J. Math. Soc. Japan
Vol. 31, No. 1, 1979

Finite groups with trivial class groups

By Shizuo ENDO and Yumiko HIRONAKA

(Received July 14, 1977)

Let A be a finite dimensional semisimple $\boldsymbol{Q}$-algebra and let Λ be a $\boldsymbol{Z}$-order in A. We mean by the class group of Λ the class group defined by using locally free left Λ-modules and denote it by $C(\Lambda)$. Let Ω be a maximal $\boldsymbol{Z}$-order in A containing Λ. We define $D(\Lambda)$ to be the kernel of the natural surjection $C(\Lambda) \to C(\Omega)$ and $d(\Lambda)$ to be the order of $D(\Lambda)$.

Let G be a finite group and let $\boldsymbol{Z}G$ be the integral group ring of G. Then $\boldsymbol{Z}G$ can be regarded as a $\boldsymbol{Z}$-order in the semisimple $\boldsymbol{Q}$-algebra $\boldsymbol{Q}G$.

In this paper we will try to determine all finite groups G for which $d(\boldsymbol{Z}G)=1$.

Let C_n $(n \geqq 1)$ denote the cyclic group of order n and let D_n $(n \geqq 2)$ denote the dihedral group of order $2n$. Let S_n, A_n denote the symmetric, alternating group on n symbols, respectively.

P. Cassou-Noguès [1] showed that, for a finite abelian group G, $d(\boldsymbol{Z}G)=1$ if and only if $G \cong C_1, C_p$ (p any prime), C_4, C_6, C_8, C_9, C_{10}, C_{14} or $C_2 \times C_2$. Hence we have only to treat the nonabelian case.

Our main result is the following:

THEOREM. *A finite nonabelian group G for which $d(\boldsymbol{Z}G)=1$ is isomorphic to one of the groups: D_n $(n \geqq 3)$, A_4, S_4, A_5.*

It is well known (e.g. [14]) that $d(\boldsymbol{Z}A_4)=d(\boldsymbol{Z}S_4)=d(\boldsymbol{Z}A_5)=1$. It is also known that $d(\boldsymbol{Z}D_n)=1$ in each of the following cases: (i) n is an odd prime ([9]); (ii) n is a power of an odd regular prime ([7]); or (iii) n is a power of 2 ([4]). Recently Cassou-Noguès [2] showed that there is an infinite number of pairs (p, q) of distinct odd primes p, q such that $d(\boldsymbol{Z}D_{pq})>1$. It seems difficult to determine all integers n for which $d(\boldsymbol{Z}D_n)=1$.

§1. The group $T(\boldsymbol{Z}G)$.

Let G be a finite group and let (Σ) be the ideal of $\boldsymbol{Z}G$ generated by $\Sigma=\sum_{\sigma \in G} \sigma$. We define the subgroup $T(\boldsymbol{Z}G)$ of $D(\boldsymbol{Z}G)$ to be the kernel of the natural surjection $D(\boldsymbol{Z}G) \to D(\boldsymbol{Z}G/(\Sigma))$ and $t(\boldsymbol{Z}G)$ to be the order of $T(\boldsymbol{Z}G)$

([13], [14]). We denote by $A(G)$ the Artin exponent of G ([8]) and by $G^{(p)}$ a Sylow p-subgroup of G for a prime divisor p of $|G|$.

Recently S. Ullom [14] showed some basic and important results on $T(\boldsymbol{Z}G)$. The following theorem which is a summary of Ullom's results will play an essential role in the proof of our main result.

THEOREM 1.1 ([14]). (1) *For any subquotient H of G $t(\boldsymbol{Z}H)$ divides $t(\boldsymbol{Z}G)$.*

(2) *The exponent of $T(\boldsymbol{Z}G)$ divides $A(G)$.*

(3) *$t(\boldsymbol{Z}C_n)=1$ for any $n\geqq 1$ ([13]).*

(4) *If G is a noncyclic p-group where p is an odd prime, then p divides $t(\boldsymbol{Z}G)$. If G is a noncyclic 2-group which is not dihedral, then 2 divides $t(\boldsymbol{Z}G)$.*

(5) *If G is the metacyclic group defined by*

$$G=\langle\sigma, \tau \mid \sigma^p=\tau^q=1, \tau^{-1}\sigma\tau=\sigma^r\rangle$$

where p is an odd prime, q is a divisor of $p-1$ and r is a primitive q-th root of unity modulo p, then $t(\boldsymbol{Z}G)=q/(q, 2)$.

From this we deduce

PROPOSITION 1.2. *Let G be a finite group for which $t(\boldsymbol{Z}G)=1$. Then the maximal normal subgroup $O(G)$ of G of odd order is cyclic and $G/O(G)\cong C_{2t}$ $(t\geqq 0)$, D_{2t} $(t\geqq 1)$, A_4, S_4 or A_5.*

PROOF. By (1.1) any subgroup of G of odd order is cyclic. Therefore $O(G)$ is cyclic and, for any odd prime $p\,||G|$, $G^{(p)}$ is also cyclic. Further, by (1.1) $G^{(2)}$ is cyclic or dihedral. Hence $G/O(G)$ is isomorphic to one of the groups: (i) C_{2t} $(t\geqq 0)$, (ii) D_{2t} $(t\geqq 1)$, (iii) the subgroups of $P\Gamma L(2, p^s)$ containing $PSL(2, p^s)$ where p is an odd prime and $s\geqq 1$, or (iv) A_7 ([12], [5]).

Since A_7 contains a subgroup which is a semidirect product of C_7 and C_3 such that C_3 acts faithfully on C_7, by (1.1) we have $t(\boldsymbol{Z}A_7)>1$, and so the case (iv) is excluded. Hence we have only to consider the case (iii). It is clear that $PSL(2, p^s)^{(p)}$ is an elementary abelian p-group of order p^s. Therefore from (1.1) it follows that $s=1$.

The group $PSL(2, p)$ contains a subgroup which is a semidirect product of C_p and $C_{p-1/2}$ such that $C_{p-1/2}$ acts faithfully on C_p. If $p\geqq 7$, then by (1.1) we have $t(\boldsymbol{Z}PSL(2, p))>1$. Since $P\Gamma L(2, p)=PGL(2, p)$, $G/O(G)$ must be isomorphic to one of the groups: $A_4(\cong PSL(2, 3))$, $S_4(\cong PGL(2, 3))$, $A_5(\cong PSL(2, 5))$, or $S_5(\cong PGL(2, 5))$. But S_5 contains a subgroup which is a semidirect product of C_5 and C_4 such that C_4 acts faithfully on C_5, and so again by (1.1) we have $t(\boldsymbol{Z}S_5)>1$. Thus we conclude that $G/O(G)\cong A_4$, S_4 or A_5.

§2. The group $T(\boldsymbol{Z}(C_2\times C_2\times C_p))$.

In this section we give the following:

PROPOSITION 2.1. *Let p be an odd prime. Then $t(\boldsymbol{Z}(C_2\times C_2\times C_p))=2$.*

We begin with

LEMMA 2.2. *Let p be an odd prime. Then $t(\boldsymbol{Z}(C_2\times C_2\times C_p))=1$ or 2.*

PROOF. Since $A(C_2\times C_2\times C_p)=2$ ([8]), this follows directly from (1.1).

Let $U(S)$ denote the unit group of a ring S. Let ζ_n be a primitive n-th root of unity and let $\Phi_n(X)$ be the n-th cyclotomic polynomial.

LEMMA 2.3. *The natural surjection $D(\boldsymbol{Z}(C_2\times C_p))\to D(\boldsymbol{Z}C_2[\zeta_p])$ is a bijection.*

PROOF. For example, see [11].

We refer to [10] and [11] for the Mayer-Vietoris sequence which will be used in §§2 and 3.

LEMMA 2.4. *The natural surjection $D(\boldsymbol{Z}(C_2\times C_2\times C_p)/(\Sigma))\to D(\boldsymbol{Z}(C_2\times C_2)[\zeta_p])$ is a bijection.*

PROOF. Write $C_2\times C_2\times C_p=\langle\tau_1, \tau_2, \sigma \mid {\tau_1}^2={\tau_2}^2=\sigma^p=1, \tau_1\tau_2=\tau_2\tau_1, \tau_1\sigma=\sigma\tau_1, \tau_2\sigma=\sigma\tau_2\rangle$. Then we have $\Sigma=(1+\tau_1)(1+\tau_2)\Phi_p(\sigma)$ and hence there is a pullback diagram

$$\begin{array}{ccc} \boldsymbol{Z}(C_2\times C_2\times C_p)/(\Sigma) & \longrightarrow & \boldsymbol{Z}(C_2\times C_p) \\ \downarrow & & \downarrow \\ \boldsymbol{Z}(C_2\times C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma)) & \longrightarrow & \boldsymbol{Z}(C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma)). \end{array}$$

From this we get an exact (Mayer-Vietoris) sequence

$$\begin{aligned} & U(\boldsymbol{Z}(C_2\times C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma)))\oplus U(\boldsymbol{Z}(C_2\times C_p)) \\ & \xrightarrow{\mu} U(\boldsymbol{Z}(C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma)))\longrightarrow D(\boldsymbol{Z}(C_2\times C_2\times C_p)/(\Sigma)) \\ & \longrightarrow D(\boldsymbol{Z}(C_2\times C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma)))\oplus D(\boldsymbol{Z}(C_2\times C_p)) \\ & \longrightarrow D(\boldsymbol{Z}(C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma))). \end{aligned}$$

It is clear that μ is surjective. Since $t(\boldsymbol{Z}(C_2\times C_p))=1$, we have $D(\boldsymbol{Z}(C_2\times C_p))\cong D(\boldsymbol{Z}(C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma)))$. Consequently it follows that

$$D(\boldsymbol{Z}(C_2\times C_2\times C_p)/(\Sigma))\cong D(\boldsymbol{Z}(C_2\times C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma))).$$

Further, from the pullback diagram

$$\begin{array}{ccc} \boldsymbol{Z}(C_2\times C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma)) & \longrightarrow & \boldsymbol{Z}(C_2\times C_p) \\ \downarrow & & \downarrow \\ \boldsymbol{Z}(C_2\times C_2)[\zeta_p] & \longrightarrow & \boldsymbol{Z}C_2[\zeta_p] \end{array}$$

we get an exact sequence

$$\begin{aligned} U(\boldsymbol{Z}(C_2\times C_2)[\zeta_p])\oplus U(\boldsymbol{Z}(C_2\times C_p)) &\xrightarrow{\mu'} U(\boldsymbol{Z}C_2[\zeta_p]) \\ &\longrightarrow D(\boldsymbol{Z}(C_2\times C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma))) \\ &\longrightarrow D(\boldsymbol{Z}(C_2\times C_2)[\zeta_p])\oplus D(\boldsymbol{Z}(C_2\times C_p)) \\ &\longrightarrow D(\boldsymbol{Z}C_2[\zeta_p]). \end{aligned}$$

Clearly μ' is surjective and by (2.3) $D(\boldsymbol{Z}(C_2\times C_p))\cong D(\boldsymbol{Z}C_2[\zeta_p])$. Therefore we have

$$D(\boldsymbol{Z}(C_2\times C_2\times C_p)/((1+\tau_2)\Phi_p(\sigma)))\cong D(\boldsymbol{Z}(C_2\times C_2)[\zeta_p]).$$

Thus we conclude that

$$D(\boldsymbol{Z}(C_2\times C_2\times C_p)/(\Sigma))\cong D(\boldsymbol{Z}(C_2\times C_2)[\zeta_p]).$$

We denote by $U^*(\boldsymbol{Z}(C_2\times C_p))$ (resp. $U^*(\boldsymbol{Z}C_2[\zeta_p])$) the image of $U(\boldsymbol{Z}(C_2\times C_p))$ (resp. $U(\boldsymbol{Z}C_2[\zeta_p])$) under the natural map $U(\boldsymbol{Z}(C_2\times C_p))\to U(\boldsymbol{F}_2(C_2\times C_p))$ (resp. $U(\boldsymbol{Z}C_2[\zeta_p])\to U(\boldsymbol{F}_2C_2[\zeta_p])$).

LEMMA 2.5. *If the order of* $U^*(\boldsymbol{Z}(C_2\times C_p))^{(2)}$ *is equal to the order of* $U^*(\boldsymbol{Z}C_2[\zeta_p])^{(2)}$, *then* $t(\boldsymbol{Z}(C_2\times C_2\times C_p))=2$.

PROOF. From the pullback diagrams

$$\begin{array}{ccc} \boldsymbol{Z}(C_2\times C_2\times C_p) & \longrightarrow & \boldsymbol{Z}(C_2\times C_p) \\ \downarrow & & \downarrow \\ \boldsymbol{Z}(C_2\times C_p) & \longrightarrow & \boldsymbol{F}_2(C_2\times C_p), \end{array} \qquad \begin{array}{ccc} \boldsymbol{Z}(C_2\times C_2)[\zeta_p] & \longrightarrow & \boldsymbol{Z}C_2[\zeta_p] \\ \downarrow & & \downarrow \\ \boldsymbol{Z}C_2[\zeta_p] & \longrightarrow & \boldsymbol{F}_2C_2[\zeta_p] \end{array}$$

we get a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 \longrightarrow & U(\boldsymbol{F}_2(C_2\times C_p))/U^*(\boldsymbol{Z}(C_2\times C_p)) & \longrightarrow & D(\boldsymbol{Z}(C_2\times C_2\times C_p)) & & & \\ & \downarrow & & \downarrow \lambda' & & & \\ 0 \longrightarrow & U(\boldsymbol{F}_2C_2[\zeta_p])/U^*(\boldsymbol{Z}C_2[\zeta_p]) & \longrightarrow & D(\boldsymbol{Z}(C_2\times C_2)[\zeta_p]) & & & \\ & & & \longrightarrow D(\boldsymbol{Z}(C_2\times C_p))\oplus D(\boldsymbol{Z}(C_2\times C_p)) & \longrightarrow & 0 & \\ & & & \downarrow \lambda & & & \\ & & & \longrightarrow D(\boldsymbol{Z}C_2[\zeta_p])\oplus D(\boldsymbol{Z}C_2[\zeta_p]) & \longrightarrow & 0. & \end{array}$$

By (2.3) λ is bijective and by (2.4) the kernel of λ' coincides with $T(\boldsymbol{Z}(C_2\times C_2\times C_p))$. Hence we have

$$\begin{aligned} &t(\boldsymbol{Z}(C_2\times C_2\times C_p)) \\ &\quad=|U(\boldsymbol{F}_2(C_2\times C_p))|\,|U^*(\boldsymbol{Z}C_2[\zeta_p])|/|U(\boldsymbol{F}_2C_2[\zeta_p])|\,|U^*(\boldsymbol{Z}(C_2\times C_p))|. \end{aligned}$$

It is easy to see that $|U(\boldsymbol{F}_2(C_2\times C_p))|=2|U(\boldsymbol{F}_2C_2[\zeta_p])|$. Therefore, if $|U^*(\boldsymbol{Z}(C_2\times C_p))^{(2)}|=|U^*(\boldsymbol{Z}C_2[\zeta_p])^{(2)}|$, then 2 divides $t(\boldsymbol{Z}(C_2\times C_2\times C_p))$. Thus we conclude by (2.2) that $t(\boldsymbol{Z}(C_2\times C_2\times C_p))=2$.

We are now ready to prove (2.1).

PROOF OF (2.1). Write $C_2\times C_p=\langle\tau, \sigma\,|\,\tau^2=\sigma^p=1, \tau\sigma=\sigma\tau\rangle$. Then we have a commutative diagram

$$\begin{array}{ccc} U(\boldsymbol{Z}[\tau, \sigma]) & \xrightarrow{\phi_2} & U(\boldsymbol{F}_2[\tau, \sigma])\cong U(\boldsymbol{F}_2[\tau])\oplus U(\boldsymbol{F}_2[\tau, \zeta_p]) \\ \downarrow{\scriptstyle \phi'} & & \downarrow{\scriptstyle \phi} \\ U(\boldsymbol{Z}[\tau, \zeta_p]) & \xrightarrow{\phi_1} & U(\boldsymbol{F}_2[\tau, \zeta_p]). \end{array}$$

By (2.5) it suffices to show that $|(\mathrm{Im}\,\phi_1)^{(2)}|=|(\mathrm{Im}\,\phi_2)^{(2)}|$.

Let a be a primitive root modulo p. The map $\boldsymbol{Z}[\zeta_p]\to\boldsymbol{F}_p$ defined by $f(\zeta_p)\to f(1)$ induces a surjection $U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])\to U(\boldsymbol{F}_p)$. Therefore there exist elements $u_i(\zeta_p)$, $1\leqq i\leqq t$ of $U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])$ such that

$$U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])=\langle u_i(\zeta_p)\,|\,1\leqq i\leqq t\rangle,$$

$$u_i(1)\equiv a \pmod p, \quad 1\leqq i\leqq t.$$

Since the exponent of $U(\boldsymbol{F}_2[\zeta_p])$ divides $2^{p-1}-1$, we can write

$$u_i(\zeta_p)^{2^{p-1}-1}=1+2v_i(\zeta_p), \quad v_i(\zeta_p)\in\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}].$$

From the fact that $u_i(1)\equiv a \pmod p$ it follows that

$$\prod_{j=1}^{p-1/2} u_i(\zeta_p{}^j)=N_{\boldsymbol{Q}(\zeta_p+\zeta_p^{-1})/\boldsymbol{Q}}(u_i(\zeta_p))=-1.$$

Through the inclusion $U(\boldsymbol{Z}[\tau, \zeta_p])\to U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z}[\zeta_p])$ we may identify $1-v_i(\zeta_p)(\tau-1)$ with $(1, u_i(\zeta_p)^{2^{p-1}-1})$. Then it is easy to see that

$$(1) \qquad \prod_{j=1}^{p-1/2}(1-v_i(\zeta_p{}^j)(\tau-1))=\tau.$$

Note that $U(\boldsymbol{Z}[\zeta_p])=\langle\zeta_p\rangle\cdot U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])$ and $2^{p-1}-1$ is odd. Then we have

$$(2) \qquad (\mathrm{Im}\,\phi_1)^{(2)}=\langle 1+\bar{v}_i(\zeta_p)(\tau+1)\,|\,1\leqq i\leqq t\rangle.$$

Let $f(\tau, \sigma)$ be an element of $\boldsymbol{Z}[\tau, \sigma]$ such that $f(\tau, \zeta_p)\in\langle 1-v_i(\zeta_p)(\tau-1)\,|\,1\leqq i\leqq t\rangle$. Then we can write

$$f(\tau, \sigma)=\prod_{i=1}^{t}(1-v_i(\sigma)(\tau-1))^{h_i}+(c+d\tau)\Phi_p(\sigma)$$

where h_i, c, d are integers. It is clear that $f(\tau, \sigma)\in U(\boldsymbol{Z}[\tau, \sigma])$ if and only if $f(\tau, 1)\in U(\boldsymbol{Z}[\tau])$, i.e., if and only if $f(1, 1)$, $f(-1, 1)\in U(\boldsymbol{Z})$. However $f(1, 1)=1+p(c+d)$ and $f(-1, 1)=\prod_i(1+2v_i(1))^{h_i}+p(c-d)\equiv a^h \pmod p$ where

$h=(2^{p-1}-1)\sum_i h_i$. Therefore, if $f(\tau, \sigma)\in U(\boldsymbol{Z}[\tau, \sigma])$, then $d=-c$ and $p-1/2|h$. Conversely, if $d=-c$ and $p-1/2|h$, then $f(1, 1)=1$, and, for some c,

$$f(-1, 1)=\begin{cases} 1 & \text{when } 2h/p-1 \text{ is even} \\ -1 & \text{when } 2h/p-1 \text{ is odd.} \end{cases}$$

In this case we have

$$f(\tau, \sigma)=\prod_i(1-v_i(\sigma)(\tau-1))^{h_i}-c(\tau-1)\Phi_p(\sigma)\in U(\boldsymbol{Z}[\tau, \sigma])$$

and

$$\phi_2(f(\tau, \sigma))=\begin{cases} (\prod_i(1+\bar{v}_i(\zeta_p)(\tau+1))^{h_i},\ 1) & \text{when } 2h/p-1 \text{ is even} \\ (\prod_i(1+\bar{v}_i(\zeta_p)(\tau+1))^{h_i},\ \tau) & \text{when } 2h/p-1 \text{ is odd.} \end{cases}$$

If we put $V=\{f(\tau, \sigma)\in U(\boldsymbol{Z}[\tau, \sigma])|f(\tau, \zeta_p)\in\langle 1-v_i(\zeta_p)(\tau-1)\,|\,1\leqq i\leqq t\rangle\}$, then we see that $(\mathrm{Im}\,\phi_2)^{(2)}=\phi_2(V)$. From this it follows that

$$(3)\qquad (\mathrm{Im}\,\phi_2)^{(2)}=\begin{cases} \langle(1+\bar{v}_i(\zeta_p)(\tau+1), \tau)\,|\,1\leqq i\leqq t\rangle & \text{when } p\equiv 3 \pmod 4 \\ \langle(1, \tau), ((1+\bar{v}_i(\zeta_p)(\tau+1))(1+\bar{v}_{i'}(\zeta_p)(\tau+1)), 1)\,|\,1\leqq i<i'\leqq t\rangle & \\ \qquad\qquad \text{when } p\equiv 1 \pmod 4. & \end{cases}$$

Let $\bar{\psi}: (\mathrm{Im}\,\phi_2)^{(2)}\to(\mathrm{Im}\,\phi_1)^{(2)}$ denote the restriction map of ψ.

In the case where $p\equiv 3 \pmod 4$ it follows from (2) and (3) that $\bar{\psi}$ is surjective. Suppose that $(1, \tau)\in(\mathrm{Im}\,\phi_2)^{(2)}$. Then by (3) we have

$$\prod_{k=1}^{r}(1+\bar{v}_{i_k}(\zeta_p)(\tau+1))=1$$

for an odd integer $r\geqq 1$ and integers $1\leqq i_k\leqq t$. Therefore

$$\prod_{j=1}^{p-1/2}\left[\prod_{k=1}^{r}(1+\bar{v}_{i_k}(\zeta_p{}^j)(\tau+1))\right]=1,$$

but by (1)

$$\prod_{k=1}^{r}\left[\prod_{j=1}^{p-1/2}(1+\bar{v}_{i_k}(\zeta_p{}^j)(\tau+1))\right]=\tau^r=\tau,$$

which is a contradiction. Hence $\mathrm{Ker}\,\psi=\langle(1, \tau)\rangle\subsetneqq(\mathrm{Im}\,\phi_2)^{(2)}$, and so $\bar{\psi}$ is injective. Thus $\bar{\psi}$ is bijective, i. e., $|(\mathrm{Im}\,\phi_1)^{(2)}|=|(\mathrm{Im}\,\phi_2)^{(2)}|$.

In the case where $p\equiv 1 \pmod 4$ $\bar{\psi}$ is not injective because $(1, \tau)\in \operatorname{Ker}\bar{\psi}$. Suppose that $\bar{\psi}$ is surjective. Then by (2) and (3)

$$\prod_{k=1}^{r}(1+\bar{v}_{i_k}(\zeta_p)(\tau+1))=1$$

for an odd integer $r\geqq 1$ and integers $1\leqq i_k\leqq t$. In the same way as above this leads to a contradiction. Hence $\bar{\psi}$ is not surjective, which implies that $|(\operatorname{Im}\phi_1)^{(2)}|=|(\operatorname{Im}\phi_2)^{(2)}|$. This completes the proof of (2.1).

§ 3. The groups $D(\boldsymbol{Z}(C_p\times D_q))$ and $D(\boldsymbol{Z}(D_p\times D_q))$.

Let A be a finite dimensional algebra over a field K. We denote by $N_{A/K}$ the norm map $A\to K$. Especially, if A is a separable K-algebra with center L, then we denote by $Nrd_{A/L}$ the reduced norm map $A\to L$.

Now let p be an odd prime. We define a map

$$\mu : U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z}) \longrightarrow U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q[\zeta_p])\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p)$$

by

$$(x, y(\zeta_p), z(\zeta_p), w)\longmapsto(\bar{x}\cdot\bar{z}(1), \bar{y}(\zeta_p)\cdot\bar{z}(\zeta_p), \bar{x}\cdot\bar{w}, \bar{y}(1)\cdot\bar{w}).$$

LEMMA 3.1. *Let a be a primitive root modulo p. Then $(1, 1, 1, \bar{a}^k)\notin\operatorname{Im}\mu$ for each odd integer k.*

PROOF. Let $\nu : U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])\oplus U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])\oplus U(\boldsymbol{Z})\to U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q[\zeta_p+\zeta_p^{-1}])\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p)$ be the restriction map of μ. Since $\mu((1, \zeta_p, 1, 1))=\mu((1, 1, \zeta_p, 1))=(1, \zeta_p, 1, 1)$ and $U(\boldsymbol{Z}[\zeta_p])=\langle\zeta_p\rangle\cdot U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])$, it suffices to show that $(1, 1, 1, \bar{a}^k)\notin\operatorname{Im}\nu$.

Define a map $N' : U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])\oplus U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])\oplus U(\boldsymbol{Z})\to U(\boldsymbol{Z})\oplus U(\boldsymbol{Z})\oplus U(\boldsymbol{Z})\oplus U(\boldsymbol{Z})$ by $(x, y(\zeta_p), z(\zeta_p), w)\mapsto(x^{p-1/2}, N_{\boldsymbol{Q}[\zeta_p+\zeta_p^{-1}]/\boldsymbol{Q}}(y(\zeta_p)), N_{\boldsymbol{Q}[\zeta_p+\zeta_p^{-1}]/\boldsymbol{Q}}(z(\zeta_p)), w^{p-1/2})$. Then we have a commutative diagram

$$\begin{array}{ccc}
U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])\oplus U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])\oplus U(\boldsymbol{Z}) & & \\
\downarrow N' & & \\
U(\boldsymbol{Z})\oplus U(\boldsymbol{Z})\oplus U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}) & & \\
\xrightarrow{\nu} U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q[\zeta_p+\zeta_p^{-1}])\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p) & & \\
\downarrow N & & \\
\xrightarrow{\nu'} U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p) & &
\end{array}$$

where ν' denotes the restriction map of ν. If $\alpha(\zeta_p)=\zeta_p^a-\zeta_p^{-a}/\zeta_p-\zeta_p^{-1}$, then $\nu((1, \alpha(\zeta_p), 1, 1))=(1, \bar{\alpha}(\zeta_p), 1, \bar{a})$ because $\bar{\alpha}(1)=\bar{a}$. Suppose that $(1, 1, 1, \bar{a}^k)\in\operatorname{Im}\nu$. Then $(1, \bar{\alpha}(\zeta_p)^k, 1, 1)\in\operatorname{Im}\nu$ and hence $N((1, \bar{\alpha}(\zeta_p)^k, 1, 1))\in\operatorname{Im}\nu'$. Since

k is odd, $N_{\boldsymbol{F}_q[\zeta_p+\zeta_p^{-1}]/\boldsymbol{F}_q}(\bar{\alpha}(\zeta_p)^k)=-1$ and so $N((1, \bar{\alpha}(\zeta_p)^k, 1, 1))=(1, -1, 1, 1)\in \mathrm{Im}\,\nu'$. However it is clear that $\mathrm{Im}\,\nu'=\langle(-1, -1, 1, 1), (1, 1, -1, -1), (-1, 1, -1, 1), (1, -1, 1, -1)\rangle$, which implies $(1, -1, 1, 1)\notin \mathrm{Im}\,\nu'$, a contradiction. This concludes that $(1, 1, 1, \bar{a}^k)\notin \mathrm{Im}\,\nu$.

PROPOSITION 3.2. *Let p, q be distinct odd primes. Then 2 divides $d(\boldsymbol{Z}(C_p\times D_q))$.*

PROOF. Write

$$C_p\times D_q=\langle\sigma, \tau \mid \sigma^{pq}=\tau^2=1, \tau\sigma^q=\sigma^q\tau, \tau\sigma^p=\sigma^{-p}\tau\rangle.$$

Then we have a pullback diagram

$$\begin{array}{ccc} \boldsymbol{Z}(C_p\times D_q) & \longrightarrow & \boldsymbol{Z}[\zeta_p, \tau]\oplus\boldsymbol{Z}[\zeta_q, \tau] \\ \downarrow & & \downarrow \\ \boldsymbol{Z}[\tau]\oplus\boldsymbol{Z}[\zeta_p, \zeta_q, \tau] & \longrightarrow & \boldsymbol{F}_p[\tau]\oplus\boldsymbol{F}_q[\zeta_p, \tau]\oplus\boldsymbol{F}_q[\tau]\oplus\boldsymbol{F}_p[\zeta_q, \tau]. \end{array}$$

From this we get an exact sequence

$$\begin{aligned} & U(\boldsymbol{Z}[\tau])\oplus U(\boldsymbol{Z}[\zeta_p, \zeta_q, \tau])\oplus U(\boldsymbol{Z}[\zeta_p, \tau])\oplus U(\boldsymbol{Z}[\zeta_q, \tau]) \\ & \xrightarrow{\mu} U(\boldsymbol{F}_p[\tau])\oplus U(\boldsymbol{F}_q[\zeta_p, \tau])\oplus U(\boldsymbol{F}_q[\tau])\oplus U(\boldsymbol{F}_p[\zeta_q, \tau]) \\ & \longrightarrow D(\boldsymbol{Z}(C_p\times D_q))\longrightarrow D(\boldsymbol{Z}[\tau])\oplus D(\boldsymbol{Z}[\zeta_p, \zeta_q, \tau]) \\ & \oplus D(\boldsymbol{Z}[\zeta_p, \tau])\oplus D(\boldsymbol{Z}[\zeta_q, \tau])\longrightarrow 0. \end{aligned}$$

Note that $\tau\zeta_p=\zeta_p\tau$ and $\tau\zeta_q=\zeta_q^{-1}\tau$. Since both $\boldsymbol{Z}[\zeta_p, \zeta_q, \tau]$ and $\boldsymbol{Z}[\zeta_q, \tau]$ are hereditary, we see that $D(\boldsymbol{Z}[\zeta_p, \zeta_q, \tau])=D(\boldsymbol{Z}[\zeta_q, \tau])=0$. Clearly $D(\boldsymbol{Z}[\tau])=0$, and by (2.2) $D(\boldsymbol{Z}[\zeta_p, \tau])\cong D(\boldsymbol{Z}C_{2p})$. Hence we have an exact sequence

$$0\longrightarrow \mathrm{Coker}\,\mu\longrightarrow D(\boldsymbol{Z}(C_p\times D_q))\longrightarrow D(\boldsymbol{Z}C_{2p})\longrightarrow 0.$$

If K denotes one of the rings $\boldsymbol{Q}[\zeta_p, \zeta_q]$, $\boldsymbol{Q}[\zeta_q]$ and $\boldsymbol{F}_p[\zeta_q]$, then $K[\tau]$ is a separable algebra with center $K^{\langle\tau\rangle}=\{z\in K \mid \tau(z)=z\}$, and we see that $Nrd_{K[\tau]/K^{\langle\tau\rangle}}(x+y\tau)=x\tau(x)-y\tau(y)$ for any $x, y\in K$. Define a map N_1': $U(\boldsymbol{Z}[\tau])\oplus U(\boldsymbol{Z}[\zeta_p, \zeta_q, \tau])\oplus U(\boldsymbol{Z}[\zeta_p, \tau])\oplus U(\boldsymbol{Z}[\zeta_q, \tau])\to U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p, \zeta_q+\zeta_q^{-1}])\oplus U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z}[\zeta_q+\zeta_q^{-1}])$ by $(x_1+x_2\tau, y_1+y_2\tau, z_1+z_2\tau, w_1+w_2\tau)\mapsto(x_1^2-x_2^2, y_1\tau(y_1)-y_2\tau(y_2), z_1^2-z_2^2, w_1\tau(w_1)-w_2\tau(w_2))$ and a map $N_1: U(\boldsymbol{F}_p[\tau])\oplus U(\boldsymbol{F}_q[\zeta_p, \tau])\oplus U(\boldsymbol{F}_q[\tau])\oplus U(\boldsymbol{F}_p[\zeta_q, \tau])\to U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q[\zeta_p])\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p[\zeta_q+\zeta_q^{-1}])$ by $(\bar{x}_1+\bar{x}_2\tau, \bar{y}_1+\bar{y}_2\tau, \bar{z}_1+\bar{z}_2\tau, \bar{w}_1+\bar{w}_2\tau)\mapsto(\bar{x}_1^2-\bar{x}_2^2, \bar{y}_1^2-\bar{y}_2^2, \bar{z}_1^2-\bar{z}_2^2, \bar{w}_1\tau(\bar{w}_1)-\bar{w}_2\tau(\bar{w}_2))$. Then we have a commutative diagram

$$\begin{array}{l} U(\boldsymbol{Z}[\tau])\oplus U(\boldsymbol{Z}[\zeta_p,\zeta_q,\tau])\oplus U(\boldsymbol{Z}[\zeta_p,\tau])\oplus U(\boldsymbol{Z}[\zeta_q,\tau]) \\ \qquad\qquad\qquad\qquad\qquad\qquad \downarrow N_1' \\ U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p,\zeta_q+\zeta_q^{-1}])\oplus U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z}[\zeta_q+\zeta_q^{-1}]) \\ \qquad\xrightarrow{\mu} U(\boldsymbol{F}_p[\tau])\oplus U(\boldsymbol{F}_q[\zeta_p,\tau])\oplus U(\boldsymbol{F}_q[\tau])\oplus U(\boldsymbol{F}_p[\zeta_q,\tau]) \\ \qquad\qquad\qquad\qquad\qquad\qquad \downarrow N_1 \\ \qquad\xrightarrow{\mu_1} \quad U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q[\zeta_p])\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p[\zeta_q+\zeta_q^{-1}]) \end{array}$$

where μ_1 denotes the restriction map of μ. Here the map N_1 is surjective and hence $|\mathrm{Coker}\,\mu_1|$ divides $d(\boldsymbol{Z}(C_p\times D_q))$. Further define a map $N_2' : U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p,\zeta_q+\zeta_q^{-1}])\oplus U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z}[\zeta_q+\zeta_q^{-1}])\to U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z})$ by $(x,y,z,w)\mapsto(x^{q-1/2}, N_{\boldsymbol{Q}[\zeta_p\cdot\zeta_q+\zeta_q^{-1}]/\boldsymbol{Q}[\zeta_p]}(y), z^{q-1/2}, N_{\boldsymbol{Q}[\zeta_q+\zeta_q^{-1}]/\boldsymbol{Q}}(w))$ and a map $N_2 : U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q[\zeta_p])\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p[\zeta_q+\zeta_q^{-1}])\to U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q[\zeta_p])\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p)$ by $(\bar{x},\bar{y},\bar{z},\bar{w})\mapsto(\bar{x}^{q-1/2},\bar{y}^{q-1/2},\bar{z}^{q-1/2}, N_{\boldsymbol{F}_p[\zeta_q+\zeta_q^{-1}]/\boldsymbol{F}_p}(\bar{w}))$. Then we get a commutative diagram

$$\begin{array}{l} U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p,\zeta_q+\zeta_q^{-1}])\oplus U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z}[\zeta_q+\zeta_q^{-1}]) \\ \qquad\qquad\qquad\qquad\qquad\qquad \downarrow N_2' \\ \qquad U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z}[\zeta_p])\oplus U(\boldsymbol{Z}) \\ \qquad\qquad\xrightarrow{\mu_1} U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q[\zeta_p])\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p[\zeta_q+\zeta_q^{-1}]) \\ \qquad\qquad\qquad\qquad\qquad\qquad \downarrow N_2 \\ \qquad\qquad\xrightarrow{\mu_2} U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q[\zeta_p])\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p) \end{array}$$

where μ_2 denotes the restriction map of μ_1. Let a be a primitive root modulo p and let k be an odd integer. By virtue of (3.1) we have $(1,1,1,\bar{a}^k)\notin\mathrm{Im}\,\mu_2$. Since $N_{\boldsymbol{F}_p[\zeta_q+\zeta_q^{-1}]/\boldsymbol{F}_p} : U(\boldsymbol{F}_p[\zeta_q+\zeta_q^{-1}])\to U(\boldsymbol{F}_p)$ is surjective, there is an element $\bar{\gamma}$ of $U(\boldsymbol{F}_p[\zeta_q+\zeta_q^{-1}])$ such that $N_{\boldsymbol{F}_p[\zeta_q+\zeta_q^{-1}]/\boldsymbol{F}_p}(\bar{\gamma})=\bar{a}$. Then we have $(1,1,1,\bar{\gamma}^k)\notin\mathrm{Im}\,\mu_1$, and therefore the Sylow 2-subgroup of the cyclic group $\langle(1,1,1,\bar{\gamma})\rangle$ is not contained in $\mathrm{Im}\,\mu_1$. This shows that 2 divides $|\mathrm{Coker}\,\mu_1|$, which completes the proof of the proposition.

REMARK 3.3. It is known (e.g. [1]) that $d(\boldsymbol{Z}C_{2p})>1$ for any prime $p\geqq 11$. Since $d(\boldsymbol{Z}C_{2p})$ divides $d(\boldsymbol{Z}(C_p\times D_q))$, this implies that $d(\boldsymbol{Z}(C_p\times D_q))>1$ for any $p\geqq 11$. However $d(\boldsymbol{Z}C_{2p})$ is odd. Hence this does not imply that 2 divides $d(\boldsymbol{Z}(C_p\times D_q))$.

PROPOSITION 3.4. *Let p, q be distinct odd primes. Then 2 divides $d(\boldsymbol{Z}(D_p\times D_q))$.*

PROOF. Write

$$D_p\times D_q=\langle\sigma,\tau_1,\tau_2\,|\,\sigma^{pq}=\tau_1^{\,2}=\tau_2^{\,2}=1,\ \tau_1\sigma^q=\sigma^{-q}\tau_1,\ \tau_1\sigma^p=\sigma^p\tau_1,$$
$$\tau_2\sigma^q=\sigma^q\tau_2,\ \tau_2\sigma^p=\sigma^{-p}\tau_2,\ \tau_1\tau_2=\tau_2\tau_1\rangle.$$

Then we have a commutative diagram

$$\begin{array}{l} \qquad\qquad\qquad\qquad\quad \boldsymbol{Z}(D_p\times D_q) \\ \qquad\qquad\qquad\qquad\quad \downarrow \\ \boldsymbol{Z}[\tau_1,\tau_2]\oplus\boldsymbol{Z}[\zeta_p,\zeta_q,\tau_1,\tau_2] \\ \qquad\qquad\longrightarrow\qquad \boldsymbol{Z}[\zeta_p,\tau_1,\tau_2]\oplus\boldsymbol{Z}[\zeta_q,\tau_1,\tau_2] \\ \qquad\qquad\qquad\qquad\quad \downarrow \\ \longrightarrow \boldsymbol{F}_p[\tau_1,\tau_2]\oplus\boldsymbol{F}_q[\zeta_p,\tau_1,\tau_2]\oplus\boldsymbol{F}_q[\tau_1,\tau_2]\oplus\boldsymbol{F}_p[\zeta_q,\tau_1,\tau_2]. \end{array}$$

From this we get an exact sequence

$$\begin{aligned} &U(\boldsymbol{Z}[\tau_1,\tau_2])\oplus U(\boldsymbol{Z}[\zeta_p,\zeta_q,\tau_1,\tau_2])\oplus U(\boldsymbol{Z}[\zeta_p,\tau_1,\tau_2])\oplus U(\boldsymbol{Z}[\zeta_q,\tau_1,\tau_2]) \\ &\xrightarrow{\nu} U(\boldsymbol{F}_p[\tau_1,\tau_2])\oplus U(\boldsymbol{F}_q[\zeta_p,\tau_1,\tau_2])\oplus U(\boldsymbol{F}_q[\tau_1,\tau_2])\oplus U(\boldsymbol{F}_p[\zeta_q,\tau_1,\tau_2]) \\ &\longrightarrow D(\boldsymbol{Z}(D_p\times D_q))\longrightarrow D(\boldsymbol{Z}[\tau_1,\tau_2])\oplus D(\boldsymbol{Z}[\zeta_p,\zeta_q,\tau_1,\tau_2]) \\ &\oplus D(\boldsymbol{Z}[\zeta_p,\tau_1,\tau_2])\oplus D(\boldsymbol{Z}[\zeta_q,\tau_1,\tau_2])\longrightarrow 0. \end{aligned}$$

Note that $\tau_1\zeta_p=\zeta_p^{-1}\tau_1$, $\tau_1\zeta_q=\zeta_q\tau_1$, $\tau_2\zeta_p=\zeta_p\tau_2$ and $\tau_2\zeta_q=\zeta_q^{-1}\tau_2$. Since $\boldsymbol{Z}[\zeta_p,\zeta_q,\tau_1,\tau_2]$ is hereditary, it follows that $D(\boldsymbol{Z}[\zeta_p,\zeta_q,\tau_1,\tau_2])=0$. It is clear that $D(\boldsymbol{Z}[\tau_1,\tau_2])=0$. Further we see that $D(\boldsymbol{Z}[\zeta_p,\tau_1,\tau_2])\cong D(\boldsymbol{Z}D_{2p})$ and $D(\boldsymbol{Z}[\zeta_q,\tau_1,\tau_2])\cong D(\boldsymbol{Z}D_{2q})$. Therefore we have an exact sequence

$$0\longrightarrow \mathrm{Coker}\,\nu\longrightarrow D(\boldsymbol{Z}(D_p\times D_q))\longrightarrow D(\boldsymbol{Z}D_{2p})\oplus D(\boldsymbol{Z}D_{2q})\longrightarrow 0.$$

Denote by S one of the rings $\boldsymbol{Z}[\zeta_p,\zeta_q]$, $\boldsymbol{Z}[\zeta_p]$, $\boldsymbol{Z}[\zeta_q]$, $\boldsymbol{Z}$, $\boldsymbol{F}_q[\zeta_p]$, $\boldsymbol{F}_p[\zeta_q]$, $\boldsymbol{F}_q$, $\boldsymbol{F}_p$ and define a map $N_S: U(S[\tau_1,\tau_2])\to U(S^{<\tau_1,\tau_2>})$ by

$$x+y\tau_1+z\tau_2+w\tau_1\tau_2\longmapsto \begin{vmatrix} x & y & z & w \\ \tau_1(y) & \tau_1(x) & \tau_1(w) & \tau_1(z) \\ \tau_2(z) & \tau_2(w) & \tau_2(x) & \tau_2(y) \\ \tau_1\tau_2(w) & \tau_1\tau_2(z) & \tau_1\tau_2(y) & \tau_1\tau_2(x) \end{vmatrix}.$$

Here it should be noted that $N_{\boldsymbol{Z}[\zeta_p,\zeta_q]}=Nrd_{\boldsymbol{Q}[\zeta_p,\zeta_q,\tau_1,\tau_2]/\boldsymbol{Q}[\zeta_p+\zeta_p^{-1},\zeta_q+\zeta_q^{-1}]}$. Let $N'=(N_{\boldsymbol{Z}}, N_{\boldsymbol{Z}[\zeta_p,\zeta_q]}, N_{\boldsymbol{Z}[\zeta_p]}, N_{\boldsymbol{Z}[\zeta_q]})$ and $N=(N_{\boldsymbol{F}_p}, N_{\boldsymbol{F}_q[\zeta_p]}, N_{\boldsymbol{F}_q}, N_{\boldsymbol{F}_p[\zeta_q]})$. Then we get a commutative diagram

$$\begin{array}{l} U(\boldsymbol{Z}[\tau_1,\tau_2])\oplus U(\boldsymbol{Z}[\zeta_p,\zeta_q,\tau_1,\tau_2])\oplus U(\boldsymbol{Z}[\zeta_p,\tau_1,\tau_2])\oplus U(\boldsymbol{Z}[\zeta_q,\tau_1,\tau_2]) \\ \qquad\qquad\qquad\qquad\qquad\qquad\quad \downarrow N' \\ U(\boldsymbol{Z})\oplus U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1},\zeta_q+\zeta_q^{-1}])\oplus U(\boldsymbol{Z}[\zeta_p+\zeta_p^{-1}])\oplus U(\boldsymbol{Z}[\zeta_q+\zeta_q^{-1}]) \\ \xrightarrow{\nu} U(\boldsymbol{F}_p[\tau_1,\tau_2])\oplus U(\boldsymbol{F}_q[\zeta_p,\tau_1,\tau_2])\oplus U(\boldsymbol{F}_q[\tau_1,\tau_2])\oplus U(\boldsymbol{F}_p[\zeta_q,\tau_1,\tau_2]) \\ \qquad\qquad\qquad\qquad\qquad\qquad\quad \downarrow N \\ \xrightarrow{\nu_1} U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_q[\zeta_p+\zeta_p^{-1}])\oplus U(\boldsymbol{F}_q)\oplus U(\boldsymbol{F}_p[\zeta_q+\zeta_q^{-1}]) \end{array}$$

where ν_1 denotes the restriction map of ν. The map N is surjective and hence $|\mathrm{Coker}\,\nu_1|$ divides $d(\boldsymbol{Z}(D_p\times D_q))$. Then, in the same way as in the proof of (3.2), we can show that 2 divides $|\mathrm{Coker}\,\nu_1|$. Thus we conclude that 2 divides $d(\boldsymbol{Z}(D_p\times D_q))$.

REMARK 3.5. In the proof of (3.4) it was shown that there exists a surjection: $D(\boldsymbol{Z}(D_p\times D_q))\to D(\boldsymbol{Z}D_{2p})\oplus D(\boldsymbol{Z}D_{2q})$. It is seen that, if p is one of the primes: $p\leqq 31$, $p=47$, 53, 59, 179, 19379, then $d(\boldsymbol{Z}D_{2p})=1$. However we do not know whether $d(\boldsymbol{Z}D_{2p})=1$ for any prime p or not.

For any integers $n\geqq 3$ and $t\geqq 2$, define the group $H_{n,t}$ as follows:

$$H_{n,t}=\langle\sigma,\tau\,|\,\sigma^n=\tau^{2^t}=1,\ \sigma\tau=\tau\sigma^{-1}\rangle.$$

PROPOSITION 3.6. *Let p be an odd prime. Then 2 divides $d(\boldsymbol{Z}H_{p,2})$.*

PROOF. By Fröhlich [3] this has already been proved in a more precise form. For completeness we give a simple proof.

Now there is an exact sequence

$$U(\boldsymbol{Z}[\zeta_p,\bar\tau])\oplus U(\boldsymbol{Z}[\bar\tau])\longrightarrow U(\boldsymbol{F}_p[\bar\tau])\longrightarrow D(\boldsymbol{Z}H_{p,2}/(\tau^2+1))$$
$$\longrightarrow D(\boldsymbol{Z}[\zeta_p,\bar\tau])\oplus D(\boldsymbol{Z}[\bar\tau])\longrightarrow 0$$

where $\bar\tau^2=-1$ and $\zeta_p\bar\tau=\bar\tau\zeta_p^{-1}$. It is clear that $D(\boldsymbol{Z}[\zeta_p,\bar\tau])=D(\boldsymbol{Z}[\bar\tau])=0$. Therefore we get an exact sequence

$$U(\boldsymbol{Z}[\zeta_p,\bar\tau])\xrightarrow{\phi}U(\boldsymbol{F}_p[\bar\tau])\longrightarrow D(\boldsymbol{Z}H_{p,2}/(\tau^2+1))\longrightarrow 0.$$

Let a be a primitive root modulo p and let (c,d), $c,d\in\boldsymbol{Z}$ be a solution of the congruence $X^2+Y^2\equiv a \pmod p$. Then $\alpha=\bar c+\bar d\bar\tau\in U(\boldsymbol{F}_p[\bar\tau])$ and $(\bar c+\bar d\bar\tau)(\bar c-\bar d\bar\tau)=\bar a$. Let k be an odd integer and suppose that $\alpha^k\in\mathrm{Im}\,\phi$. Then there exists $f(\zeta_p,\bar\tau)\in U(\boldsymbol{Z}[\zeta_p,\bar\tau])$ such that $\bar f(1,\bar\tau)=\alpha^k$. Write $f(\zeta_p,\bar\tau)=f_1(\zeta_p)+f_2(\zeta_p)\bar\tau$, $f_1(\zeta_p)$, $f_2(\zeta_p)\in\boldsymbol{Z}[\zeta_p]$ and let $g(\zeta_p,\bar\tau)=f_1(\zeta_p^{-1})-f_2(\zeta_p^{-1})\bar\tau$. Then $Nrd_{\boldsymbol{Q}[\zeta_p,\bar\tau]/\boldsymbol{Q}[\zeta_p+\zeta_p^{-1}]}(f(\zeta_p,\bar\tau))=f(\zeta_p,\bar\tau)g(\zeta_p,\bar\tau)=f_1(\zeta_p)f_1(\zeta_p^{-1})+f_2(\zeta_p)f_2(\zeta_p^{-1})>0$. Consequently $N_{\boldsymbol{Q}[\zeta_p+\zeta_p^{-1}]/\boldsymbol{Q}}(f(\zeta_p,\bar\tau)g(\zeta_p,\bar\tau))=1$. However $\bar f(1,\bar\tau)\bar g(1,\bar\tau)=\bar a^k$, and therefore $\overline{(N_{\boldsymbol{Q}[\zeta_p+\zeta_p^{-1}]/\boldsymbol{Q}}(f(\zeta_p,\bar\tau)g(\zeta_p,\bar\tau)))}=(\bar a^k)^{p-1/2}=\overline{-1}$, a contradiction. Hence $\alpha^k\notin\mathrm{Im}\,\phi$. This implies that $\langle\alpha\rangle^{(2)}$ is not contained in $\mathrm{Im}\,\phi$, which concludes that 2 divides $d(\boldsymbol{Z}H_{p,2})$.

§ 4. The main result.

We are now in a position to prove our main result.

THEOREM 4.1. *A finite nonabelian group G for which $d(\boldsymbol{Z}G)=1$ is isomorphic to one of the groups: D_n $(n\geqq 3)$, A_4, S_4, A_5.*

PROOF. By (1.2) $O(G)$ is cyclic and $G/O(G)\cong C_{2t}$, D_{2t}, A_4, S_4 or A_5. Write $O(G)=\langle\rho\rangle$ and let $m=|O(G)|$. Let $C(G)$ denote the center of G.

(i) Assume that $G/O(G)\cong C_{2t}$. Then $G^{(2)}\cong C_{2t}$ and so we may write $G^{(2)}=\langle\tau\rangle$. The action of $\langle\tau\rangle$ on $\langle\rho\rangle$ by conjugation yields a map $\phi:\langle\tau\rangle\to \mathrm{Aut}\langle\rho\rangle$. Since G is nonabelian, we have $\mathrm{Ker}\,\phi\subsetneqq\langle\tau\rangle$. If $[\langle\tau\rangle:\mathrm{Ker}\,\phi]=2^s$, $s\geqq 2$, then there is a prime $p\mid m$ such that $\langle\tau\rangle/\mathrm{Ker}\,\phi$ acts faithfully on $\langle\rho\rangle^{(p)}$. Therefore by (1.1) $d(\boldsymbol{Z}G/(\tau^{2^s}-1, \rho^{m/p}-1))>1$ and so $d(\boldsymbol{Z}G)>1$. Thus we must have $[\langle\tau\rangle:\mathrm{Ker}\,\phi]=2$. In this case, suppose that $O(G)\cap C(G)\neq\{1\}$ and let $O(G)\cap C(G)=\langle\rho^{m'}\rangle$, $m'\mid m$. Then $m''=m/m'>1$ and $(m', m'')=1$. Hence $G=\langle\rho^{m'}\rangle\times\langle\rho^{m''}, \tau\rangle$ and so $G/\langle\tau^2\rangle\cong C_{m'}\times D_{m''}$. According to (3.2) $d(\boldsymbol{Z}G/(\tau^2-1))>1$ and therefore $d(\boldsymbol{Z}G)>1$. Consequently we have $O(G)\cap C(G)=\{1\}$. Then $G=\langle\rho, \tau\mid\rho^m=\tau^{2^t}=1, \rho\tau=\tau\rho^{-1}\rangle$. By virtue of (3.6), $d(\boldsymbol{Z}G)>1$ if $t\geqq 2$. Hence we must have $t=1$, i.e., $G\cong D_m$.

(ii) Assume that $G/O(G)\cong D_{2t}$, $t\geqq 2$. Then $G^{(2)}\cong D_{2t}$ and so we may write $G^{(2)}=\langle\sigma, \tau\mid\sigma^{2^t}=\tau^2=1, \sigma\tau=\tau\sigma^{-1}\rangle$. If $O(G)\cap C(G)\neq\{1\}$, then there exists a subquotient of G which is isomorphic to $C_2\times C_2\times C_p$ for a prime $p\mid m$. From (1.1) and (2.1) it follows that $t(\boldsymbol{Z}G)>1$. Therefore we have $O(G)\cap C(G)=\{1\}$.

Let p_i, $1\leqq i\leqq r$, be all prime divisors of m and let $\langle\rho_i\rangle=\langle\rho\rangle^{(p_i)}$. The action of $G^{(2)}$ on $\langle\rho_i\rangle$ by conjugation yields a map $\phi_i: G^{(2)}\to\mathrm{Aut}\langle\rho_i\rangle$. Let $N_i=\mathrm{Ker}\,\phi_i$. Since $\mathrm{Aut}\langle\rho_i\rangle$ is abelian, $[G^{(2)}, G^{(2)}]=\langle\sigma^2\rangle\subset N_i$. Only one of σ, τ, $\tau\sigma$ is contained in N_i because $O(G)\cap C(G)=\{1\}$. If $\sigma\notin N_i$ for some i, then either τ or $\sigma\tau$ is contained in N_i. Since $\langle\sigma^2, \tau\rangle\cong\langle\sigma^2, \tau\sigma\rangle\cong D_{2t-1}$, this shows that there exists a subquotient of G which is isomorphic to $C_2\times C_2\times C_{p_i}$. Again from (2.1) it follows that $t(\boldsymbol{Z}G)>1$. Thus we must have $\sigma\in N_i$ for each i, which implies that $G\cong D_{2tm}$.

(iii) Assume that $G/O(G)\cong D_2\cong C_2\times C_2$. Then we have $G^{(2)}\cong C_2\times C_2$ and $O(G)\neq\{1\}$. In the same way as in the case (ii) it can be shown that $O(G)\cap C(G)=\{1\}$. If there exist $\tau_1, \tau_2\in G^{(2)}$ such that $\rho\tau_1=\tau_1\rho^{-1}$ and $\rho\tau_2=\tau_2\rho$, then $G\cong C_2\times D_m\cong D_{2m}$.

Now suppose that there exist $\tau_1, \tau_2\in G^{(2)}$ such that $\rho\tau_1=\tau_1\rho^{-1}$ but $\rho\tau_2\neq\tau_2\rho^{-1}, \tau_2\rho$. Then we can find $\rho_1, \rho_2\in\langle\rho\rangle$ such that $\rho=\rho_1\rho_2$, $\rho_1\tau_2=\tau_2\rho_1^{-1}$ and $\rho_2\tau_2=\tau_2\rho_2$. Clearly $\rho_1\tau_1\tau_2=\tau_1\tau_2\rho_1$ and $\rho_2\tau_1\tau_2=\tau_1\tau_2\rho_2^{-1}$, and so $G=\langle\rho_1, \tau_1\tau_2\rangle\times\langle\rho_2, \tau_2\rangle$. Let $m_1=|\langle\rho_1\rangle|$ and $m_2=|\langle\rho_2\rangle|$. Then $(m_1, m_2)=1$ and $G\cong D_{m_1}\times D_{m_2}$. Therefore by (3.4) we have $d(\boldsymbol{Z}G)>1$.

Next suppose that, for any $\tau\in G^{(2)}-\{1\}$, $\rho\tau\neq\tau\rho^{-1}, \tau\rho$. Let $\tau_1\in G^{(2)}-\{1\}$. We can find $\rho_1, \rho_2\in\langle\rho\rangle$ such that $\rho=\rho_1\rho_2$, $\rho_1\tau_1=\tau_1\rho_1^{-1}$ and $\rho_2\tau_1=\tau_1\rho_2$. By assumption both ρ_1 and ρ_2 are different from 1. Further let $\tau_2\in G^{(2)}-\{1, \tau_1\}$. Then $\rho_2\tau_2=\tau_2\rho_2^{-1}$ because $O(G)\cap C(G)=\{1\}$, and hence we can find $\rho_1', \rho_2'\in\langle\rho_1\rangle$ such that $\rho_1=\rho_1'\rho_2'$, $\rho_1'\tau_2=\tau_2\rho_1'$ and $\rho_2'\tau_2=\tau_2\rho_2'^{-1}$. By assumption we have

$\rho_1' \neq 1$. Let $m_1=|\langle\rho_1'\rangle|$ and $m_2=|\langle\rho_2\rangle|$. Then $G/\langle\rho_2'\rangle \cong D_{m_1}\times D_{m_2}$ and therefore, by (3.4), $d(\boldsymbol{Z}G)>1$.

(iv) Assume that $G/O(G)\cong A_4$, S_4 or A_5. If $O(G)=\{1\}$, then $G\cong A_4$, S_4 or A_5, as required. Suppose that $O(G)\neq\{1\}$ and let $\phi: G\to \mathrm{Aut}\langle\rho\rangle$ be the map defined by the action of G on $\langle\rho\rangle$ by conjugation. Note that $G^{(2)}\cong (G/O(G))^{(2)}$. Then we see that $\mathrm{Ker}\,\phi$ contains a subgroup which is isomorphic to $C_2\times C_2$. Therefore there exists a subgroup H of G which is isomorphic to $C_2\times C_2\times C_m$. According to (2.1) we have $t(\boldsymbol{Z}G)>1$.

From (i)$\sim$(iv) we conclude that $G\cong D_n$ $(n\geqq 3)$, A_4, S_4 or A_5.

REMARK 4.2. It is fairly difficult to determine all integers n for which $d(\boldsymbol{Z}D_n)=1$. It should be noted ([2]) that there exists an infinite number of pairs (p, q) of distinct odd primes p, q such that $d(\boldsymbol{Z}D_{pq})>1$. Some further results on the group $T(\boldsymbol{Z}G)$ will be given in a forthcoming paper.

References

[1] P. Cassou-Noguès, Classes d'idéaux de l'algèbre d'un groupe abélien, C. R. Acad. Sci. Paris, **276** (1973), A 973-A 975. (Doctorat de Spécialité, Bordeaux, 1972).

[2] P. Cassou-Noguès, Groupe de classes de l'algèbre d'un groupe métacyclique, J. Algebra, **41** (1976), 116-136.

[3] A Fröhlich, Module invariants and root numbers for quaternion fields of degree $4l^r$, Proc. Cambridge Philos. Soc., **76** (1974), 393-399.

[4] A. Fröhlich, M.E. Keating and S.M.J. Wilson, The class group of quaternion and dihedral 2-groups, Mathematika, **21** (1974), 64-71.

[5] D. Gorenstein, Finite groups, Harper & Row Publ., New York, 1968.

[6] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie Verlag, Berlin, 1952.

[7] M.E. Keating, Class groups of metacyclic groups of order $p^r q$, p a regular prime, Mathematika, **21** (1974), 90-95.

[8] T.Y. Lam, Artin exponent of finite groups, J. Algebra, **9** (1968), 94-119.

[9] M.P. Lee, Integral representations of dihedral groups of order $2p$, Trans. Amer. Math. Soc., **110** (1964), 213-231.

[10] J. Milnor, Introduction to algebraic K-theory, Ann. of Math. Studies, Princeton Univ. Press, Princeton, 1971.

[11] I. Reiner and S. Ullom, A Mayer-Vietoris sequence for class groups, J. Algebra, **31** (1974), 305-342.

[12] M. Suzuki, On finite groups with cyclic Sylow subgroups for all odd primes, Amer. J. Math., **77** (1955), 657-691.

[13] R.G. Swan, Periodic resolutions for finite groups, Ann. of Math., **72** (1960), 267-291.

[14] S. Ullom, Nontrivial lower bounds for class groups of integral group rings, Illinois J. Math., **20** (1976), 361-371.

Shizuo ENDO
Department of Mathematics
Tokyo Metropolitan University
Fukazawa-cho, Setagaya-ku,
Tokyo, 158 Japan

Yumiko HIRONAKA
Department of Mathematics
University of Tsukuba
Sakura-mura, Niihari-gun,
Ibaraki, 300-31 Japan