TSUKUBA J. MATH.
Vol. 6 No. 2 (1982). 157—175

CLASS GROUPS OF GROUP RINGS WHOSE COEFFICIENTS ARE ALGEBRAIC INTEGERS

By

Yumiko HIRONAKA-KOBAYASHI

Let R be the ring of integers of an algebraic number field k. Let Λ be an R-order in a finite dimensional semisimple k-algebra A. We mean by the class group of Λ the class group defined by using locally free left Λ-modules and denote it by $C(\Lambda)$. We define $D(\Lambda)$ to be the kernel of the natural subjection $C(\Lambda)\rightarrow C(\Omega)$, where Ω is a maximal R-order in A containing Λ, and denote by $d(\Lambda)$ the order of $D(\Lambda)$. $C(\Omega)$ is isomorphic to a (narrow) ideal class group of the center of A, which is a product of the ideal class groups of algebraic number fields with modulus some real infinite primes. Hence, in a sense, we may concentrate on $D(\Lambda)$.

Let G be a finite group and let RG be the group ring of G with coefficients in R. Then RG can be regarded as an R-order in the semisimple k-algebra kG. We define $T(RG)$ to be the kernel of the natural surjection $C(RG)\rightarrow G(R)\oplus C(RG/(\Sigma_G))$, where $\Sigma_G=\sum_{g\in G} g\in RG$, and denote by $t(RG)$ the order of $T(RG)$. Then $T(RG)\cong\mathrm{Ker}\,(D(RG)\rightarrow D(RG/(\Sigma_G)))$. Throughout this paper, C_n denotes the cyclic group of order n and p stands for a rational prime.

Much investigation has been done on $D(\boldsymbol{Z}G)$ and $T(\boldsymbol{Z}G)$ (cf. [8]), but the results seem to depend on the speciality of $\boldsymbol{Z}$.

The purpose of this paper is to study $D(RG)$ for the case where $R\neq\boldsymbol{Z}$. In §1 we give some basic results on $D(RG)$ and $T(RG)$. In §2~§4 we assume that R is the ring of integers in a quadratic field. We first give some results on $D(RC_{p^e})$, and next examine the structure of $D(RC_p)$.

The author wishes to express her gratitude to Prof. S. Endo for the generous contribution of his time and advice, in fact, some part of this manuscript has been collabolated by those persons.

§1.

For a ring S, $U(S)$ denotes its unit group. For an abelian group A and a positive integer q, $A^{(q)}$ denotes the q-part of A and $A^{(q')}$ denotes the maximal

Received November 19, 1981.

subgroup of A whose order is coprime to q. In the case where $G=C_n$, we denote Σ_n instead of Σ_G. Let k be an algebraic number field and let R be the ring of integers of k. Let $\Phi_n(X)$ be the cyclotomic polynomial of degree n. Write $R[X]/(\Phi_n(X))=R[\zeta_n]$ (resp. $k[X]/(\Phi_n(X))=k[\zeta_n]$) where ζ_n denotes the class of X in $R[X]/(\Phi_n(X))$ (resp. $k[X]/(\Phi_n(X))$).

PROPOSITION 1.1. *$d(RC_{p^e})=|T(RC_p)^{(p')}|^e\cdot p^{f(e)}\circ\prod_{i=1}^{e} d(R[\zeta_{p^i}])$ for some integer $f(e)\geqq 0$.*

PROOF. Let $e\geqq 1$. From the pullback diagrams

$$\begin{tikzcd} RC_{p^{e+1}} \arrow[r] \arrow[d] & R[X]/(\Phi_{p^{e+1}}(X))=R[\zeta_{p^{e+1}}] \arrow[d] \\ RC_{p^e} \arrow[r] & (R/pR)C_{p^e} \end{tikzcd}, \qquad \begin{tikzcd} RC_p \arrow[r] \arrow[d] & R[\zeta_p] \arrow[d] \\ R \arrow[r] & R/pR \end{tikzcd},$$

we have an exact sequence

$$0 \longrightarrow K \longrightarrow D(RC_{p^{e+1}}) \longrightarrow D(RC_{p^e})\oplus D(R[\zeta_{p^{e+1}}]) \longrightarrow 0$$

and a commutative diagram with exact rows

$$\begin{tikzcd} U(RC_{p^e})\oplus U(R[\zeta_{p^{e+1}}]) \arrow[r] \arrow[d, "\varphi'"] & U((R/pR)C_{p^e}) \arrow[r] \arrow[d, "\varphi"] & K \arrow[r] \arrow[d] & 0 \\ U(R)\oplus U(R[\zeta_p]) \arrow[r] & U(R/pR) \arrow[r] & T(RC_p) \arrow[r] & 0, \end{tikzcd}$$

where the vertical maps are induced by the norm maps. Since φ is bijective on the p'-parts and Coker φ' is a p-group, we see that $K^{(p')}\cong T(RC_p)^{(p')}$. Hence, by induction on e, we have the equality as desired.

COROLLARY 1.2. *Suppose that p is unramified in R. Then*
 i) *$D(RC_p)$ $(=T(RC_p))$ is a p'-group.*
 ii) *If $d(RC_p)=1$, then $D(RP)$ is a p-group for every p-group P.*

PROOF. i) Since p is unramified in R, $U(R/pR)$ is a p'-group and $R[\zeta_{p^i}]$ is a Dedekind domain for every $i\geqq 1$. The assertion follows from these facts. ii) If $d(RC_p)=1$, then $D(RC_{p^e})$ is a p-group by (1.1). Then, by the induction theorem of Artin ([1, § 1]), we see that $D(RP)$ is a p-group for every p-group P.

PROPOSITION 1.3. i) *$T(RC_n)\cong\bigoplus_{p|n} T(RC_{p^{e_p}})$ where $p^{e_p}\|n$ for each $p|n$.*
 ii) *There is an exact sequence*

$$0 \longrightarrow P_e \longrightarrow T(RC_{p^e}) \longrightarrow T(RC_p) \longrightarrow 0,$$

where P_e is a p-group whose exponent divides p^{e-1} (resp. p^e) if p is unramified in R (resp. ramified in R).

iii) *Let G be a finite group of order n. If $p|t(RG)$, then $p|n$ or $p|t(RC_q)$ for some prime factor q of n.*

Proof. i) Let $\tilde{\mathcal{M}}=R\oplus\mathcal{M}$ be a maximal R-order in $kC_n\cong k\oplus kC_n/(\Sigma_n)$ containing RC_n. By ([2, Theorem 1]), we have

$$D(RC_n)\cong\frac{\prod_{p|n}U(\tilde{\mathcal{M}}_p)}{U(\tilde{\mathcal{M}})\prod_{p|n}U(R_pC_n)},$$

where $\tilde{\mathcal{M}}_p=\boldsymbol{Z}_p\underset{\boldsymbol{Z}}{\otimes}\tilde{\mathcal{M}}$ and $R_p=\boldsymbol{Z}_p\underset{\boldsymbol{Z}}{\otimes}R$. Since R_p can be embedded in $\mathcal{M}_p$, the map $U(\tilde{\mathcal{M}}_p)=U(R_p)\times U(\mathcal{M}_p)\to U(\mathcal{M}_p)$; $(x, y)\mapsto yx^{-1}$, induces an isomorphism

$$D(RC_n)\cong\frac{\prod_{p|n}U(\mathcal{M}_p)}{U(\mathcal{M})\prod_{p|n}u(R_pC_n)},$$

where $u(R_pC_n)=\{x|(1, x)\in U(R_pC_n)\hookrightarrow U(R_p)\times U(R_pC_n/(\Sigma_n))\}$. On the other hand, we have

$$D(RC_n/(\Sigma_n))\cong\frac{\prod_{p|n}U(\mathcal{M}_p)}{U(\mathcal{M})\prod_{p|n}U(R_pC_n/(\Sigma_n))}.$$

Hence we get

$$T(RC_n)\cong\frac{U(\mathcal{M})\prod_{p|n}U(R_pC_n/(\Sigma_n))}{U(\mathcal{M})\prod_{p|n}u(R_pC_n)}.$$

For each $p|n$, let e_p be the integer such that $p^{e_p}\|n$. Since $R_pC_n/(\Sigma_n)\cong R_pC_{p^{e_p}}/(\Sigma_{p^{e_p}})\oplus(\bigoplus_{\substack{d|n/p^{e_p}\\ d\neq1}}R_pC_{p^{e_p}}[\zeta_d])$ and $R_pC_n\cong R_pC_{p^{e_p}}\oplus(\bigoplus_{\substack{d|n/p^{e_p}\\ d\neq1}}R_pC_{p^{e_p}}[\zeta_d])$, we see that

$$T(RC_n)\cong\prod_{p|n}\frac{U(\mathcal{M}(p))U(R_pC_{p^{e_p}}/(\Sigma_{p^{e_p}}))}{U(\mathcal{M}(p))n(R_pC_{p^{e_p}})},$$

where $\mathcal{M}(p)$ is a maximal R-order in $kC_p/(\Sigma_{p^{e_p}})$ containing $RC_{p^{e_p}}/(\Sigma_{p^{e_p}})$. This shows that $T(RC_n)\cong\bigoplus_{p|n}T(RC_{p^{e_p}})$.

ii) Let $\mathcal{O}_i$ be the maximal R-order in $k[\zeta_{p^i}]$ containing $R[\zeta_{p^i}]$, $1\leqq i\leqq e$. Then $\mathcal{M}=\bigoplus_{i=1}^{e}\mathcal{O}_i$ is a maximal R-order in $kC_{p^e}/(\Sigma_{p^e})$ containing $RC_{p^e}/(\Sigma_{p^e})$, and we have

$$T(RC_{p^e})\cong\frac{U(\mathcal{M})U(R_pC_{p^e}/(\Sigma_{p^e}))}{U(\mathcal{M})u(R_pC_{p^e})}\quad\text{and}\quad T(RC_p)\cong\frac{U(\mathcal{O}_1)U(R[\zeta_p])}{U(\mathcal{O}_1)u(R_pC_p)}.$$

The natural surjection $C_{p^e}\to C_{p^e}/C_{p^{e-1}}\cong C_p$ induces the surjection $T(RC_{p^e})\to T(RC_p)$; $(x, y)\mapsto x$ where $(x, y)\in U(\mathcal{O}_{1,p}\oplus(\bigoplus_{i=2}^{e}\mathcal{O}_{i,p}))$. Set $P_e=\mathrm{Ker}(T(RC_{p^e})\to T(RC_p))$. Each $\alpha\in P_e$ is represented by an element $(x, y)\in U(R_pC_{p^e}/(\Sigma_{p^e}))$ such that $x=uv$ for some $u\in U(\mathcal{O}_1)$ and $(1, v)\in U(R_pC_p)$. Let $f(\bar{\sigma})=\sum_{i=0}^{p^e-2}b_i\bar{\sigma}^i=(x, y)$ $\in U(R_pC_{p^e}/(\Sigma_{p^e}))$, where $b_i\in R_p$ and $\bar{\sigma}$ denotes the image of a generator σ of C_{p^e} in $R_pC_{p^e}/(\Sigma_{p^e})$, and let $f(\sigma)=\sum_{i=0}^{p^e-2}b_i\sigma^i\in R_pC_{p^e}$. Then $x=f(\zeta_p)\equiv\sum_{i=0}^{p^e-2}b_i\equiv uv$ $\equiv u\ (\mathrm{mod}\,(\zeta_p-1)\mathcal{O}_{1,p})$, and so we see that $f(1)=\sum_{i=0}^{p^e-2}b_i\in U(R_p)$. Hence $f(\sigma)\in U(R_pC_{p^e})$. Then $\alpha=\overline{(x, y)}=\overline{(f(1), f(1))}$, because $(x^{-1}f(1), y^{-1}f(1))\in u(R_pC_{p^e})$. Thus we know that

$$P_e\subseteq N=\left\{\rho_x=(x, x)\in T(RC_{p^e})\,\middle|\,\begin{array}{l}x\in U(R_p),\ x\equiv u\ (\mathrm{mod}\,(\zeta_p-1)\mathcal{O}_{1,p})\\ \text{for some } u\in U(\mathcal{O}_1)\end{array}\right\}.$$

It is easily verified that

$$(*)\qquad p^eR\oplus p^{e-1}(\zeta_p-1)R[\zeta_p]\oplus p^{e-2}(\zeta_p-1)R[\zeta_{p^2}]\oplus\cdots\oplus(\zeta_p-1)R[\zeta_{p^e}]\subseteq RC_{p^e}.$$

Let $\rho_x\in N$ and $x\equiv u\ (\mathrm{mod}\,(\zeta_p-1)\mathcal{O}_{1,p})$, $u\in U(\mathcal{O}_1)$. If p is unramified in R, then $\mathcal{O}_i=R[\zeta_{p^i}]$ and $u^{-1}x\in 1+(\zeta_p-1)\mathcal{O}_{1,p}$, and hence $(u^{-1}x)^{p^{e-1}}\in 1+(\zeta_p-1)p^{e-1}\mathcal{O}_{1,p}$. By force of (*), we know that $\rho_x^{p^{e-1}}=1$ in $T(RC_{p^e})$. Thus we see that $\exp(P_e)\,|\,p^{e-1}$. Even if p is ramified in R, $(u^{-1}x)^p\in 1+(\zeta_p-1)R_p[\zeta_p]$, and so we have $\exp(P_e)\,|\,p^e$.

iii) By the induction theorem of Artin ([1, § 1]), we have that $T(RG)^{(n')}\cong\sum_C T(RC)^{(n')}$, where C ranges over all cyclic subgroups of G. The result follows from i) and ii).

REMARK 1.4. By force of (*) above, if p is unramified in R, we can see that the exponent of $D(RC_{p^e})^{(p)}$ divides p^{e-1}. Further assume that R is the ring of integers of a real algebraic number field k and $p\geqq 5$. Then $\exp(D(RC_{p^e})^{(p)})=p^{e-1}$.

In fact, let τ denote the endomorphism of RC_{p^e} induced by $\sigma\mapsto\sigma^{-1}$, where $C_{p^e}=\langle\sigma\rangle$. Then $D(RC_{p^e})$ can be regarded as a $\langle\tau\rangle$-module. For every $\langle\tau\rangle$-module M, we put $M^-=\{m\in M\,|\,m^\tau=m^{-1}\}$. Let V be the kernel of the natural surjection $D(RC_{p^{e+1}})^{(p)}\to D(RC_{p^e})^{(p)}$. Then, along the almost same line as in ([4]), we can show that $V^-\cong\bigoplus_{a=1}^{e}(\boldsymbol{Z}/p^a\boldsymbol{Z})^{v_a}$, where $v_a=(1/2)[k:\boldsymbol{Q}](p-1)^2p^{e-a-1}$ for $a<e$ and $v_e=(1/2)[k:\boldsymbol{Q}](p-1)-g$, g is the number of prime ideals in R over p.

PROPOSITION 1.5. *Suppose that p is unramified in R. Then*

$$D(RC_{p^e})^{(p')} \cong D(RC_p)^e \qquad (direct\ sum).$$

PROOF. Let $\mathcal{O}_i = R[\zeta_{p^i}]$, $1 \leqq i \leqq e$. Then $\mathcal{O}_i$ is a Dedekind domain and $\bigoplus_{i=1}^{e} \mathcal{O}_i$ is a maximal R-order in $kC_{p^e}/(\Sigma_{p^e})$ containing $RC_{p^e}/(\Sigma_{p^e})$, and the product p_i of all prime ideals over p in $\mathcal{O}_i$ equals $(1-\zeta_{p^i})$, $1 \leqq i \leqq e$. Hence we get

$$D(RC_{p^e}) \cong \prod_{i=1}^{e} U(\mathcal{O}_{i,p}) \Big/ \prod_{i=1}^{e} U(\mathcal{O}_i) u(R_p C_{p^e})$$

$$= \left[\prod_{i=1}^{e} \frac{U(R/pR)}{\varphi_i(U(\mathcal{O}_i))} \right] \times \left[\frac{\prod_{i=1}^{e} (1+p_i \mathcal{O}_{i,p})}{\prod_{i=1}^{e} U^1(\mathcal{O}_i) u(R_p C_{p^e})} \right],$$

where φ_i is induced by the natural surjection $\mathcal{O}_i \to \mathcal{O}_i/p_i \cong R/pR$ and $U^1(\mathcal{O}_i) = \operatorname{Ker} \varphi_i = U(\mathcal{O}_i) \cap (1+p_i \mathcal{O}_{i,p})$. Then it is easily seen that the former factor is isomorphic to $D(RC_{p^e})^{(p')}$. On the other hand, $|D(RC_{p^e})^{(p')}| = d(RC_p)^e$ by (1.1) and (1.2), and so we have

$$U(R/pR)/\varphi_i(U(\mathcal{O}_i)) \cong D(RC_p), \qquad 1 \leqq i \leqq e.$$

Thus we complete the proof.

§2.

Hereafter, let k denote $\boldsymbol{Q}(\sqrt{m})$, a quadratic field, where m is a square-free integer, and R be the ring of integers of k. We write $w_m = \sqrt{m}$ (resp. $\sqrt{m}+1/2$) if $m \not\equiv 1 \pmod 4$ (resp. $m \equiv 1 \pmod 4$).

Let $\mathcal{O}_i$ be the maximal R-order in $k[\zeta_{p^i}]$ and p_i be the product of all the prime ideals over p in $\mathcal{O}_i$, $1 \leqq i \leqq e$. Then

$$D(RC_{p^e}) \cong \prod_{i=1}^{e} U(\mathcal{O}_{i,p}) \Big/ \prod_{i=1}^{e} U(\mathcal{O}_i) u(R_p C_{p^e})$$

$$\cong \left[\prod_{i=1}^{e} \frac{U(\mathcal{O}_i/p_i)}{\varphi_i(U(\mathcal{O}_i))} \right] \times \left[\frac{\prod_{i=1}^{e} (1+p_i \mathcal{O}_{i,p})}{\prod_{i=1}^{e} U^1(\mathcal{O}_i) u(R_p C_{p^e})} \right],$$

where $\varphi_i : U(\mathcal{O}_i) \to U(\mathcal{O}_i/p_i)$ is the natural map and $U^1(\mathcal{O}_i) = \operatorname{Ker} \varphi_i$, $1 \leqq i \leqq e$. It is easily seen that the latter factor is isomorphic to $D(RC_{p^e})^{(p)}$.

PROPOSITION 2.1. *Let p be unramified in R, i.e. $p \nmid m$ if $p \neq 2$ and $m \equiv 1$ (mod 4) if $p=2$. Then*

$$\exp(D(RC_{p^e})^{(p)}) \mid p^{e-1} \quad and \quad D(RC_{p^e})^{(p')} \cong D(RC_p)^e.$$

PROOF. This is a special case of (1.4) and (1.5).

We write $p^*=(-1)^{p-1/2}p$.

PROPOSITION 2.2. *Let $p|m$, and $m\neq p^*$ if $p\neq 2$, and let $m\not\equiv 1$ (mod 4) and $m\neq -1$, ± 2 if $p=2$. Then*

i) *The exponent of $D(RC_{p^e})^{(p)}$ divides*

$$\begin{cases} 2^{e+1} & \text{if } p=2,\ m\equiv 2 \pmod 4 \text{ and } e>1, \text{ or} \\ p^e & \text{otherwise.} \end{cases}$$

ii) *For the case $p\neq 2$ and $m=np^*$,*

$$D(RC_{p^e})^{(p')}\cong D(R'C_p)^e \qquad \text{where } R'=\boldsymbol{Z}[w_n].$$

iii) *For the case $p=2$ and $m=-n$ where $n\equiv 1$ (mod 4),*

$$D(RC_{2^e})^{(2')}\cong D(R'C_2)^{e-1} \qquad \text{where } R'=\boldsymbol{Z}[w_n].$$

iv) *For the case $p=2$ and $m=2n$ or $-2n$ where $n\equiv 1$ (mod 4),*

$$D(RC_{2^e})^{(2')}\cong\begin{cases} 0 & \text{if } e=1,2 \\ D(R'C_2)^{e-2} & \text{if } e\geqq 3, \end{cases}$$

where $R'=\boldsymbol{Z}[w_n]$.

PROOF. If $p\neq 2$ and $m=np^*$, then we see that $\mathcal{O}_i=\boldsymbol{Z}[w_n, \zeta_{p^i}]$, $p_i=(1-\zeta_{p^i})$ and $p\mathcal{O}_i\subseteqq R[\zeta_{p^i}]$, $1\leqq i\leqq e$. Hence we get that $\exp(D(RC_{p^e})^{(p)})\,|\,p^e$ and $D(RC_{p^e})^{(p')}\cong D(R'C_{p^e})^{(p')}\cong D(R'C_p)^e$, where $R'=\boldsymbol{Z}[w_n]$.

If $p=2$, $m=-n$ and $n\equiv 1$ (mod 4), then we see that $\mathcal{O}_1=R$ and $\mathcal{O}_i=\boldsymbol{Z}[w_n, \zeta_{2^i}]$ for $i\geqq 2$. Then, it is easy to see that $\exp(D(RC_{2^e})^{(2)})\,|\,2^e$ and $D(RC_2)=0$. For $e\geqq 2$, we have

$$D(RC_{2^e})^{(2')}\oplus D(R'C_2)\cong D(R'C_{2^e})^{(2')},$$

where $R'=\boldsymbol{Z}[w_n]$, and so, by (2.1),

$$D(RC_{2^e})^{(2')}\cong D(R'C_2)^{e-1}.$$

If $p=2$, $m=2n$ or $-2n$ and $n\equiv 1$ (mod 4), then $\mathcal{O}_1=R$, $\mathcal{O}_2=\boldsymbol{Z}[\sqrt{m}, \sqrt{-1}, \sqrt{m}+\sqrt{-1}/2]$ and $\mathcal{O}_i=\boldsymbol{Z}[w_n, \zeta_{2^i}]$ for $i\geqq 3$. The assertion can be shown similarly for this case.

PROPOSITION 2.3. *Let $m=p^*$ if $p\neq 2$ and let $m=-1$, ± 2 if $p=2$. Then the exponent of $D(RC_{p^e})$ divides p^e. Especially, it divides p^{e-1} if $p=3$, 5 or $p=2$ and $m=-1$.*

PROOF. Put $\mathcal{O}_i=\boldsymbol{Z}[\zeta_{p^i}]$, $1\leqq i\leqq e$. If $p\neq 2$, then $R\oplus\bigoplus_{i=1}^{e}(\mathcal{O}_i\oplus\mathcal{O}_i)$ is a maximal R-order in kC_{p^e} containing RC_{p^e}, and so we have

$$D(RC_{p^e}) \cong \frac{\prod_{i=1}^{e} U(\mathcal{O}_{i,p}\oplus\mathcal{O}_{i,p})}{\prod_{i=1}^{e} U(\mathcal{O}_i\oplus\mathcal{O}_i)u(R_pC_{p^e})}$$

$$\cong \frac{\prod_{i=1}^{e} \{(1+\pi_i\mathcal{O}_{i,p})\times(1+\pi_i\mathcal{O}_{i,p})\}}{\{\prod_{i=1}^{e} U^1(\mathcal{O}_i)\times U^1(\mathcal{O}_i)\}\, u(R_pC_{p^e})},$$

where $\pi_i=\zeta_{p^i}-1$ is a prime element of $\mathcal{O}_{i,p}$ and $U^1(\mathcal{O}_i)=U(\mathcal{O}_i)\cap(1+\pi_i\mathcal{O}_{i,p})$. Hence $D(RC_{p^e})$ is a p-group. It is easy to see that $u(R_pC_{p^e})$ contains $\prod_{i=1}^{e} \{(1+\pi^{t_i}\mathcal{O}_{i,p})\times(1+\pi^{t_i}\mathcal{O}_{i,p})\}$, where $\pi=\pi_1$ and $t_i=1+(p-1/2)+(p-1)(e-i)$. The assertion follows from the facts that $U^1(\mathcal{O}_i)\ni\zeta_{p^i}=1+\pi_i$ for each p^i and $U(\mathcal{O}_i)\ni 3+(\zeta_{p^i}+\zeta_{p^i}^{-1}-2)$ unless $p=3$ and that $(1+\pi_i{}^k\mathcal{O}_{i,p})^{p^{i-1}p^m}\subseteqq 1+\pi^{(p-1)m+k}\mathcal{O}_{i,p}$ for every $1\leqq k\leqq p-1$, $m\geqq 1$ and $i\geqq 1$. The assertion for $p=2$ can be similarly shown.

§ 3.

Let R be the ring of integers of $k=\boldsymbol{Q}(\sqrt{m})$. In the case $m>0$, we denote a fundamental unit of R by ε_m. ε_m can be written as $a+b\sqrt{m}$, $a, b\in\boldsymbol{Z}$ or $(a+b\sqrt{m})/2$, $a, b\in\boldsymbol{Z}$, $2\nmid ab$.

Here we investigate $D(RC_p)$ more precisely.

There is an exact sequence

$$0 \longrightarrow D(RC_2) \longrightarrow C(RC_2) \longrightarrow C(R)\oplus C(R) \longrightarrow 0$$

and $T(RC_2)=D(RC_2)$. Further we have easily

PROPOSITION 3.1.

$D(RC_2)$	$m<0$	$m>0$
$\boldsymbol{Z}/3\boldsymbol{Z}$	$m\equiv 5 \pmod 8$ *and* $m<-3$	$m\equiv 5 \pmod 8$ *and* $\varepsilon_m\in\boldsymbol{Z}[\sqrt{m}]$
$\boldsymbol{Z}/2\boldsymbol{Z}$	$m\equiv 2$ *or* $3 \pmod 4$ *and* $m<-1$	$m\equiv 2$ *or* $3 \pmod 4$ *and* $2\mid b$
0	$m\equiv 1 \pmod 8$, $m=-1$ *or* -3	$m\equiv 1 \pmod 8$, $m\equiv 5 \pmod 8$ *and* $\varepsilon_m\notin\boldsymbol{Z}[\sqrt{m}]$ *or* $m\equiv 2$ *or* $3 \pmod 4$ *and* $2\nmid b$

From now on, p is assumed to be an odd prime. From the pullback diagram

$$\begin{array}{ccc} RC_p & \longrightarrow & R \\ \downarrow & & \downarrow \\ R[\bar{\sigma}]=RC_p/(\Sigma_p) & \xrightarrow[\tilde{\psi}]{} & R/pR=\boldsymbol{F}_p[\sqrt{m}], \end{array} \quad \text{where } C_p=\langle\sigma\rangle,$$

we have exact sequences

$$U(R[\bar{\sigma}]) \xrightarrow{\psi} U(\boldsymbol{F}_p[\sqrt{m}]) \xrightarrow{\xi} T(RC_p) \longrightarrow 0$$

$$0 \longrightarrow T(RC_p) \longrightarrow D(RC_p) \longrightarrow D(R[\bar{\sigma}]) \longrightarrow 0.$$

Here ψ is the restriction of the canonical surjection $\tilde{\psi}: R[\bar{\sigma}]\to R[\bar{\sigma}]/(\bar{\sigma}-1)$, $\xi(\tilde{\psi}(x))=$ *the class of the ideal* (x, Σ_p) and

$$\boldsymbol{F}_p[\sqrt{m}]=\begin{cases} \boldsymbol{F}_p\oplus\boldsymbol{F}_p & \text{if } \left(\dfrac{m}{p}\right)=1 \\ \boldsymbol{F}_{p^2} & \text{if } \left(\dfrac{m}{p}\right)=-1, \end{cases}$$

where $\left(\dfrac{m}{p}\right)$ is the quadratic residue symbol.

Let $p\nmid m$ and let r be an element of $R[\bar{\sigma}]=R[\zeta_p]$ such that

i) if $\left(\dfrac{m}{p}\right)=1$, then $\psi(r)=(a, 1)\in U(\boldsymbol{F}_p)\oplus U(\boldsymbol{F}_p)$, where a is a generator of $U(\boldsymbol{F}_p)$,

ii) if $\left(\dfrac{m}{p}\right)=-1$, then $\psi(r)$ is a generator of $U(\boldsymbol{F}_{p^2})$.

Noticing that $\psi(U(\boldsymbol{Z}[\zeta_p]))=U(\boldsymbol{F}_p)$, we have

LEMMA 3.2. *In the case $p\nmid m$, $D(RC_p)$ $(=T(RC_p))$ is a cyclic group generated by the class of (r, Σ_p), where r is given as above. Its order divides $p-1$ (resp. $p+1$) if $\left(\dfrac{m}{p}\right)=1$ (resp. $\left(\dfrac{m}{p}\right)=-1$).*

For an imaginary abelian field K, let K_0 be the maximal real subfield of K. Denote by U (resp. U_0) the group of units in the ring of integers of K (resp. K_0) and denote by W the group of roots of unity contained in K. Then the unit index Q_K of K is defined by the index $[U: WU_0]$. It is known that $Q_K=1$ or 2. (cf. [3, § 20-26])

Assume that $p\nmid m$ and $m<0$. Let $K=\boldsymbol{Q}(\zeta_p, \sqrt{m})$ and $K_1=\boldsymbol{Q}(\zeta_p+\zeta_p^{-1})$. Let $\mathrm{Gal}(K/\boldsymbol{Q})=\langle\sigma, \tau \mid \sigma^{p-1}=\tau^2=1,\ \sigma\tau=\tau\sigma\rangle$, $\mathrm{Gal}(K/K_0)=\langle\sigma^{p-1/2}\tau\rangle$ and $\mathrm{Gal}(K/K_1)=\langle\sigma^{p-1/2}, \tau\rangle$. The characters of K are given as follows:

i) the characters of K/K_0;

$$\begin{cases} \sigma \longmapsto \zeta_{p-1}^{i} \\ \tau \longmapsto 1, \qquad 1 \leqq i \leqq p-1 \text{ and } 2 \nmid i. \end{cases}$$

$$\begin{cases} \sigma \longmapsto \zeta_{p-1/2}^{j} \\ \tau \longmapsto -1, \qquad 1 \leqq j \leqq \dfrac{p-1}{2}. \end{cases}$$

ii) the characters of K_0;

$$\begin{cases} \sigma \longmapsto \zeta_{p-1}^{i} \\ \tau \longmapsto -1, \qquad 1 \leqq i \leqq p-1 \text{ and } 2 \nmid i. \end{cases}$$

$$\begin{cases} \sigma \longmapsto \zeta_{p-1/2}^{j} \\ \tau \longmapsto 1, \qquad 1 \leqq j \leqq \dfrac{p-1}{2}. \end{cases}$$

Then we see that K/K_0 is unramified at p. Since we can compute the absolute discriminants of K_1 and K_0, we see that the discriminant $d_{K_0/K_1}=(\pi^2 m^*)$, where $\pi=\zeta_p-\zeta_p^{-1}$ and $m^*=\begin{cases} m & \text{if } m\equiv 1 \pmod 4 \\ 4m & \text{otherwise} \end{cases}$. Thus, (p) is totally ramified in K_0/Q, and so there is a unique prime ideal $\mathfrak{P}$ over (p) in K_0. It is easy to see that $\mathfrak{P}=(\pi^2, \pi\sqrt{m})$.

PROPOSITION 3.3. *Assume that $p \nmid m$ and $m<0$. Let $K=\boldsymbol{Q}(\zeta_p, \sqrt{m})$ and let $\mathcal{O}$ be the ring of integers of K. Then the following conditions are equivalent.*

i) $Q_K=2$.

ii) *$\mathfrak{P}$ is a principal ideal in K_0.*

iii) *There exists a unit of $\mathcal{O}$ of the form $(\pi x+\sqrt{m}y)/2$, where $x, y\in \boldsymbol{Z}[\zeta_p+\zeta_p^{-1}]$.*

PROOF. It is easy to see that i) is equivalent to

i′) $K=K_0(\sqrt{\varepsilon})$ for some unit ε of the ring $\mathcal{O}_0$ of integers of K_0.

On the other hand, we have

$$K=K_0(\zeta_p)=K_0(\sqrt{(\zeta_p-\zeta_p^{-1})^2}) \quad \text{and}$$

$$((\zeta_p-\zeta_p^{-1})^2)=\mathfrak{P}^2 \qquad \text{as ideals in } \mathcal{O}_0.$$

Thus we get the equivalence between i) and ii). Let $K_1=\boldsymbol{Q}(\zeta_p+\zeta_p^{-1})$ and $\mathcal{O}_1$ be the ring of integers of K_1. Then $K_0=K_1(\pi\sqrt{m^*})$, and so $\mathcal{O}_1$ has an integral basis with respected to $\mathcal{O}_0$, since $d_{K_0/K_1}=(\pi^2 m^*)$ ([6]). As the discriminant of $\pi\sqrt{m}$ with respected to K_0/K_1 is equals to $4\pi^2 m$, we see that $[\mathcal{O}_0 : \mathcal{O}_1[\pi\sqrt{m}]]=1$ or 2. Thus every element of $\mathcal{O}_0$ can be written uniquely with the form

$(x+\pi\sqrt{m}y)/2$, $x, y\in\mathcal{O}_1$. Assume the condition ii). Let $\alpha=(x'+\pi\sqrt{m}y)/2$, x', $y\in\mathcal{O}_1$, be a generator of $\mathcal{P}$. Since $\mathcal{P}\mathcal{O}=\pi\mathcal{O}$, π must divide x', and so we have $\pi^2|x'$. Thus α can be writtn as $(\pi^2x+\pi\sqrt{m}y)/2$. Then it is clear that $(\pi x+\sqrt{m}y)/2$ is a unit of $\mathcal{O}$, hence we have iii). Conversely, if there exists such a unit ε in $\mathcal{O}$, then $\pi\varepsilon$ is an element of K_0 and generates $\mathcal{P}$. This completes the proof.

THEOREM 3.4. *Assume that $p\nmid m$ and $m<0$. Let $K=\boldsymbol{Q}(\zeta_p, \sqrt{m})$. Then*

i) *The case where $m\neq -1, -3$:*

$$d(RC_p)=\begin{cases} p-1 & \text{if } \left(\frac{m}{p}\right)=1 \text{ and } Q_K=1 \\ \frac{p-1}{2} & \text{if } \left(\frac{m}{p}\right)=1 \text{ and } Q_K=2 \\ p+1 & \text{if } \left(\frac{m}{p}\right)=-1 \text{ and } Q_K=1 \\ \frac{p+1}{2} & \text{if } \left(\frac{m}{p}\right)=-1 \text{ and } Q_K=2. \end{cases}$$

ii) *The case where $m=-1$:*

$$d(RC_p)=\begin{cases} \frac{p-1}{4} & \text{if } p\equiv 1 \pmod 4 \\ \frac{p+1}{4} & \text{if } p\equiv 3 \pmod 4. \end{cases}$$

iii) *The case where $m=-3$:*

$$d(RC_p)=\begin{cases} \frac{p-1}{6} & \text{if } p\equiv 1 \pmod 3 \\ \frac{p+1}{6} & \text{if } p\equiv -1 \pmod 3. \end{cases}$$

PROOF. There is an exact sequence

$$U(\mathcal{O}) \xrightarrow{\phi} U(\boldsymbol{F}_p[\sqrt{m}]) \longrightarrow D(RC_p) \longrightarrow 0.$$

Since (p) is totally ramified in $K_0/\boldsymbol{Q}$, we see that $\phi(U(\mathcal{O}_0))\subseteqq U(\boldsymbol{F}_p)$. On the other hand, we have $\phi(U(\mathcal{O}_1))=U(\boldsymbol{F}_p)$. Let $m\neq -1, -3$. If $Q_K=1$, then $U(\mathcal{O})=\langle\zeta_p\rangle U(\mathcal{O}_0)$. Thus we have

$$d(RC_p)=\begin{cases} p-1 & \text{if } \left(\frac{m}{p}\right)=1 \\ p+1 & \text{if } \left(\frac{m}{p}\right)=-1. \end{cases}$$

If $Q_K=2$, then $U(\mathcal{O})=\langle\zeta_p,\ \varepsilon=(\pi x+my)/2\rangle U(\mathcal{O}_0)$, for some $\varepsilon\in U(\mathcal{O})$ by (3.3). $\phi(\varepsilon)\notin U(\boldsymbol{F}_p)$ and $\varepsilon^2\in\langle\zeta_p\rangle U(\mathcal{O}_0)$, hence we see that

$$d(RC_p)=\begin{cases}\dfrac{p-1}{2} & \text{if } \left(\dfrac{m}{p}\right)=1\\[2ex] \dfrac{p+1}{2} & \text{if } \left(\dfrac{m}{p}\right)=-1\,.\end{cases}$$

Let $m=-1$. Then $K=\boldsymbol{Q}(\zeta_p,\zeta_4)$ and $U(\mathcal{O})=\langle\zeta_p,\sqrt{-1},\ \varepsilon=1-\sqrt{-1}\,\zeta_p\rangle U(\mathcal{O}_0)$. $\phi(\varepsilon)$ is of order 4 in $U(\boldsymbol{F}_p[\sqrt{-1}])/U(\boldsymbol{F}_p)$. Thus we see that

$$d(RC_p)=\begin{cases}\dfrac{p-1}{4} & \text{if } p\equiv 1 \pmod 4\\[2ex] \dfrac{p+1}{4} & \text{if } p\equiv 3 \pmod 4\,.\end{cases}$$

Let $m=-3$. Then $K=\boldsymbol{Q}(\zeta_p,\zeta_3)$ and $U(\mathcal{O})=\langle\zeta_p,\zeta_3,\ \varepsilon=1-\zeta_3\zeta_p\rangle U(\mathcal{O}_0)$. $\phi(\varepsilon)$ is of order 6 in $U(\boldsymbol{F}_p[\sqrt{-3}])/U(\boldsymbol{F}_p)$. Since $\left(\dfrac{-3}{p}\right)=\left(\dfrac{p}{3}\right)$, we see that

$$d(RC_p)=\begin{cases}\dfrac{p-1}{6} & \text{if } p\equiv 1 \pmod 3\\[2ex] \dfrac{p+1}{6} & \text{if } p\equiv -1 \pmod 3\,.\end{cases}$$

REMARK 3.5. 1) Assume that $p\equiv 3 \pmod 4$ and $m\neq -1,\ -3$. Let $M=\boldsymbol{Q}(\sqrt{-p},\sqrt{m})$ and let $\varepsilon>0$ be a fundamental unit of $M_0=\boldsymbol{Q}(\sqrt{-mp})$. Then the following conditions are equivalent.

i) $Q_K=2$ ii) $Q_M=2$ iii) $\sqrt{-\varepsilon}\in M$.

2) Assume that $p\equiv 1 \pmod 4$ and $m=-q$, where q is a prime and $q\equiv 3 \pmod 4$. Then $Q_K=2$.

PROOF. 1) The equivalence between ii) and iii) is clear. By [3, Satz 29], ii) implies i). Let p be the unique prime ideal over (p) in M_0. Then it is easy to see that ii) is equivalent to the condition that p is principal. If $Q_K=2$, then we can take a generator α of $\mathcal{P}$. Since $N_{K_0/M_0}(\mathcal{P})=p$, we see that $N_{K_0/M_0}(\alpha)$ generates p. This establishes 1). 2) We may assume that $q\neq 3$. Let b be a primitive root modulo q, and let $\varepsilon=\prod_{i=0}^{q-3/2}(1-\zeta_q^{b^{2i}}\zeta_p)$. Then $\varepsilon\in U(\mathcal{O})$ and $\phi(\varepsilon)=\tilde{\phi}(\prod_{i=0}^{q-3/2}(1-\zeta_q^{b^{2i}}))=\tilde{\phi}(\pm\sqrt{-q})\notin U(\boldsymbol{F}_p)$. Hence $\varepsilon\notin\langle\zeta_p\rangle U(\mathcal{O}_0)$, and so $Q_K=2$.

The next result is a special case of [3, Satz 22]. We give a direct proof based on the idea of T. Miyata ([7, (2.6)]).

LEMMA 3.6. *Suppose that* $m>0$ *and* $w_m \notin Z[\zeta_p]$. *Then* $U(Z[w_m, \zeta_p])=\langle\zeta_p\rangle U(Z[w_m, \zeta_p+\zeta_p^{-1}])$.

PROOF. Let τ be the complex conjugation. For every $u\in U(Z[w_m, \zeta_p])$, $(u^\tau/u)(u^\tau/u)^\tau=1$. So we see that u^τ/u is a root of unity in $U(Z[w_m, \zeta_p])$. Since u^τ/u is mapped to 1 by the map ψ: $U(Z[w_m, \zeta_p])\to U(F_p[w_m])$, $u^\tau/u=\zeta_p{}^i$ for some i. Then there is an integer j such that $(\zeta_p{}^j u)^\tau=\zeta_p{}^j u$. Hence we see that $U(Z[w_m, \zeta_p])=\langle\zeta_p\rangle U(Z[w_m, \zeta_p+\zeta_p^{-1}])$.

Let $p \nmid m$, $m>0$, $N_{Q(\sqrt{m})/Q}(\varepsilon_m)=-1$ and $p\equiv 1 \pmod 4$. Then a system of fundamental units of $Z[w_p, w_m]$ is given as one of the following three types ([5, Satz 11]):

(a) ε_p, ε_m and ε_{pm},

(b) ε_p, ε_m and $\sqrt{\varepsilon_{pm}}$ (in this case, $N_{Q(\sqrt{pm})/Q}(\varepsilon_{pm})=1$), or

(c) ε_p, ε_m and $\sqrt{\varepsilon_p\varepsilon_m\varepsilon_{pm}}$ (in this case, $N_{Q(\sqrt{pm})/Q}(\varepsilon_{pm})=-1$).

THEOREM 3.7. *Suppose that* $p\nmid m$ *and* $m>0$. *Then*

i) *If* $N_{Q(\sqrt{m})/Q}(\varepsilon_m)=1$, *then* $D(RC_p)^{(2)}\neq 0$.

ii) *If* $p\equiv 3 \pmod 4$ *and* $N_{Q(\sqrt{m})/Q}(\varepsilon_m)=-1$, *then* $D(RC_p)^{(2)}=0$.

iii) *If* $p\equiv 1 \pmod 4$ *and* $N_{Q(\sqrt{m})/Q}(\varepsilon_m)=-1$, *then* $D(RC_p)^{(2)}\neq 0$ *when the type of fundamental units of* $Z[w_p, w_m]$ *is* (a) *or* (b), *and* $D(RC_p)^{(2)}=0$ *when the type of fundamental units of* $Z[w_p, w_m]$ *is* (c) *and* $p\equiv 5 \pmod 8$.

PROOF. Let φ: $U(Z[w_m, \zeta_p+\zeta_p^{-1}])\to U(F_p[\sqrt{m}])$ be the restriction of Ψ to $U(Z[w_m, \zeta_p+\zeta_p^{-1}])$. Then, by force of (3.5), $D(RC_p)\cong\mathrm{Coker}\,\varphi$. There is a commutative diagram with surjective vertical maps

$$\begin{array}{ccc}
U(Z[w_m, \zeta_p+\zeta_p^{-1}]) & \xrightarrow{\quad\varphi\quad} & U(F_p[\sqrt{m}]) \\
{\scriptstyle N_1}\downarrow & & \downarrow{\scriptstyle N_1'} \\
U(Z[w_m])\supseteqq \mathrm{Im}\,N_1 & \xrightarrow{\quad\varphi'\quad} & U(F_p[\sqrt{m}])^{p-1/2} \\
{\scriptstyle N_2}\downarrow & & \downarrow{\scriptstyle N_2'} \\
U(Z)\supseteqq \mathrm{Im}\,N_2 & \xrightarrow{\quad\varphi''\quad} & U(F_p)^{p-1/2},
\end{array}$$

where $N_1=N_{Q(\sqrt{m},\zeta_p+\zeta_p^{-1})/Q(\sqrt{m})}$, $N_2=N_{Q(\sqrt{m})/Q}$, $N_1'(x)=x^{p-1/2}$, $N_2'=N_{F_p[\sqrt{m}]/F_p}$ and φ' and φ'' are the restrictions of φ to $\mathrm{Im}\,N_1$ and $\mathrm{Im}\,N_2$ respectively. If $N_2(\varepsilon_m)=1$, then $\mathrm{Im}\,N_2\circ N_1=\{1\}$, and so $2\,|\,|\mathrm{Coker}\,\varphi|$. For the case where $N_2(\varepsilon_m)=-1$, $p\equiv 3 \pmod 4$ and $\left(\frac{m}{p}\right)=1$, $\varphi'\circ N_1(\varepsilon_m)=(\bar{1}, \overline{-1})$ or $(\overline{-1}, \bar{1})$ in $U(F_p[\sqrt{m}])\cong U(F_p)\times U(F_p)$. Since $|U(F_p[\sqrt{m}])^{(2)}|=4$, this shows that $(\mathrm{Coker}\,\varphi)^{(2)}=0$. For the case where $N_2(\varepsilon_m)=-1$, $p\equiv 3 \pmod 4$ and $\left(\frac{m}{p}\right)=-1$, $U(F_p[\sqrt{m}])^{(2)}=\langle\varphi(\varepsilon_m)\rangle^{(2)}$, because $\varepsilon_m^{p+1} \equiv -1 \pmod{p}$, and therefore we see that $(\mathrm{Coker}\,\varphi)^{(2)}=0$.

To prove iii), we form the following commutative diagram with surjective vertical maps:

$$\begin{tikzcd}
U(\boldsymbol{Z}[w_m, \zeta_p+\zeta_p^{-1}]) \arrow[r, "\varphi"] \arrow[d, "N_1"'] & U(\boldsymbol{F}_p[\sqrt{m}]) \arrow[d] \\
U(\boldsymbol{Z}[w_m, w_p]) \supseteq \mathrm{Im}\, N_1 \arrow[r] \arrow[d, "N_2"'] & U(\boldsymbol{F}_p[\sqrt{m}])^{p-1/4} \arrow[d] \\
U(\boldsymbol{Z}[w_{pm}]) \supseteq \mathrm{Im}\, N_2 \arrow[r] \arrow[d, "N_3"'] & U(\boldsymbol{F}_p)^{p-1/4} \arrow[d] \\
U(\boldsymbol{Z}) \supseteq \mathrm{Im}\, N_3 \arrow[r, "\varphi'"] & U(\boldsymbol{F}_p)^{p-1/2},
\end{tikzcd}$$

where N_i, $i=1, 2$ and 3, are the norm maps and the other maps are natural. For the case of type (a), $\mathrm{Im}\, N_2 \subseteq \langle -1, \varepsilon_{pm}^2\rangle$, and for the case of type (b), $\mathrm{Im}\, N_2 \subseteq \langle -1, \varepsilon_{pm}\rangle$ and $N_3(\varepsilon_{pm})=1$. Hence, for either case, $\mathrm{Im}\,\varphi'\circ N_3\circ N_2\circ N_1=\{1\}$, and so $2\,|\,|\mathrm{Coker}\,\varphi|$. If $p\equiv 5 \pmod 8$, $U(\boldsymbol{F}_p[\sqrt{m}])^{(2)}=(U(\boldsymbol{F}_p[\sqrt{m}])^{p-1/4})^{(2)}$. Now consider the case of type (c). If $\left(\frac{m}{p}\right)=1$, $U(\boldsymbol{F}_p[\sqrt{m}])^{p-1/4}=\boldsymbol{Z}/4\boldsymbol{Z}\oplus\boldsymbol{Z}/4\boldsymbol{Z}$. Since $\varphi'\circ N_3\circ N_2\circ N_1(\sqrt{\varepsilon_p\varepsilon_m\varepsilon_{pm}})=\varphi'\circ N_3\circ N_2(\sqrt{\varepsilon_p\varepsilon_m\varepsilon_{pm}}^{p-1/4})=\varphi'\circ N_3(\pm\varepsilon_{pm}{}^{p-1/4})=\varphi'(-1)=\overline{-1}$, $\varphi(\sqrt{\varepsilon_p\varepsilon_m\varepsilon_{pm}}^{p-1/4})$ is of type $(\overline{\pm 1}, c)$ or $(c, \overline{\pm 1})$ in $U(\boldsymbol{F}_p)\times U(\boldsymbol{F}_p)$, where c is of order 4 in $U(\boldsymbol{F}_p)$. Hence $(\mathrm{Coker}\,\varphi)^{(2)}=0$, because $\mathrm{Im}\,\varphi\supseteq\{(a, a)\,|\,a\in U(\boldsymbol{F}_p)\}$. If $\left(\frac{m}{p}\right)=-1$, $U(\boldsymbol{F}_p[\sqrt{m}])^{p-1/4}\cong\boldsymbol{Z}/4(p+1)\boldsymbol{Z}$. We see that the order of $(\sqrt{\varepsilon_p\varepsilon_m\varepsilon_{pm}}^{p+1/2})$ is 8, because $\varepsilon_m^{p+1}\equiv -1 \pmod{p}$. This shows that $(\mathrm{Coker}\,\varphi)^{(2)}=0$, and thus the proof is completed.

REMARK 3.8. For the case where the type of fundamental units of $\boldsymbol{Z}[w_p, w_m]$ is (c) and $p\equiv 1 \pmod 8$, we do not know whether $D(RC_p)^{(2)}=0$ or not.

PROPOSITION 3.9. *Suppose that* $p\,|\,m$ *and write* $m=np^*$. *Then*

i) $D(RC_p)\cong T(RC_p)\oplus D(RC_p/(\Sigma_p))$.

ii) $T(RC_p)\cong\begin{cases}\boldsymbol{Z}/p\boldsymbol{Z} & \text{if } m<-3 \text{ or } m>0 \text{ and } p\,|\,b\\ 0 & \text{otherwise.}\end{cases}$

iii) $D(RC_p/(\Sigma_p))^{(p)}$ *is an elementary p-group of rank*$\leqq(p-3)/2$. *Especially, if* $n=1$, *then* $D(RC_p/(\Sigma_p))$ *is an elementary p-group of rank*$\leqq\max(0, (p-7)/2)$.

PROOF. ii) There is a commutative diagram

$$\begin{tikzcd} U(R[\bar{\sigma}]) \arrow[r, "\phi"] \arrow[d, "N"'] & U(F_p[\sqrt{m}]) \cong Z/p(p-1)Z \arrow[r] \arrow[d, "N'"] & T(RC_p) \arrow[r] & 0 \\ U(R) \supseteq \operatorname{Im} N \arrow[r, "\phi'"] & U(F_p[\sqrt{m}])^{p-1} \cong Z/pZ, & & \end{tikzcd}$$

where $N(f(\bar{\sigma}))=\prod_{i=1}^{p-1} f(\bar{\sigma}^i)$ for every $f(\bar{\sigma})\in U(R[\bar{\sigma}])$, $N'(x)=x^{p-1}$ for every $x\in U(F_p[\sqrt{m}])$ and ϕ' is the restriction of ϕ to $\operatorname{Im} N$. Then $\operatorname{Coker}\phi\cong Z/pZ$ or 0, and $\operatorname{Coker}\phi\cong Z/pZ$ if and only if $\operatorname{Coker}\phi'\cong Z/pZ$. If $m>0$, then $\phi'\circ N(\varepsilon_m)=\phi'(\varepsilon_m^{p-1})=\bar{1}$ if and only if $p|b$. If $m<-3$, then $U(R)=\{\pm 1\}$, and hence $\operatorname{Coker}\phi'\cong Z/pZ$. For $m=-3$, we can compute directly that ϕ is surjective.

i) The conclusion follows from ii) and (2.2 i).

iii) Let $n\neq 1$. Then we can write as

$$D(RC_p/(\Sigma_p))^{(p)}\cong\frac{1+p\bar{S}_p}{U^1(\bar{S})(1+pS_p)},$$

where $S=Z[w_{np^*}, \zeta_p]$, $\bar{S}=Z[w_n, \zeta_p]$, p is the unique prime ideal over p in S and $\bar{p}=p\bar{S}$. Then the conclusion follows from (2.2 i) and the fact that $\left|\frac{1+\bar{p}\bar{S}_p}{1+pS_p}\right|=p^{p-3/2}$. Next assume that $n=1$. By force of (2.3), we may assume that $p\geqq 7$. Then

$$D(RC_p/(\Sigma_p))\cong\frac{(1+\pi\mathcal{O}_p)\times(1+\pi\mathcal{O}_p)}{\{U^1(\mathcal{O})\times U^1(\mathcal{O})\}\,\{U(R_pC_p/(\Sigma_p))\cap((1+\pi\mathcal{O}_p)\times(1+\pi\mathcal{O}_p))\}},$$

where $\pi=\zeta_p-1$ and $\mathcal{O}=Z[\zeta_p]$. The map $U(R_pC_p/(\Sigma_p))\cap((1+\pi\mathcal{O}_p)\times(1+\pi\mathcal{O}_p))\hookrightarrow(1+\pi\mathcal{O}_p)\times(1+\pi\mathcal{O}_p)\xrightarrow{\varphi}(1+\pi\mathcal{O}_p)$ is surjective where $\varphi(x, y)=x$. Since $U^1(\mathcal{O})$ contains $1+\pi$ and $1+\pi^2-\pi^3\zeta_p^{-1}$, each element of $D(RC_p/(\Sigma_p))$ has a representative of the form $(1, 1+\pi^3x)\in(1+\pi\mathcal{O}_p)\times(1+\pi\mathcal{O}_p)$, $x\in\mathcal{O}_p$. The conclusion follows from this, because $u(R_pC_p/(\Sigma_p))\supseteq\{1\}\times(1+\pi^{p-1/2}\mathcal{O}_p)$.

REMARK 3.10. If $p=5$ and $n>1$, then $D(RC_5/(\Sigma_5))^{(5)}\cong Z/5Z$. In fact, since $U(\bar{S})=\langle\zeta_5\rangle U(Z[w_n, w_5])$, it is easy to see that $U^1(\bar{S})=U^1(S)\subseteqq 1+pS_p$. On the other hand, there are examples of n for which $D(RC_5/(\Sigma_5))^{(5)}=0$, e.g. $n=-1$, -3, -7 or -11.

§ 4.

In this section, we shall determine completely the structure of $D(RC_3)$.

LEMMA 4.1. *Let $m>0$ and $3\nmid m$. Put $\varepsilon_m=(a+b\sqrt{m})/2$. Then*

i) $3 \nmid a$ *or* $3 \nmid b$.

ii) *If* $m \equiv 1 \pmod 3$, *then* $3 | ab$.

iii) $N_{k/Q}(\varepsilon_m)=1$ *if and only if* $m \equiv 1 \pmod 3$ *and* $3 \nmid a$ *or* $m \equiv -1 \pmod 3$ *and* $3 | ab$.

PROOF. The results follow from the facts that $N_{k/Q}(\varepsilon_m) \equiv a^2 - b^2 \pmod 3$ if $m \equiv 1 \pmod 3$ and that $N_{k/Q}(\varepsilon_m) \equiv a^2 + b^2 \pmod 3$ if $m \equiv -1 \pmod 3$.

We can refine (3.4) and (3.7) as follows.

THEOREM 4.2. *Suppose that* $3 \nmid m$. *Then* $(\sqrt{m}, \Sigma_3)$ *(resp.* $(-1+\sqrt{m}, \Sigma_3)$*) is a Representative of a generator of* $D(RC_3)$ *if* $(m/p)=1$ *(resp.* $(m/p)=-1$*), and*

$D(RC_3)$	$m<0$	$m>0$
0	$m \equiv 1 \pmod 3$ *and* (A), *or* $m=-1$	$N_{k/Q}(\varepsilon_m)=-1$
$\boldsymbol{Z}/2\boldsymbol{Z}$	$m \equiv 1 \pmod 3$ *and not* (A), *or* $m \equiv -1 \pmod 3$, $m \neq -1$ *and* (A)	$m \equiv 1 \pmod 3$ *and* $3	b$, *or* $m \equiv -1 \pmod 3$, $3	a$
$\boldsymbol{Z}/4\boldsymbol{Z}$	$m \equiv -1 \pmod 3$ *and not* (A)	$m \equiv -1 \pmod 3$ *and* $3	b$

where, for $m<0$, (A) *means the property that* $\sqrt{-\varepsilon_{-3m}} \in U(\boldsymbol{Z}[w_m, \zeta_3])$.

PROOF. For the case $m<0$, the result follows from (3.4), since the condition (A) is equivalent to the condition $Q_K=2$, where $K=Q(\zeta_3, \sqrt{m})$. For the case $m>0$, we see that $D(RC_3)=U(\boldsymbol{F}_3[\sqrt{m}])/\varphi(U(\boldsymbol{Z}[w_m]))$ by (3.6), and so $D(RC_3)$ is a 2-qroup. Therefore the result follows from (3.7 ii) and (4.1).

For the case $m=-3n$, we have, by (3.9) and (2.2),

$$D(RC_3) \cong T(RC_3) \oplus D(RC_3/(\Sigma_3)) \text{ and}$$

$$D(RC_3/(\Sigma_3)) \cong \begin{cases} 0 & \text{if } n=1 \\ D(R'C_3) & \text{if } n \neq 1, \text{ where } R'=\boldsymbol{Z}[w_m]. \end{cases}$$

Hence we have

THEOREM 4.3. *Suppose that* $3 | m$ *and wrie* $m=-3n$. *Then*

$D(RC_3)$	$n<0$	$n>0$
0	$n\equiv 1 \pmod 3$, (A) *and* $3\nmid d$, *or* $n=-1$	$n=1$
$Z/2Z$	$n\equiv 1 \pmod 3$, *not* (A) *and* $3\nmid d$, *or* $n\equiv -1 \pmod 3$, $n\neq -1$, (A) *and* $3\nmid d$	
$Z/3Z$	$n\equiv 1 \pmod 3$, (A) *and* $3\mid d$	$n\neq 1$ *and* $N(\varepsilon_n)=-1$
$Z/4Z$	$n\equiv -1 \pmod 3$, *not* (A) *and* $3\mid d$	
$Z/2Z\oplus Z/3Z$	$n\equiv 1 \pmod 3$, *not* (A) *and* $3\mid d$, *or* $n\equiv -1 \pmod 3$, $n\neq -1$, *not* (A) *and* $3\mid d$	$n\equiv 1 \pmod 3$, $n\neq 1$ *and* $3\mid b$, *or* $n\equiv -1 \pmod 3$, *and* $3\mid a$
$Z/3Z\oplus Z/4Z$	$n\equiv -1 \pmod 3$, *not* (A) *and* $3\mid d$	$n\equiv -1 \pmod 3$, $3\mid b$

where $\varepsilon_n=(a+b\sqrt{n})/2$ *if* $n>1$, $\varepsilon_m=(c+d\sqrt{m})/2$ *if* $m>0$, (A) *means the property that* $\sqrt{-\varepsilon_m}\in U(Z[w_n, \zeta_3])$ *if* $m>0$, *and* $N=N_{Q(\sqrt{n})/Q}$.

Next we want to know representatives of generators of $D(RC_3)$ in the case of $3\mid m$. Since $T(RC_3)$ is generated by the class of $(1+\sqrt{m}, \Sigma_3)$, we have only to consider $D(RC_3/(\Sigma_3))$. Write $m=-3n$ assume that $n\neq\pm 1$. Let $R=Z[w_{-3n}]$, $S=R[\zeta_3]$ and $\bar{S}=Z[w_n, \zeta_3]$. Then we see that $\bar{S}$ is the integral closure of S. Put $p=(\sqrt{-3}, \sqrt{-3n})$ (resp. $(\sqrt{-3}, 1+(1+\sqrt{-3n})/2)$) if $n\not\equiv 1 \pmod 4$ (resp. $n\equiv 1 \pmod 4$). Then we see that p is a unique prime ideal of S which contains $p^2=(\sqrt{-3})p$ and $p\bar{S}=(\sqrt{-3})$. First we note

LEMMA 4.4. *An invertible ideal C of S such that $C\bar{S}$ is principal in $\bar{S}$ is isomorphic to some p-primary invertible ideal of S not contained in p^2.*

PROOF. Let C' be an invertible ideal of S such that $C'\cong C^{-1}$. Since p is a unique non-invertible prime ideal of S, we have $S[1/3]=\bar{S}[1/3]$. Hence, there is $c'\in C'$ such that $C'S[1/3]=(c')$ in $S[1/3]$, and so there is a p-primary invertible ideal g of S such that $(c')=C'g$ in S. Since $p^2=(\sqrt{-3})p$, g is isomorphic to a p-primary invertible not contained in p^2. Since $C\cong C'^{-1}\cong g$, this completes the proof.

Put $a=(3, \sqrt{-3n})$ (resp. $(3, 1+(1+\sqrt{-3n})/2)$) if $n\not\equiv 1 \pmod 4$ (resp. $n\equiv 1 \pmod 4$). Then $a\bar{S}=(\sqrt{-3})$ and $a^2=(3)$.

LEMMA 4.5. *The following statements are equivalent:*

i) *$\mathfrak{a}$ is non-principal in S.*

ii) *In the case where $n<0$, $U(\boldsymbol{Z}[w_n, \zeta_3])=\langle -1, \zeta_3, \varepsilon_{-3n}\rangle$, and in the case where $n>0$, $\varepsilon_n=(a+b\sqrt{n})/2$, $3\nmid a$, $3|b$.*

PROOF. Let $n\not\equiv 1 \pmod 4$. If $\mathfrak{a}$ is principal, then we can write as $\mathfrak{a}=(3x+y\sqrt{-3n})$ for some $x, y\in \boldsymbol{Z}[\zeta_3]$. Further we see that $\sqrt{-3}\nmid y$ and $(x, y)=(1)$. Since $3\in\mathfrak{a}$,

$$(v'+z\sqrt{-3n})(3x+y\sqrt{-3n})=3 \qquad \text{for some } v', z\in \boldsymbol{Z}[\zeta_3].$$

Hence we have that $3xz+yv'=0$, and so $v'=3v$ for some $v\in\boldsymbol{Z}[\zeta_3]$. Then the equality $xz+yz=0$ implies that $v=ux$ and $z=-uy$ for some $u\in\boldsymbol{Z}[\zeta_3]$. Thus $u(3x-y\sqrt{-3n})(3x+y\sqrt{-3n})=3$, and so $u(x\sqrt{-3}+y\sqrt{n})(x\sqrt{-3}-y\sqrt{n})=-1$ in $\bar{S}$. Hence there is a unit of type $x\sqrt{-3}+y\sqrt{n}$ $(x, y\in\boldsymbol{Z}[\zeta_3])$ in $\bar{S}$. Conversely, if there is a unit in $\bar{S}$ of the above type, we see that $\mathfrak{a}=(3x+y\sqrt{-3n})$. If $n<0$, then there is a unit of the above type when and only when the unit index of $Q(\zeta_3, w_n)$ is 2, i.e. $U(\bar{S})=\langle -1, \zeta_3, \sqrt{-\varepsilon_{-3n}}\rangle$. If $n>0$, then $U(\bar{S})=\langle -1, \zeta_3, \varepsilon_n\rangle$ by (3.6), $\varepsilon_n=a+b\sqrt{n}$, and there is a unit in $\bar{S}$ of the above when and only when $3|a$ and $3\nmid b$. We can similarly prove the assertion for the case where $n\equiv 1 \pmod 4$.

LEMMA 4.6. *Assume that $n\equiv -1 \pmod 3$. Put $\mathfrak{g}=(3, \sqrt{-3n}+\sqrt{-3})$ (resp. $(3, \sqrt{-3}+(3+\sqrt{-3n}))$) if $n\not\equiv 1 \pmod 4$ (resp. $n\equiv 1 \pmod 4$). Then $\mathfrak{g}$ is a $\mathfrak{p}$-primary invertible ideal in S such that $\mathfrak{g}^2=(\sqrt{-3})\mathfrak{a}$ and $\mathfrak{g}\nsubseteq\mathfrak{p}^2$. Further, $\mathfrak{g}$ is principal in S if and only if $n>0$ and $3\nmid ab$, where $\varepsilon_n=(a+b\sqrt{n})/2$.*

PROOF. Let $n\not\equiv 1 \pmod 4$. The first statement is obvious, so we have only to show the second one. If $\mathfrak{g}$ is principal in S, then $\mathfrak{g}=(3(x+y\sqrt{-3n})+(z+v\sqrt{-3n})(\sqrt{-3}+\sqrt{-3n}))$ for some $x, y, z, v\in\boldsymbol{Z}[\zeta_3]$, and so $\mathfrak{g}=(s\sqrt{-3}+t\sqrt{-3n})$, where $s=-\sqrt{-3}x+z+\sqrt{-3}nv$ and $t=3y+z+\sqrt{-3}v$. Since $\mathfrak{g}\nsubseteq\mathfrak{p}^2$, we have $\sqrt{-3}\nmid z$, and hence $\sqrt{-3}\nmid st$ and $(s, t)=(1)$. Since $3\in\mathfrak{g}$, $3=u(s\sqrt{-3}+t\sqrt{-3n})(s\sqrt{-3}-t\sqrt{-3n})$ for some $u\in\boldsymbol{Z}[\zeta_3]$. Hence $u(s+t\sqrt{n})x(s-t\sqrt{n})=-1$ in $\bar{S}$ and so

$$(*) \qquad s+t\sqrt{n}\in U(\boldsymbol{Z}[\sqrt{n}, \zeta_3]) \qquad \text{where } s, t\in\boldsymbol{Z}[\zeta_3] \text{ and } \sqrt{-3}\nmid st.$$

If $n<0$, then $U(\boldsymbol{Z}[\sqrt{n}, \zeta_3])=\langle -1, \zeta_3, \varepsilon_{-3n}\rangle$ or $\langle -1, \zeta_3, \sqrt{-\varepsilon_{-3n}}\rangle$, where $\sqrt{-\varepsilon_{-3n}}=x\sqrt{-3}+y\sqrt{n}$ for some $x, y\neq 0$. Therefore (*) is impossible, and hence $\mathfrak{g}$ is non-principal. If $n>0$, then $U(\boldsymbol{Z}[\sqrt{n}, \zeta_3])=\langle -1, \zeta_3, \varepsilon_n\rangle$ where $\varepsilon_n=a+b\sqrt{n}$. This shows that (*) is possible if and only if $3\nmid ab$. We can similarly prove the assertion for the case where $n\equiv 1 \pmod 4$.

Combining (4.3), (4.5) and (4.6), we have

THEOREM 4.7. *Suppose that* $3|m$ *and* $m\neq\pm 3$. *Let*

$$a=\begin{cases}(3,\sqrt{m}) & \text{if } m\not\equiv 1 \pmod 4\\ \left(3,\ 1+\dfrac{1+\sqrt{m}}{2}\right) & \text{if } m\equiv 1 \pmod 4\,,\end{cases}$$

and

$$g=\begin{cases}(3,\sqrt{-3}+\sqrt{m}) & \text{if } m\not\equiv 1 \pmod 4\\ \left(3,\ \sqrt{-3}+\dfrac{3+\sqrt{m}}{2}\right) & \text{if } m\equiv 1 \pmod 4\,.\end{cases}$$

Then $D(RC_3/(\Sigma_3))$ *is generated by the class of* a (*resp.* g) *if* $m/3\equiv -1 \pmod 3$ (*resp.* $m/3\equiv 1 \pmod 3$).

REMARK 4.8. We can also determine the structure of $D(RC_5)$ for the case that k is a real quadratic field. Let $R=\boldsymbol{Z}[w_m]$, $S=\boldsymbol{Z}[w_m, w_5]$, where $5\nmid m>0$, and $\varepsilon_m=(a+b\sqrt{m}/2)$. Then a system of fundamental units of S is given as one of the following:

(*a*) $\varepsilon_5,\ \varepsilon_m,\ \varepsilon_{5m}$,

(*b*) $\varepsilon_5,\ \varepsilon_m,\ \sqrt{\varepsilon_{5m}}$ (in this case $N(\varepsilon_{5m})=1$ and $\left(\frac{m}{5}\right)=1$),

(*c*) $\varepsilon_5,\ \varepsilon_m,\ \sqrt{\varepsilon_5\varepsilon_m\varepsilon_{5m}}$ (in this case $N(\varepsilon_m)=N(\varepsilon_{5m})=-1$, or $N(\varepsilon_m)=1$, $\left(\frac{m}{5}\right)=-1$ and $5\nmid b$), or

(*d*) $\varepsilon_5,\ \varepsilon_m,\ \sqrt{\varepsilon_m\varepsilon_{5m}}$ (in this case $N(\varepsilon_m)=N(\varepsilon_{5m})=1$, $\left(\frac{m}{5}\right)=-1$ and $5\nmid b$),

where, for a sequare-free positive integer d, $N(\varepsilon_d)=N_{Q(\sqrt{d})/Q}(\varepsilon_d)$.

We have a following table:

$D(RC_5)$	$\left(\frac{m}{5}\right)=1$	$\left(\frac{m}{5}\right)=-1$
0	$N(\varepsilon_m)=-1$ *and* (*c*)	$N(\varepsilon_m)=-1$, (*c*) *and* $5\nmid b$
$\boldsymbol{Z}/2\boldsymbol{Z}$	(*a*) *and* $5\nmid b$, *or* (*b*)	(*a*) *and* $5\nmid b$, *or* $N(\varepsilon_m)=1$ *and* (*c*) *or* (*d*)
$\boldsymbol{Z}/3\boldsymbol{Z}$		$N(\varepsilon_m)=-1$, (*c*) *and* $5\mid b$
$\boldsymbol{Z}/4\boldsymbol{Z}$	(*a*) *and* $5\mid b$	
$\boldsymbol{Z}/6\boldsymbol{Z}$		(*a*) *and* $5\mid b$

where (*a*) means that the type of fundamental units of S is (*a*).

Further, let $R'=\boldsymbol{Z}[w_{5m}]$ and $\varepsilon_{5m}=(c+d\sqrt{5m})/2$. Then

$$D(R'C_5)\cong D(RC_5)\oplus \boldsymbol{Z}/5\boldsymbol{Z}\oplus T(R'C_5)$$

and

$$T(R'C_5)\cong\begin{cases} 0 & \text{if } 5\nmid d \\ \boldsymbol{Z}/5\boldsymbol{Z} & \text{if } 5\mid d\,. \end{cases}$$

References

]1] Endo, S. and Miyata, T., Quasi-permutation modules over finite groups, II, J. Math. Soc. Japan **26** (1974), 698–713.

[2] Frohlich, A., On the class group of integral group rings of finite Abelian groups, Mathematika **16** (1969), 143-152.

[3] Hasse, H., Über die Klassenzahl Abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.

[4] Kervaire, M. A. and Murthy, M. P., On the projective class group of cyclic groups of prime power order, Comment. Math. Helvetici **52** (1977), 415-452.

[5] Kuroda, S., Über den Dirichletschen Körper, J. Fac. Soc. Imp. Univ. Tokyo **3** (1943), 383-406.

[6] Mann, H. B., On integral basis, Proc. Amer. Math. Soc. **9** (1958), 167-172.

[7] Miyata, T., A normal integral basis theorem for dihedral groups, Tohoku Math. J. **32** (1980), 49-62.

[8] Ullom, S. V., A survey of class groups of integral group rings, Algebraic Number Fields (Proc. Durham Symposium), Academic Press, London, 1977.

University of Tsukuba
Present Adress
Department of Mathematics
Faculty of Science
Shinshu University
Matsumoto, 390 Japan.