without loss of generality. Let V_i be the inertia group for the prime ideal $\mathfrak{p}_i$. For $\sigma \in V_i$, we have $\sigma(g)g^{-1} \equiv 1_n \bmod \mathfrak{p}_i$ and hence $A_\sigma \in G(\mathfrak{p}_i)$ is diagonal. Since p is the only rational prime that ramifies in K, $V_1, \dots, V_g$ generate Γ and so for every $\sigma \in \Gamma$, A_σ is diagonal. By Lemma 1 in [3], there exists a diagonal matrix $A \in GL_n(K)$ such that $A_\sigma = \sigma(A^{-1})A$ and $A^w \in GL_n(\mathbf{Q})$, where w is the number of roots of unity in K. Thus we have $\sigma(g)g^{-1} = A_\sigma = \sigma(A^{-1})A$ and hence $\sigma(Ag) = Ag$ for every $\sigma \in \Gamma$. Therefore Ag is in $GL_n(\mathbf{Q})$ and we write $Ag = Dh$, where $D, h \in GL_n(\mathbf{Q})$, D is diagonal and the greatest common divisor of entries of each row of h is one. Then $g = (A^{-1}D)h$ implies $A^{-1}D \in GL_n(O_K)$, since the entries of each row of h and g are relatively prime. Now $(A^{-1}D)^w = (A^w)^{-1}D^w \in GL_n(\mathbf{Q})$ yields that the diagonal entries of $A^{-1}D$ are roots of unity. Thus we have $g = (A^{-1}D)h \in GL_n(K')$ and hence $G \subset GL_n(K')$. By Lemma 1.1, G is of A-type. □

Under the postposition of the proof of Lemma 1.6, we have completed the proof of the theorem.

Remark. To generalize the theorem to an arbitrary size of matrices, it is enough to generalize Lemmas 1.5, 1.6.

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

§2. The proof of Lemma 1.6 for odd prime numbers

In this section, p is an odd prime number and K is a Galois extension of $\mathbf{Q}$ with Galois group Γ such that p is the only prime number ramified in K, and G is a Γ-stable finite subgroup of $GL_2(O_K)$. We remark that if a root of unity ϵ is congruent to 1 modulo a prime ideal of K lying above p, the order of ϵ is a power of p, and that if $[g,h] = ghg^{-1}h^{-1}$ is scalar for $g, h \in GL_2(K)$, then $[g,h] = \pm 1_2$.

LEMMA 2.1. *Let $\mathfrak{p}$ be a prime ideal of K lying above p. Then $G(\mathfrak{p})$ is commutative.*

Proof. Suppose that $G(\mathfrak{p})$ is not commutative. By regarding it as a representation of degree 2, it is an irreducible representation and so the center Z of $G(\mathfrak{p})$ consists of scalar matrices by Schur's lemma. The assumption implies $G(\mathfrak{p}) \neq Z$ and the order of $G(\mathfrak{p})$ is a power of the prime number p by Lemma 1.3. Hence $G(\mathfrak{p})/Z$ is a non-trivial p-group, and we can take $h \in G(\mathfrak{p}) \setminus Z$ so that h gives a non-trivial center of $G(\mathfrak{p})/Z$. Then we have, for $g \in G(\mathfrak{p})$

$$[g,h] \in Z,$$

and hence there exists $s \in K^\times$ such that $[g,h] = s1_2$ with $s = \pm 1$. On the other hand, $s1_2 = [g,h] \in G(\mathfrak{p})$ yields that the order of s is a power of p. Hence we have $s = 1$. This means that h is a center of $G(\mathfrak{p})$, which contradicts $h \notin Z$. ∎

LEMMA 2.2. *Let $\mathfrak{p}_1$, $\mathfrak{p}_2$ be prime ideals in K lying above p. Then the elements in $G(\mathfrak{p}_1)$ and $G(\mathfrak{p}_2)$ are commutative.*

Proof. (i) The case that $G(\mathfrak{p}_1) \cap G(\mathfrak{p}_2)$ contains a non-scalar matrix g.

By the previous lemma, $G(\mathfrak{p}_1)$ is commutative and hence there exists a complex regular matrix T such that $T^{-1}G(\mathfrak{p}_1)T$ consists of diagonal matrices and put $g = T\begin{pmatrix} \zeta_1 & 0 \\ 0 & \zeta_2 \end{pmatrix}T^{-1}$ with $\zeta_1 \neq \zeta_2$. Since $G(\mathfrak{p}_2)$ is commutative, we have $gh = hg$ for $h \in G(\mathfrak{p}_2)$. Putting $h := T\begin{pmatrix} a & b \\ c & d \end{pmatrix}T^{-1}$, we have

$$\begin{pmatrix} \zeta_1 a & \zeta_1 b \\ \zeta_2 c & \zeta_2 d \end{pmatrix} = \begin{pmatrix} \zeta_1 a & \zeta_2 b \\ \zeta_1 c & \zeta_2 d \end{pmatrix},$$

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

and hence $b = c = 0$ by virtue of $\zeta_1 \neq \zeta_2$. Hence $T^{-1}G(\mathfrak{p}_2)T$ also consists of diagonal matrices, and so the elements of $G(\mathfrak{p}_1)$ and $G(\mathfrak{p}_2)$ are commutative.

(ii) The case that $G(\mathfrak{p}_1) \cap G(\mathfrak{p}_2)$ consists of scalar matrices.

Take $g_i \in G(\mathfrak{p}_i)$ $(i = 1, 2)$; then $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1} \in G(\mathfrak{p}_1) \cap G(\mathfrak{p}_2)$ is clear and there exists $s \in K^\times$ such that $[g_1, g_2] = s1_2$ with $s = \pm 1$. By $[g_1, g_2] \in G(\mathfrak{p}_1)$, the order of $[g_1, g_2]$ and hence of s is a power of p. Hence we have $s = 1$. Thus g_1, g_2 are commutative. □

Thus Lemma 1.6 has been proved for odd primes.

§3. The proof of Lemma 1.6 for $p = 2$

Through this section, K is a Galois extension of $\mathbf{Q}$ with Galois group Γ such that 2 is the only prime number ramified in K, and G is a Γ-stable finite subgroup of $GL_2(O_K)$. F_2 denotes $\mathbf{Z}/2\mathbf{Z}$. We remark that the group of automorphisms of a vector space over F_2 of dimension 2 is isomorphic to the symmetric group $\mathfrak{S}_3$ of degree 3.

LEMMA 3.1. *Let* $h := T\begin{pmatrix} \zeta_1 & 0 \\ 0 & \zeta_2 \end{pmatrix}T^{-1}$ *be a regular matrix, where* $\zeta_1 \neq \zeta_2$, $\zeta_1\zeta_2 \neq 0$ *and a matrix* T *is regular. Let* $g := T\begin{pmatrix} a & b \\ c & d \end{pmatrix}T^{-1}$ *be a regular complex matrix.*

If $[g, h] = 1_2$, *then we have* $g = T\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}T^{-1}$.

If $[g, h] = -1_2$, *then we have* $\zeta_1 = -\zeta_2$ *and* $g = T\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}T^{-1}$.

Proof. Since

$$gh = T\begin{pmatrix} a\zeta_1 & b\zeta_2 \\ c\zeta_1 & d\zeta_2 \end{pmatrix}T^{-1}, \quad hg = T\begin{pmatrix} a\zeta_1 & b\zeta_1 \\ c\zeta_2 & d\zeta_2 \end{pmatrix}T^{-1},$$

$[g, h] = 1_2$ implies $b = c = 0$, and $[g, h] = -1_2$ implies $a = d = 0$, and so $b \neq 0$ and then we have $\zeta_1 = -\zeta_2$. □

LEMMA 3.2. *Let* $\mathfrak{p}$ *be a prime ideal of* K *lying above* 2. *Suppose that* $G(\mathfrak{p})$ *is not commutative. Then the center* Z *of* G *is equal to the center of* $G(\mathfrak{p})$ *and it consists of the scalar matrices in* G, *and one of the following properties holds:*

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

1. *$G(\mathfrak{p})/Z \cong F_2 \oplus F_2$ and for $g \in G(\mathfrak{p}) \setminus Z, \mathrm{tr}(g) = 0$ holds. Moreover, for h_1, $h_2 \in G(\mathfrak{p}) \setminus Z$ we have $[h_1, h_2] = -1_2$ if $h_1 Z \neq h_2 Z$.*

2. *The order of the center of $G(\mathfrak{p})/Z$ is two and a commutative subgroup G' of $G(\mathfrak{p})$ of index 2 is unique.*

Proof. By regarding $G(\mathfrak{p})$ itself as a representation of degree 2, it is irreducible, since $G(\mathfrak{p})$ is not commutative. Hence its center $Z(G(\mathfrak{p}))$ consists of scalar matrices. Similarly, the center Z of G consists of scalar matrices. The inclusion $Z(G(\mathfrak{p})) \subset Z$ is clear. Suppose $g = \epsilon 1_2 \in Z$. Since g is of finite order, ϵ is a root of unity and 2 is the only prime number which ramifies in K, the order of ϵ is a power of 2. Let $\mathfrak{P}$ be the unique prime ideal of the maximal abelian subfield of K lying below $\mathfrak{p}$; then $\epsilon \equiv 1 \bmod \mathfrak{P}$, which means $g = \epsilon 1_2 \in G(\mathfrak{P}) \subset G(\mathfrak{p})$. Thus we have shown $Z(G(\mathfrak{p})) = Z$. By virtue of Lemma 1.3, the orders of the elements of $G(\mathfrak{p})$ are powers of 2 and hence $G(\mathfrak{p})/Z$ is a 2-group. Therefore we can choose an element $h \in G(\mathfrak{p}) \setminus Z$ so that hZ is a non-trivial center of $G(\mathfrak{p})/Z$. This yields $[g, h] \in Z$ for $g \in G(\mathfrak{p})$, and hence

$$[g, h] = \pm 1_2 \text{ for every } g \in G(\mathfrak{p}).$$

Setting

$$G_0 := \{g \in G(\mathfrak{p}) \mid [g, h] = 1_2\},$$

we have $[G(\mathfrak{p}) : G_0] \leq 2$. We take a regular matrix T so that

$$h = T \begin{pmatrix} h_1 & 0 \\ 0 & h_4 \end{pmatrix} T^{-1} \qquad (h_1 \neq h_4).$$

Lemma 3.1 yields that $T^{-1} G_0 T$ consists of diagonal matrices and hence G_0 is commutative. Since $G(\mathfrak{p})$ is not commutative, we have $G(\mathfrak{p}) \neq G_0$ and so

$$(1) \qquad [G(\mathfrak{p}) : G_0] = 2$$

and hence there exists an element $g \in G(\mathfrak{p})$ so that $[g, h] = -1_2$. Then Lemma 3.1 yields that

$$h_4 = -h_1.$$

We divide the proof into two cases.

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

(i) The case that there exists an element $c \in G(\mathfrak{p})$ which gives a center of $G(\mathfrak{p})/Z$, but is not in G_0.

The property $[c, h] = -1_2$ implies $c = T\begin{pmatrix} 0 & c_2 \\ c_3 & 0 \end{pmatrix}T^{-1}$ by virtue of Lemma 3.1. Then $\{Z, hZ, cZ, hcZ\}$ is a subgroup of $G(\mathfrak{p})/Z$ and is isomorphic to $F_2 \oplus F_2$. It is easy to see $[c, h] = [c, hc] = [h, hc] = -1_2$. Once $[G(\mathfrak{p}) : Z] = 4$ has been proved, this case (i) gives the first case in the lemma. By virtue of (1), we have only to prove $[G_0 : Z] = 2$, and as a matter of fact we show

$$G_0 = Z \cup hZ.$$

$G_0 \supset Z \cup hZ$ is clear. Let us take $f \in G_0$. By virtue of Lemma 3.1, we have $f = T\begin{pmatrix} f_1 & 0 \\ 0 & f_4 \end{pmatrix}T^{-1}$. Since c gives a center of $G(\mathfrak{p})/Z$, there is a complex number s so that $[c, f] = s1_2$ with $s = \pm 1$. By noting that

$$\begin{aligned}[c, f] &= T\begin{pmatrix} 0 & c_2 \\ c_3 & 0 \end{pmatrix}\begin{pmatrix} f_1 & 0 \\ 0 & f_4 \end{pmatrix}\begin{pmatrix} 0 & c_2 \\ c_3 & 0 \end{pmatrix}^{-1}\begin{pmatrix} f_1 & 0 \\ 0 & f_4 \end{pmatrix}^{-1}T^{-1} \\ &= T\begin{pmatrix} f_4/f_1 & 0 \\ 0 & f_1/f_4 \end{pmatrix}T^{-1},\end{aligned}$$

if the condition $s = 1$ holds, then $f_1 = f_4$ and hence $f \in Z$. The condition $s = -1$ implies $f_4 = -f_1$ and so $f \in hZ$. Thus we have shown $G_0 = Z \cup hZ$ and complete the case (i).

(ii) The case that every element $c \in G(\mathfrak{p})$ which gives a center of $G(\mathfrak{p})/Z$ is contained in G_0.

First, we show that the center of $G(\mathfrak{p})/Z$ is $\{Z, hZ\}$. Let $c \in G(\mathfrak{p})$ give a center of $G(\mathfrak{p})/Z$. We must show $c \in Z \cup hZ$. The assumption implies $[c, h] = 1_2$ and hence $c = T\begin{pmatrix} c_1 & 0 \\ 0 & c_4 \end{pmatrix}T^{-1}$ by Lemma 3.1. Take an element $g \in G(\mathfrak{p}) \setminus G_0$; then $[g, h] = -1_2$ yields $g = T\begin{pmatrix} 0 & g_2 \\ g_3 & 0 \end{pmatrix}T^{-1}$ Since c gives a center of $G(\mathfrak{p})/Z$, i.e., $[g, c] \in Z$, we have $[g, c] = s1_2$ with $s = \pm 1$. On the other hand, from $[g, c] = T\begin{pmatrix} c_4/c_1 & 0 \\ 0 & c_1/c_4 \end{pmatrix}T^{-1}$ follows that $c_4 = \pm c_1$, which means $c \in Z$ or hZ. Thus we have shown that $\{Z, hZ\}$

contains the center of $G(\mathfrak{p})/Z$. The converse inclusion is clear, and hence the center of $G(\mathfrak{p})/Z$ is $\{Z, hZ\}$.

We recall that G_0 is a commutative subgroup of $G(\mathfrak{p})$ with $[G(\mathfrak{p}) : G_0] = 2$. Let S be a commutative subgroup of $G(\mathfrak{p})$ with $[G(\mathfrak{p}) : S] = 2$, and suppose $S \neq G_0$. We show $[G(\mathfrak{p}) : Z] \leq 4$. The canonical homomorphism $\phi : G_0/G_1 \mapsto G(\mathfrak{p})/S$ is clearly injective, where we put $G_1 := G_0 \cap S$. By the assumption, $G_0/G_1 \neq \{1\}$ and $[G(\mathfrak{p}) : S] = 2$ hold and so ϕ is isomorphism. Thus we have $[G_0 : G_1] = 2$ and hence $[G(\mathfrak{p}) : G_1] = 4$. We take $g \in G(\mathfrak{p}) \setminus G_0$, $g' \in G_0 \setminus G_1$; then $G(\mathfrak{p}) = G_1 \cup g'G_1 \cup gG_1 \cup gg'G_1$ is trivial. On the other hand, $S \neq G_0$ and $[S : G_1] = 2$ imply $S = G_1 \cup gG_1$ or $G_1 \cup gg'G_1$. Neither g nor gg' is contained in G_0. Putting $f = g$ or gg', we have $S = G_1 \cup fG_1$ and $f \in G(\mathfrak{p}) \setminus G_0$. Lemma 3.1 yields $f = T \begin{pmatrix} 0 & f_2 \\ f_3 & 0 \end{pmatrix} T^{-1}$ by $[f, h] = -1_2$. Take an element $b \in G_1$. Since b is commutative with h by virtue of $b \in G_0$, we can write $b = T \begin{pmatrix} b_1 & 0 \\ 0 & b_4 \end{pmatrix} T^{-1}$. On the other hand, S is commutative and so $b, f \in S$ implies $[b, f] = 1_2$, which implies $b_1 = b_4$, i.e., $b \in Z$. Thus $G_1 \subset Z$ follows and then $[G(\mathfrak{p}) : G_1] = 4$ implies $[G(\mathfrak{p}) : Z] \leq 4$. Thus $G(\mathfrak{p})/Z$ is commutative. As we have shown that the center of $G(\mathfrak{p})/Z$ is equal to $\{Z, hZ\}$, we have $[G(\mathfrak{p}) : Z] = 2$. It yields that $G(\mathfrak{p})$ is commutative, which contradicts our assumption. Thus this case gives the second case in the lemma. □

LEMMA 3.3. *Let $\mathfrak{p}$ be a prime ideal of K lying above 2. Suppose that $G(\mathfrak{p})$ is not commutative. Then the case (2) in Lemma 3.2 does not occur.*

Proof. Let Z be the center of $G(\mathfrak{p})$, and suppose that the case (2) occurs; then the order of the center of $G(\mathfrak{p})/Z$ is two and a commutative subgroup G_0 of $G(\mathfrak{p})$ of index 2 is uniquely determined and is equal to $\{g \in G(\mathfrak{p}) \mid [g, h] = 1_2\}$ as in the proof of Lemma 3.2, where $h \in G(\mathfrak{p})$ is an element such that hZ is the unique non-trivial center of $G(\mathfrak{p})/Z$. Since $G(\mathfrak{p})$ is a normal subgroup of G, the mapping $x \mapsto gxg^{-1}$ induces an automorphism of $G(\mathfrak{p})/Z$ for every $g \in G$. Hence $g(hZ)g^{-1}$ is the non-trivial center of $G(\mathfrak{p})/Z$ and so we have

$$ghg^{-1} \in hZ \quad \text{for every } g \in G,$$

which implies $[g, h] \in Z$, and by virtue of Lemma 3.2, Z consists of scalar matrices, and hence we have

$$(1) \qquad [g, h] = \pm 1_2 \quad \text{for every } g \in G.$$

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

For $\sigma \in \Gamma$, we put

$$G_\sigma := \{g \mid g \in \sigma(G(\mathfrak{p})), [g,h] = 1_2\},$$

which is commutative by Lemma 3.1. We show

$$G_\sigma = \sigma(G_0).$$

The inequality $[\sigma(G(\mathfrak{p})) : G_\sigma] \leq 2$ follows from (1). If $[\sigma(G(\mathfrak{p})) : G_\sigma] = 1$, then $\sigma(G(\mathfrak{p}))$ is commutative, which contradicts the non-commutativity of $G(\mathfrak{p})$. Hence we have $[\sigma(G(\mathfrak{p})) : G_\sigma] = 2$, and $\sigma^{-1}(G_\sigma)$ is a commutative subgroup of $G(\mathfrak{p})$ of index 2, and hence $\sigma^{-1}(G_\sigma) = G_0$. Thus we have shown the claim.
We can take a matrix T so that $T^{-1}G_0T$ consists of diagonal matrices and put $h := T\begin{pmatrix}\zeta_1 & 0\\ 0 & \zeta_2\end{pmatrix}T^{-1}$. Since $\sigma(h)$ $(\in \sigma(G_0) = G_\sigma)$ is commutative with h for $\sigma \in \Gamma$, there exist η_1, η_2 such that $\sigma(h) = T\begin{pmatrix}\eta_1 & 0\\ 0 & \eta_2\end{pmatrix}T^{-1}$. Therefore the set $\{\sigma(h) \mid \sigma \in \Gamma\}$ generates a Γ-stable abelian finite subgroup G' of $GL_2(O_K)$. Hence Lemma 1.5 yields that $G' \subset GL_2(K')$, where K' is the maximal abelian subfield of K. Since there exists a matrix $S \in GL_2(\mathbf{Z})$ such that $S^{-1}G'S$ consists of diagonal matrices by Lemma 1.4, we may assume that $(h \in)$ G' consists of diagonal matrices without loss of generality, considering $S^{-1}GS$ instead of G. So, put $h := \begin{pmatrix}h_1 & 0\\ 0 & h_4\end{pmatrix}$, and the non-commutativity of $G(\mathfrak{p})$ implies the existence of an element $g \in G(\mathfrak{p})$ so that $[g,h] = -1_2$, noting (1) and Lemma 3.1. By the same lemma, we have $g = \begin{pmatrix}0 & g_2\\ g_3 & 0\end{pmatrix}$, which contradicts $g \in G(\mathfrak{p})$. Thus we have completed the proof. □

LEMMA 3.4. *Let $\mathfrak{p}$ be a prime ideal of K lying above 2. Suppose that $G(\mathfrak{p})$ is not commutative. Denote the center of G by Z. If the mapping $x \mapsto gxg^{-1}$ for $g \in G$ induces the trivial automorphism of $G(\mathfrak{p})/Z$, then we have $g \in G(\mathfrak{p})$.*

Proof. By virtue of Lemmas 3.2, 3.3, we can take $h_1, h_2 \in G(\mathfrak{p})$ so that $G(\mathfrak{p})/Z = \{Z, h_1Z, h_2Z, h_3Z\}$ with $h_3 := h_1h_2$. Suppose that the inner automorphism by $g \in G$ induces the trivial automorphism of $G(\mathfrak{p})/Z$; then

$$gh_i g^{-1} h_i^{-1} \in Z \qquad \text{for } i = 1, 2, 3.$$

Define $\epsilon_i = \pm 1$ by $[g, h_i] = \epsilon_i 1_2$. Moreover $h_3 = h_1 h_2$ implies $\epsilon_3 = \epsilon_1 \epsilon_2$. If $\epsilon_1 = \epsilon_2 = \epsilon_3 = 1$, and g is not scalar, then Lemma 3.1 implies that $T^{-1} h_i T$ is diagonal, taking a matrix T so that $T^{-1} g T$ is diagonal. Hence $G(\mathfrak{p})$ is commutative, which is a contradiction. Thus we may assume $\epsilon_1 = 1, \epsilon_2 = \epsilon_3 = -1$ without loss of generality. We can put $h_1 = T_1 \begin{pmatrix} h_1' & 0 \\ 0 & -h_1' \end{pmatrix} T_1^{-1}$ by Lemma 3.2; then by $[g, h_1] = 1_2$ and Lemma 3.1, we see $g = T_1 \begin{pmatrix} g_1 & 0 \\ 0 & g_4 \end{pmatrix} T_1^{-1}$. If $g_1 = g_4$, then g is scalar and so $g \in Z \subset G(\mathfrak{p})$. Suppose $g_1 \neq g_4$; then $[g, h_2] = -1_2$ and Lemma 3.1 implies $\mathrm{tr}(g) = 0$ and hence $g_4 = -g_1$ and gh_1^{-1} is scalar and so $gh_1^{-1} \in Z \subset G(\mathfrak{p})$, which implies $g \in G(\mathfrak{p})$, too. Thus we have completed the proof. □

LEMMA 3.5. *Let $\mathfrak{p}$ be a prime ideal of K lying above 2. Suppose that $G(\mathfrak{p})$ is not commutative. Then $G(\mathfrak{p})$ is Γ-stable.*

Proof. Let Z be the center of G; then $Z \subset G(\mathfrak{p})$ and $G(\mathfrak{p})/Z \cong F_2 \oplus F_2$. Define the automorphism $\phi(g)$ of $G(\mathfrak{p})/Z$ for $g \in G$ by $\phi(g)(xZ) = gxg^{-1}Z$. By the previous lemma, we have $\ker(\phi) = G(\mathfrak{p})$. Then $G/G(\mathfrak{p})$ is isomorphic to a subgroup of the symmetric group $\mathfrak{S}_3$ of degree 3. We divide the proof into three cases.

(i) The case that the order of $\phi(G)$ is odd.

In this case, $G(\mathfrak{p})/Z$ is the unique 2-Sylow subgroup of G/Z. Since for $\sigma \in \Gamma$, $\sigma(G(\mathfrak{p}))/Z$ is also a 2-Sylow subgroup of G/Z, we have $\sigma(G(\mathfrak{p})) = G(\mathfrak{p})$ for $\sigma \in \Gamma$.

(ii) The case that the order of $\phi(G)$ is 2.

We show that this case does not happen. Take an element $H \in G \backslash G(\mathfrak{p})$; then the assumption yields $G/G(\mathfrak{p}) = \{G(\mathfrak{p}), HG(\mathfrak{p})\}$. $\phi(H)$ is a non-trivial automorphism of order 2 of $G(\mathfrak{p})/Z$, and so we can take $h_1, h_2 \in G(\mathfrak{p}) \setminus Z$ so that

$$Hh_2H^{-1} \in h_1 Z, \quad Hh_1H^{-1} \in h_2 Z.$$

Then the representatives of G/Z are $\{1, h_1, h_2, h_1h_2, H, h_1H, h_2H, h_1h_2H\}$. The equalities $[h_1h_2, h_1]Z = [h_1h_2, h_2]Z = [h_1h_2, H]Z = Z$ imply that

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

h_1h_2Z is a center of G/Z. $[H, h_i]Z = h_1h_2Z$ for $i = 1, 2$ yield that the center of $G/Z = \{Z, h_1h_2Z\}$. Let $\sigma \in \Gamma$; then σ induces an automorphism of G/Z, and hence we have

$$\sigma(h_1h_2)Z = h_1h_2Z. \tag{1}$$

Hence $\{Z \cup h_1h_2Z\}$ is a Γ-stable finite abelian subgroup of $GL_2(O_K)$. By Lemma 1.5, (1) yields that $h_1h_2 \in GL_2(K')$, where K' is the maximal abelian subfield of K. Since $h_1h_2 \in G(\mathfrak{p}) \cap GL_2(K')$, as in the proof of Lemma 3.3, we may assume that h_1h_2 is diagonal and we see that $[h_1, h_1h_2] = -1_2$ follows from Lemma 3.2 and so Lemma 3.1 yields that $h_1 = \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \in G(\mathfrak{p})$, which is a contradiction. Thus this case does not happen.

(iii) The case of $\phi(G) \cong \mathfrak{S}_3$.

We can take generators $A, B(\in G)$ of $G/G(\mathfrak{p})$ so that $A^2 \in G(\mathfrak{p})$, $B^3 \in G(\mathfrak{p})$, $ABA^{-1} \in B^2G(\mathfrak{p})$. Then the 2-Sylow subgroups of G/Z are $\{AZ/Z, G(\mathfrak{p})/Z\}$, $\{BAB^{-1}Z/Z, G(\mathfrak{p})/Z\} = \{ABZ/Z, G(\mathfrak{p})/Z\}$ and $\{B^2AB^{-2}Z/Z, G(\mathfrak{p})/Z\} = \{AB^2Z/Z, G(\mathfrak{p})/Z\}$. Thus $G(\mathfrak{p})/Z$ is the intersection of all 2-Sylow subgroups of G/Z. Take $\sigma \in \Gamma$. Then σ induces an automorphism of G/Z and so $\sigma(G(\mathfrak{p})) = G(\mathfrak{p})$, that is $G(\mathfrak{p})$ is Γ-stable. □

LEMMA 3.6. *Let $\mathfrak{p}$ be a prime ideal of K lying above 2. Then $G(\mathfrak{p})$ is commutative.*

Proof. Suppose that $G(\mathfrak{p})$ is not commutative; then $G(\mathfrak{p})$ is Γ-stable by the previous lemma. Denote the center of G by Z. Every element $\sigma \in \Gamma$ induces an automorphism of $G(\mathfrak{p})/Z \cong F_2 \oplus F_2$, and so, by putting

$$\Gamma_0 := \{\sigma \mid \sigma(gZ) = gZ \text{ for every } g \in G(\mathfrak{p})\},$$

Γ/Γ_0 is isomorpic to a subgroup of $\mathfrak{S}_3$. Denote the subfield of K corresponding to Γ_0 by H. We divide the proof into four cases.

(i) The case of $\Gamma = \Gamma_0$.

We take $h_1, h_2 \in G(\mathfrak{p})$ so that the set $\{1_2, h_1, h_2, h_1h_2\}$ is a set of the representatives of $G(\mathfrak{p})/Z$. We may assume that K contains a sufficiently many roots of unity whose orders are powers of 2, and then we may assume

$$h_1h_2 = T \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} T^{-1}$$

for some $T \in GL_2(K)$ by Lemmas 3.1 and 3.2. The condition $\Gamma = \Gamma_0$ implies $\sigma(h_1h_2) = \epsilon_\sigma h_1h_2$ for some $\epsilon_\sigma \in K$. Comparing the determinants, we have $\epsilon_\sigma = \pm 1$. Putting

$$\Gamma_1 := \{\sigma \in \Gamma \mid \sigma(h_1h_2) = h_1h_2\},$$

we have $[\Gamma : \Gamma_1] \leq 2$. Hence the entries of h_1h_2 belong to a quadratic field. Let K' be the maximal abelian subfield of K; then by Lemma 1.1, we may assume that the elements of $G(\mathfrak{p}) \cap GL_2(K')$ are diagonal and hence h_1h_2 is diagonal. By Lemmas 3.1, 3.2 and $[h_1, h_1h_2] = -1_2$, we have $h_1 = \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$, which contradicts $h_1 \in G(\mathfrak{p})$.

(ii) The case of $\Gamma/\Gamma_0 \cong \mathbf{Z}/2\mathbf{Z}$.

We take an element $\sigma \in \Gamma \setminus \Gamma_0$; then σ induces an automorphism of $G(\mathfrak{p})/Z$ of order 2. Therefore there exists $h_1, h_2 \in G(\mathfrak{p})$ so that $\sigma(h_1) \in h_2Z$ and $\sigma(h_2) \in h_1Z$, and that the set $\{1_1, h_1, h_2, h_1h_2\}$ is a set of the representatives of $G(\mathfrak{p})/Z$. Hence we have $\sigma(h_1h_2) \in h_1h_2Z$, and so h_1h_2Z is Γ-stable. This is the contradiction as in the previous case.

(iii) The case of $\Gamma/\Gamma_0 \cong \mathbf{Z}/3\mathbf{Z}$.

The assumption yields that the field L corresponding to Γ_0 is a cyclic extension of $\mathbf{Q}$ with $[L : \mathbf{Q}] = 3$. But 2 is the only prime which ramifies in K and hence in L, which implies that $[L : \mathbf{Q}]$ is a power of 2. Thus we have a contradiction and this case does not happen.

(iv) The case of $\Gamma/\Gamma_0 \cong \mathfrak{S}_3$.

Let L be the subfield of K corresponding to Γ_0; then 2 is the only prime which ramifies in L. A quadratic field M in L is $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-2})$ or $\mathbf{Q}(\sqrt{2})$, and in such a field, the norm of the unique prime ideal lying above 2 is 2 and the class number is 1. The class field theory tells us that the degree of an abelian extension of M is a power of 2. This contradicts $[L : M] = 3$. Thus this case does not happen either. □

LEMMA 3.7. *Let $\mathfrak{p}_1, \mathfrak{p}_2$ be distinct prime ideals of K lying above 2. Suppose that $G(\mathfrak{p}_1) \cap G(\mathfrak{p}_2)$ consists of scalar matrices. If there exists $g_i \in G(\mathfrak{p}_i)$ $i = 1, 2$ such that $[g_1, g_2] \neq 1_2$, then we have $G(\mathfrak{p}_1) = Z \cup g_1Z$ and $G(\mathfrak{p}_2) = Z \cup g_2Z$, where Z is the subgroup consisting of the scalar matrices in G.*

https://doi.org/10.1017/S0027763000006231 Published online by Cambridge University Press

Proof. Since $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1} \in G(\mathfrak{p}_1) \cap G(\mathfrak{p}_2)$, $[g_1, g_2]$ is scalar and hence is equal to $\pm 1_2$. Moreover $[g_1, g_2] \neq 1_2$ implies that g_1, g_2 are not scalar and that $[g_1, g_2] = -1_2$. By Lemma 3.1, we can write

$$g_1 = T \begin{pmatrix} \zeta & 0 \\ 0 & -\zeta \end{pmatrix} T^{-1}, \qquad g_2 = T \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} T^{-1},$$

and the commutativity of $G(\mathfrak{p}_1)$ yields that $T^{-1}G(\mathfrak{p}_1)T$ consists of diagonal matrices. For $g \in G(\mathfrak{p}_1)$, we have $[g, g_2] \in G(\mathfrak{p}_1) \cap G(\mathfrak{p}_2)$ and hence $[g, g_2] = \pm 1_2$. Put $g = T \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} T^{-1}$; then we have

$$[g, g_2] = T \begin{pmatrix} a/d & 0 \\ 0 & d/a \end{pmatrix} T^{-1},$$

and hence $a = \pm d$. If $a = d$, then $g = a1_2$. Otherwise, we have $g = a\zeta^{-1} g_1$. Thus we have $G(\mathfrak{p}_1) \subset Z \cup g_1 Z$, and the converse inclusion is clear and hence $G(\mathfrak{p}_1) = Z \cup g_1 Z$. □

LEMMA 3.8. *Let $\mathfrak{p}_1, \mathfrak{p}_2$ be distinct prime ideals of K lying above 2. Then $G(\mathfrak{p}_1)$ and $G(\mathfrak{p}_2)$ are element-wise commutative.*

Proof. Let 2^n be the order of $G(\mathfrak{p}_1)$ and we may assume that K contains a primitive 2^nth root of unity without loss of generality. We divide the proof into two cases.

(i) The case that $G(\mathfrak{p}_1) \cap G(\mathfrak{p}_2)$ contains a non-scalar matrix.

Take a non-scalar matrix $g \in G(\mathfrak{p}_1) \cap G(\mathfrak{p}_2)$ and write

$$g = T \begin{pmatrix} \zeta_1 & 0 \\ 0 & \zeta_2 \end{pmatrix} T^{-1}.$$

Since $\zeta_1 \neq \zeta_2$ and $G(\mathfrak{p}_1)$, $G(\mathfrak{p}_2)$ are commutative, respectively, Lemma 3.1 yields that both $T^{-1}G(\mathfrak{p}_1)T$ and $T^{-1}G(\mathfrak{p}_2)T$ consist of diagonal matrices. Thus elements of $G(\mathfrak{p}_1)$ and $G(\mathfrak{p}_2)$ are commutative.

(ii) The case that $G(\mathfrak{p}_1) \cap G(\mathfrak{p}_2)$ consists of scalar matrices.

Denote the subgroup consisting of scalar matrices in G by Z. Suppose that $h_1 \in G(\mathfrak{p}_1)$, $h_2 \in G(\mathfrak{p}_2)$ are not commutative. By $[h_1, h_2] \in G(\mathfrak{p}_1) \cap G(\mathfrak{p}_2)$, $[h_1, h_2]$ is scalar and so $[h_1, h_2] = -1_2$. Since $G(\mathfrak{p}_1)$ is commutative, there exists $T \in GL_2(K)$ so that $T^{-1}G(\mathfrak{p}_1)T$ consists of diagonal matrices. By Lemma 3.1, we may assume

$$h_1 = T\begin{pmatrix} \zeta & 0 \\ 0 & -\zeta \end{pmatrix}T^{-1}, \qquad h_2 = T\begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}T^{-1}.$$

Since $\zeta 1_2$ is in Z, we may assume $\zeta = 1$ for h_1. By the previous lemma, we have $G(\mathfrak{p}_1) = Z \cup h_1 Z$ and $G(\mathfrak{p}_2) = Z \cup h_2 Z$. Now we claim that if $\mathfrak{p}$ is a prime ideal of K lying above 2, then $G(\mathfrak{p})$ is one of the following:

$$(1) \qquad \{Z \cup h_1 Z\}, \quad \{Z \cup h_2 Z\}, \quad \{Z \cup h_1 h_2 Z\}.$$

Let $\mathfrak{p}$ be a prime ideal lying above 2. Since there exists an element $\sigma \in \Gamma$ such that $G(\mathfrak{p}) = G(\sigma(\mathfrak{p}_1)) = \sigma(G(\mathfrak{p}_1))$, we have $[G(\mathfrak{p}) : Z] = 2$, and the trace of every element of $G(\mathfrak{p}) \setminus Z$ equals 0.

Suppose that $G(\mathfrak{p})$ and $G(\mathfrak{p}_1)$ are element-wise commutative; by virtue of Lemma 3.1, $T^{-1}G(\mathfrak{p})T$ consists of diagonal matrices, since $G(\mathfrak{p})$ is commutative with h_1. Hence $[G(\mathfrak{p}) : Z] = 2$ implies $G(\mathfrak{p}) = Z \cup hZ$ for some $h = T\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}T^{-1} = ah_1$. h, $h_1 \in G$ implies $a1_2 \in G$ and hence $a1_2 \in Z$. Thus $G(\mathfrak{p}) = G(\mathfrak{p}_1)$ follows.

Suppose that $G(\mathfrak{p})$ and $G(\mathfrak{p}_1)$ are not commutative; then we have $G(\mathfrak{p}) \neq G(\mathfrak{p}_1)$ and let $G(\mathfrak{p}) = Z \cup hZ$; then we have $[h, h_1] \in G(\mathfrak{p}) \cap G(\mathfrak{p}_1) = Z$, and hence $[h, h_1] = -1_2$, which implies $h = T\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}T^{-1}$. If $G(\mathfrak{p})$ and $G(\mathfrak{p}_2)$ are commutative, then $G(\mathfrak{p}) = G(\mathfrak{p}_2)$ follows as above. So, we may assume that $G(\mathfrak{p})$ and $G(\mathfrak{p}_2)$ are not commutative. Then we have $[h, h_2] = -1_2$ similarly as above, and hence $b\gamma = -\beta c$. Thus we obtain $h = -c\gamma^{-1}T\begin{pmatrix} 0 & \beta \\ -\gamma & 0 \end{pmatrix}T^{-1} = -c\gamma^{-1}h_1 h_2$, and so $G(\mathfrak{p}) = Z \cup h_1 h_2 Z$. Thus we have shown the claim (1).

By virtue of $\sigma(G(\mathfrak{p})) = G(\sigma(\mathfrak{p}))$ for $\sigma \in \Gamma$, Γ acts on the set $\{G(\mathfrak{p}) \mid \mathfrak{p}$ is a prime ideal lying above $2\}$, which consists of the three elements in (1). Denote by Γ_0 the set of elements of Γ which induce the trivial permutation; then Γ/Γ_0 is isomorphic to a subgroup of $\mathfrak{S}_3$. Since there is no Galois extension of $\mathbf{Q}$ whose Galois group is isomorphic to $\mathbf{Z}/3\mathbf{Z}$ or $\mathfrak{S}_3$ if 2 is the only ramified prime number, as in the proof of Lemma 3.6, we have $[\Gamma : \Gamma_0] \leq 2$. Therefore Γ/Γ_0 has a fixed point as an action on the three elements in (1), and let it be $\{Z \cup h_1 Z\}$, say. Thus we have $\sigma(h_1) \in h_1 Z$

for every $\sigma \in \Gamma$. Therefore $G(\mathfrak{p}_1) = \{Z \cup h_1 Z\}$ is a Γ-stable abelian finite subgroup of $GL_2(O_K)$ and hence we may assume that h_1 is diagonal and then $[h_1, h_2] = -1_2$ and Lemma 3.1 imply $h_2 = \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$. This contradicts $h_2 \in G(\mathfrak{p}_2)$. Thus we have incuced the contradiction, assuming that $G(\mathfrak{p}_1)$ and $G(\mathfrak{p}_2)$ are not commutative. □

Thus we have completed the proof of Lemma 1.6 in the case of $p = 2$.

References

[1] Y. Kitaoka, *Finite arithmetic subgroups of GL_n*, II, Nagoya Math. J., **77** (1980), 137–143.

[2] ———, Arithmetic of quadratic forms, Cambridge University Press, 1993.

[3] ———, *Finite arithmetic subgroups of GL_n*, III, Proc. Indian Acad. Sci., **104** (1994), 201–206.

[4] Y. Kitaoka and H. Suzuki, *Finite arithmetic subgroups of GL_n*, IV, Nagoya Math. J., **142** (1996), 183–188.

Graduate School of Polymathematics
Nagoya University
Furo-cho, Chikusa-ku, Nagoya 464-01
Japan
kitaoka@math.nagoya-u.ac.jp