CLEAN GROUP RINGS OVER LOCALIZATIONS OF RINGS OF INTEGERS

YUANLIN LI AND QINGHAI ZHONG

Abstract. A ring $R$ is said to be clean if each element of $R$ can be written as the sum of a unit and an idempotent. In a recent article (J. Algebra, 405 (2014), 168-178), Immormino and McGoven characterized when the group ring $\mathbb{Z}((p))[C_n]$ is clean, where $\mathbb{Z}((p))$ is the localization of the integers at the prime $p$. In this paper, we consider a more general setting. Let $K$ be an algebraic number field, $\mathcal{O}_K$ be its ring of integers, and $R$ be a local ring between $\mathcal{O}_K$ and $K$. We investigate when $R[G]$ is clean, where $G$ is a finite abelian group, and obtain a complete characterization for such a group ring to be clean for the case when $K = \mathbb{Q}(\zeta_n)$ is a cyclotomic field or $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field.

1. Introduction

All rings considered here are associative with identity $1 \neq 0$. An element of a ring $R$ is called clean if it is the sum of a unit and an idempotent, and a ring $R$ is called clean if each element of $R$ is clean. Clean rings were introduced and related to exchange rings by Nicholson in 1977 [12] and the study of clean rings has attracted a great deal of attention in recent 2 decades. For some fundamental properties about clean rings as well as a nice history of clean rings we suggest the interested reader to check the article [10].

Recall that for a ring $R$ with identity and a multiplicative group $G$, the group ring of $G$ over $R$ is the ring $R[G]$ of all formal sums

$$\alpha = \sum_{g \in G} \alpha_g g,$$

where $\alpha_g \in R$ and the support of $\alpha$, $\text{supp}(\alpha) = \{g \in G \mid \alpha_g \neq 0\}$, is finite. Addition is defined componentwise and multiplication is defined by the following way: for $\alpha, \beta \in R[G]$,

$$\alpha \beta = \left( \sum_{g \in G} \alpha_g g \right) \left( \sum_{h \in G} \beta_h h \right) = \sum_{g, h \in G} \alpha_g \beta_h (gh).$$

For more information on the group ring, we refer [11] as a reference. We let $C_n$ denote the cyclic group of order $n$. Since a homomorphic image of a clean ring is a clean ring, it follows that it is necessary that $R$ is clean whenever $R[G]$ is.

In this paper, we investigate the question of when a commutative group ring $R[G]$ over a local ring $R$ is clean. We also study when such a group ring is $\ast$-clean (see next section for the definition of $\ast$-clean rings). Let $\mathbb{Z}((p))$ denote the localization of the ring $\mathbb{Z}$ of integers at the prime $p$. In [3], the authors proved that $\mathbb{Z}((p))[C_3]$ is not clean. It then follows that since $\mathbb{Z}((p))$ is a clean ring (as it is local) that $R$ being a commutative clean ring is not sufficient for $R[G]$ to be a clean ring. In a recent paper [4], it was shown that $\mathbb{Z}((p))[C_3]$ is clean if and only if $p \equiv 1 \pmod{3}$. More generally, the authors gave a complete characterization of when $\mathbb{Z}((p))[C_n]$ is clean. Note that $\mathbb{Z}((p))$ is a local ring between $\mathbb{Z}$ and $\mathbb{Q}$. In this paper, we consider a more general setting. Let $(\bar{R}, \mathfrak{m})$ be a commutative local ring and we denote $\bar{R} = R/\mathfrak{m}$. Let

2010 Mathematics Subject Classification. Primary: 16S34 Secondary: 11R11, 11R18.

Key words and phrases. Clean ring; Group ring; Ring of algebraic integers; Primitive root of unity; Cyclotomic field.

This research was supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada and by the Austrian Science Fund FWF, Project Number P 28864-N35.
Let $K$ be an algebraic number field, $\mathcal{O}_K$ be its ring of integers, and $R$ be a localization of $\mathcal{O}_K$ at some prime ideal $p$. We investigate when $R[G]$ is clean, where $G$ is a finite abelian group, and provide a complete characterization for such a group ring to be clean for the case when $K = \mathbb{Q}(\sqrt{d})$ is a cyclotomic field or $K = \mathbb{Q}(\sqrt{-1})$ is a quadratic field. Our main results are as follows.

**Theorem 1.1.** Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field for some $n \in \mathbb{N}$, $\mathcal{O} = \mathbb{Z}[\zeta_n]$ its rings of integers, $p \subset \mathcal{O}$ a nonzero prime ideal, and $G$ a finite abelian group. Let $p$ be the prime with $p\mathbb{Z} = p \cap \mathbb{Z}$, let $n_0$ be the maximal positive divisor of $n$ with $p \nmid n_0$, let $n_1$ be the maximal divisor of $\exp(G)$ with $p \nmid n_1$ and $\gcd(n_1, n_0) = 1$, and let $m'$ be the maximal divisor of $\frac{\varphi(n)}{\gcd(\varphi(n), n_0)}$ with $p \nmid m'$.

Then the group ring $\mathcal{O}_p[G]$ is clean if and only if one of the following holds

1. $\gcd(\varphi(n), n_0) = 1$ and $\gcd(\varphi(n), n_1) = 1$.
2. $\gcd(\varphi(n), n_0) = 1$ and $\gcd(\varphi(n), n_1) = 1$.
3. $\gcd(\varphi(n), n_0) = 1$ and $\gcd(\varphi(n), n_1) = 1$.

Note that if $n = 1$ (i.e. $K = \mathbb{Q}$), then $n_0 = 1$ and $m' = 1$. Therefore, Theorem 1.1 implies the following corollary which is exactly the main result of [7, Theorem 3.3].

**Corollary 1.2.** Let $G$ be a finite abelian group, let $p$ be a prime number, and let $n$ be the maximal divisor of $\exp(G)$ with $p \nmid n$. Then $\mathbb{Z}_p[G]$ is clean if and only if $\gcd(n, p) = \varphi(n)/2$ (i.e. $p$ is a primitive root of $n$).

**Theorem 1.3.** Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field for some non-zero square-free integer $d \neq 1$, $\mathcal{O}$ its rings of integers, $p \subset \mathcal{O}$ a nonzero prime ideal, and $G$ a finite abelian group. Let $\Delta$ be the discriminant of $K$ and let $n$ be the maximal positive divisor of $\exp(G)$ with $p \nmid n$. Then

1. if $\Delta \nmid n$, then $\mathcal{O}_p[G]$ is clean if and only if one of the following holds
   (a) $p = 2$ is a primitive root of unity of $n$ and $\Delta \equiv 5 \pmod{8}$;
   (b) $p \neq 2$ is a primitive root of unity of $n$ and $\left(\frac{\Delta}{p}\right) = 1$ or $0$, where $\left(\frac{\Delta}{p}\right)$ is the Legendre symbol.
2. if $\Delta | n$ and $d \equiv 2, 3 \pmod{4}$, then $\mathcal{O}_p[G]$ is clean if and only if $\gcd(d, n) = 1$ and $\gcd(n, p) = \varphi(n)/2$.
3. if $\Delta | n$ and $d \equiv 1 \pmod{4}$, then $\mathcal{O}_p[G]$ is clean if and only if one of the following holds
   (a) $\gcd(d, n) = 1$ and $\gcd(n, p) = \varphi(n)/2$.
   (b) $\gcd(d, n) = 1$ and $\gcd(n, p) = \varphi(n)/2$.

In Section 2, we collect some necessary knowledge of the structure of the group of unites $(\mathbb{Z}/m\mathbb{Z})^\times$ and field extension. Furthermore, we give some general characterization theorems for clean and $*$-clean group rings. In Section 3, we deal with group rings over local subrings of cyclotomic fields and provide a proof of Theorem 1.1. In Section 4, we consider group rings over local subrings of quadratic fields and give a proof of Theorem 1.3.

2. Preliminaries

For a finite abelian group $G$, we denote by $\exp(G)$ the exponent of $G$. We denote by $\mathbb{N}$ the set of all positive integers and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $n \in \mathbb{N}$, we denote by $\varphi(n)$ the Euler function. Let $n \in \mathbb{N}$ and let $n = p_1^{k_1} \ldots p_s^{k_s}$ be the prime factorization, where $s, k_1, \ldots, k_s \in \mathbb{N}$ and $p_1, \ldots, p_s$ are pair-wise distinct primes. It is well-known that

$$\varphi(n) = \prod_{i=1}^s \varphi(p_i^{k_i}) = \prod_{i=1}^s p_i^{k_i-1}(p_i - 1)$$

and $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_s^{k_s}\mathbb{Z})^\times$. 

Furthermore,
\[ (\mathbb{Z}/p^n\mathbb{Z})^\times \cong C_{p^{n-1}(p-1)} \] where \( p \geq 3, \)
\[ (\mathbb{Z}/2^\ell\mathbb{Z})^\times = (-1) \times (5) \cong C_2 \oplus C_{2^{\ell-2}} \] where \( \ell \geq 3, \)
and
\[ (\mathbb{Z}/4\mathbb{Z})^\times \cong C_2. \]

For every \( m \in \mathbb{N} \) with \( \gcd(m, n) = 1 \), we denote by \( \text{ord}_n m = \text{ord}_{\mathbb{Z}/(mn)\mathbb{Z}} m \) the multiplicative order of \( m \) modulo \( n \). If \( \text{ord}_n m = \varphi(n) \), we say \( m \) is a primitive root of \( n \) and \( n \) has a primitive root if and only if \( n = 2, 4, q^\ell \), or \( 2q^\ell \), where \( q \) is an odd prime and \( \ell \in \mathbb{N} \). Let \( n_1 \in \mathbb{N} \) be another integer with \( \gcd(n_1, m) = 1 \). Then
\[ \text{ord}_n m \leq \text{ord}_{n_1} m \leq n_1 \text{ord}_n m, \]
and \( \text{lcm}(\text{ord}_n m, \text{ord}_{n_1} m) = \text{lcm}(\text{ord}_{n_1} m, m) \).

Let \( \zeta_n \) be the \( n \)th primitive root of unity over \( \mathbb{Q} \). Then \( [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) \). Let \( m \) be another positive integer. Then
\[ \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\gcd(n,m)}) \]
and \( \mathbb{Q}(\zeta_n)(\zeta_m) = \mathbb{Q}(\zeta_{\text{lcm}(n,m)}) \).

Let \((R, m)\) be a commutative local ring and we denote \( \overline{R} = R/m \). Then \( \overline{R} \) is a field and we denote by \( \text{char} \overline{R} \) the characteristic of \( \overline{R} \). For any polynomial \( f(x) = a_n x^n + \ldots + a_0 \in \overline{R}[x] \), we denote \( f(\overline{x}) = a_n x^n + \ldots + a_0 \in \overline{R}[x] \), where \( \overline{a_i} = a_i + m \) for all \( i \in \{0, \ldots, n\} \).

**Theorem 2.1.** Let \((R, m)\) be a commutative noetherian local ring with \( \text{char} \overline{R} = p \geq 0 \), let \( G \) be a finite abelian group, and let \( n \) be the maximal divisor of \( \exp(G) \) with \( p \nmid n \). Then \( R[G] \) is clean if and only if each monic factor of \( x^n - 1 \) in \( 

\begin{array}{l}
\text{Proof. This follows from [7] Proposition 2.1} \quad \text{and [13] Theorem 5.8].}
\end{array}
\]

Let \( K \) be an algebraic number field, \( \mathcal{O} \) its rings of integers, and \( p \subset \mathcal{O} \) a nonzero prime ideal. Then there exists a prime \( p \) such that \( p \cap \mathbb{Z} = p\mathbb{Z} \) and the localization \( \mathcal{O}_p \) is a discrete valuation ring, which implies that \( \mathcal{O}_p[x] \) is a UFD (uniquely factorization domain). Furthermore, the norm \( N(p) = |\mathcal{O}/p| = |\mathcal{O}_p/x| \) is a prime power of \( p \).

Let \( \mathbb{F}_q \) be a finite field, where \( q \) is a power of some prime \( p \) and let \( \overline{\mathbb{F}_q} \) be the \( n \)th primitive root of unity over \( \mathbb{F}_p \) with \( \gcd(n, q) = 1 \). Then \( \overline{\mathbb{F}_q}(\zeta_n) : \mathbb{F}_q = \text{ord}_n q \). Let \( F \) be an arbitrary field and let \( f(x) \) be a polynomial of \( F[x] \). If \( \alpha \) is a root of \( f(x) \), then \( [F(\alpha) : F] = \deg(f(x)) \) if and only if \( f(x) \) is irreducible in \( F[x] \).

**Theorem 2.2.** Let \( K \) be an algebraic number field, \( \mathcal{O} \) its rings of integers, \( p \subset \mathcal{O} \) a nonzero prime ideal, and \( G \) a finite abelian group. Then the group ring \( \mathcal{O}_p[G] \) is clean if and only if \([K[\zeta_m] : K] = \text{ord}_m(N(p)) \) for every positive divisor \( m \) of \( \exp(G) \) with \( p \nmid m \), where \( \zeta_m \) is an \( m \)th primitive root of unity over \( \mathbb{Q} \).

**Proof.** Let \( n \) be the maximal divisor of \( \exp(G) \) with \( p \nmid \exp(G) \). Since \( \mathcal{O}_p[x] \) is a UFD, we suppose that \( x^n - 1 = f_1(x) \cdot \ldots \cdot f_s(x) \), where \( s \in \mathbb{N} \) and \( f_1(x), \ldots, f_s(x) \) are monic irreducible polynomials in \( \mathcal{O}_p[x] \). Then the Generalized Gauss’ Primitive Polynomial Lemma implies that \( f_1(x), \ldots, f_s(x) \) are also monic irreducible polynomials in \( K[x] \). For every positive divisor \( m \) of \( n \), let \( \Phi_m(x) \) be the \( m \)th cyclotomic polynomial. Then \( \Phi_m(x) \in \mathbb{Z}[x] \subset \mathcal{O}_p[x] \) and
\[ x^n - 1 = \prod_{1 \leq m < n} \Phi_m(x) = f_1(x) \cdot \ldots \cdot f_s(x). \]

1. Suppose \( \mathcal{O}_p[G] \) is clean. Let \( f(x) \) be a monic irreducible factor of \( x^n - 1 \) in \( \mathcal{O}_p[x] \) and let \( h(x) \) be a monic irreducible factor of \( f(x) \) in \( \mathcal{O}_p[x] \). By Theorem 2.1, there exists a monic irreducible factor
Let $h(x)$ be a factor of $x^n - 1$ in $\mathcal{O}_p[x]$ such that $\overline{h(x)} = h(x)$. If $h(x) \neq f(x)$, it follows by $\mathcal{O}_p[x]$ is a UFD that $f(x)h(x)$ is a monic factor of $x^n - 1$ in $\mathcal{O}_p[x]$ and hence $\overline{h(x)}^2$ is a monic factor of $x^n - 1$ in $\overline{\mathcal{O}_p}[x]$. Since $\text{gcd}(n,p) = 1$, we obtain $x^n - 1 \in \overline{\mathcal{O}_p}[x]$ has no multiple root in any extension of $\overline{\mathcal{O}_p}$, a contradiction. Therefore $h(x) = f(x)$ and hence $\overline{h(x)} = h(x)$ is irreducible in $\overline{\mathcal{O}_p}[x]$.

Let $m$ be a positive divisor of $n$. It follows by $\mathcal{O}_p[x]$ is a UFD that there exists $i \in [1, s]$ such that $f_i(x)$ divides $\Phi_m(x)$ in $\mathcal{O}_p[x]$. Thus every root of $f_i(x)$ is an $m$th primitive root of unity in $K$ and hence $[K(\zeta_m) : K] = \text{deg}(f_i(x)) = \text{deg}(\overline{f_i(x)})$. Since $f_i(x)$ is irreducible in $\overline{\mathcal{O}_p}[x]$ and every root of $\overline{f_i(x)}$ is an $m$th primitive root of unity in $\overline{\mathcal{O}_p}$, we have $\text{deg}(f_i(x)) = [\overline{\mathcal{O}_p}(\zeta_m) : \overline{\mathcal{O}_p}] = \text{ord}_m(N(p))$, where $\zeta_m$ is an $m$th primitive root of unity over $\mathbb{F}_p$. Therefore $[K(\zeta_m) : K] = \text{ord}_m(N(p))$.

2. Conversely, suppose $[K(\zeta_m) : K] = \text{ord}_m(N(p))$ for every divisor $m$ of $n$. Let $i \in [1, s]$. Then $f_i(x)$ is a factor of some $m$th cyclotomic polynomial $\Phi_m(x)$ with $m | n$. Since $f_i(x)$ is irreducible in $K[x]$, we have $\text{deg}(f_i(x)) = [K(\zeta_m) : K]$ and hence

\[
\text{deg}(\overline{f_i(x)}) = \text{deg}(f_i(x)) = [K(\zeta_m) : K] = \text{ord}_m(N(p)) = [\overline{\mathcal{O}_p}(\zeta_m) : \overline{\mathcal{O}_p}] = \overline{\mathcal{O}_p}[x].
\]

Therefore $\overline{f_i(x)}$ is irreducible in $\overline{\mathcal{O}_p}[x]$ and

\[
x^n - 1 = f_1(x) \cdots f_s(x) \in \overline{\mathcal{O}_p}[x].
\]

Let $h(x)$ be a monic factor of $x^n - 1 \in \overline{\mathcal{O}_p}[x]$. Since $\overline{\mathcal{O}_p}[x]$ is a UFD, there exists a subset $I \subset [1, s]$ such that $\overline{h(x)} = \prod_{i \in I} \overline{f_i(x)}$ and hence $\overline{\prod_{i \in I} f_i(x)} = h(x)$. Therefore every monic factor of $x^n - 1 \in \overline{\mathcal{O}_p}[x]$ can be lifted to a monic factor of $x^n - 1 \in \mathcal{O}_p[x]$. It follows from Theorem 2.1 that $\mathcal{O}_p[G]$ is clean. □

A ring $R$ is called a $\ast$-ring if there exists an operation $\ast : R \to R$ such that $(x + y)^\ast = x^\ast + y^\ast$, $(xy)^\ast = x^\ast y^\ast$, and $(x^\ast)^\ast = x$ for all $x, y \in R$. An element $p \in R$ is said to be a projection if $p^2 = p = p^\ast$ and a $\ast$-ring $R$ is said to be a $\ast$-clean ring if every element of $R$ is the sum of a unit and a projection. A commutative $\ast$-ring is $\ast$-clean if and only if it is clean and every idempotent is a projection([8, Theorem 2.2]). Let $G$ be an abelian group. With the classical involution

\[
\ast : R[G] \to R[G], \text{given by }
\]

\[
(\sum a_g g)\ast = \sum a_g g^{-1},
\]

the group ring $R[G]$ is a $\ast$-ring. The question of when a group ring $R[G]$ is $\ast$-clean has been recently studied by several authors and many interesting results were obtained (see, for example, [2, 4, 5, 6, 8, 9], for some recent developments). Next we provide a characterization for $\mathcal{O}_p[G]$ to be $\ast$-clean.

**Theorem 2.3.** Let $K$ be an algebraic number field, $\mathcal{O}$ its rings of integers, $p \in \mathcal{O}$ a nonzero prime ideal with $p \mathbb{Z} = p \cap \mathbb{Z}$, and $G$ a finite abelian group with $p \nmid \exp(G)$. If the group ring $\mathcal{O}_p[G]$ is clean, then $\mathcal{O}_p[G]$ is $\ast$-clean if and only if $K[G]$ is $\ast$-clean.

**Proof.** Let $\mathcal{O}_p[G]$ be clean. Suppose $K[G]$ is $\ast$-clean. Since every idempotent of $\mathcal{O}_p[G]$ is an idempotent of $K[G]$, thus every idempotent of $\mathcal{O}_p[G]$ is a projective. It follows that $\mathcal{O}_p[G]$ is $\ast$-clean.

Suppose $\mathcal{O}_p[G]$ is $\ast$-clean. Let $\mathcal{O}_{K(\exp(G))}/\mathbb{Q}$ be the ring of integers of $K(\exp(G))$ and let $I$ be a prime ideal of $\mathcal{O}_{K(\exp(G))}/\mathbb{Q}$ with $I \cap \mathcal{O} = p$. By [4, The beginning of Section 5] and $p \nmid \exp(G)$, there is a complete family of orthogonal idempotents of $K(\exp(G))|G|$ which lies in $(\mathcal{O}_{K(\exp(G))}/\mathbb{Q})_I[G]$. It follows from [4, Lemma 4.3] that every idempotent of $K[G]$ lies in $(\mathcal{O}_{K(\exp(G))}/\mathbb{Q})_I[G] \cap K[G] = \mathcal{O}_p[G]$. Since every idempotent of $\mathcal{O}_p[G]$ is a projective, we obtain every idempotent of $K[G]$ is a projective. Note that $K[G]$ is clean. Thus $K[G]$ is $\ast$-clean. □
3. Group rings over local subrings of cyclotomic fields

In this section, we investigate when a group ring over a local subring of a cyclotomic field is clean and provide a proof for our main theorem [1.1]. We also characterize when such a group ring is *-clean. We start with the following lemma which we will use without further mention.

**Lemma 3.1.** Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field for some $n \in \mathbb{N}$, $\mathcal{O} = \mathbb{Z}[\zeta_n]$ its rings of integers, and $p \subset \mathcal{O}$ a nonzero prime ideal with $p \cap \mathbb{Z} = p\mathbb{Z}$ for some prime $p$. Suppose $n = p^sn_0$ with $p \nmid n_0$. Then $N(p) = p^{\text{lcm}(n_0)}$.

**Proof.** This follows by [1] VI.1.12 and VI.1.15. □

**Proof of Theorem 1.1.** Let $n_2$ be the maximal divisor of $\exp(G)$ such that $p \nmid n_2$ and let $n_3 = \frac{n_2}{n_1}$. Since

$$m' = \frac{\text{lcm}(n_2, n_0)}{n_0n_1} = \frac{\text{lcm}(n_3, n_0)}{n_0},$$

we have $\text{lcm}(n_3, n_0) = n_0m'$ and $\text{lcm}(n_2, n_0) = n_0m'n_1$.

Let $m$ be a divisor of $n_2$. Then

$$[\mathbb{Q}(\zeta_n)(\zeta_m) : \mathbb{Q}(\zeta_n)] = [\mathbb{Q}(\zeta_{\text{lcm}(n,m)}) : \mathbb{Q}(\zeta_n)] = \frac{\varphi(\text{lcm}(n,m))}{\varphi(n)} = \frac{\varphi(\text{lcm}(n_0,m))}{\varphi(n_0)}$$

and

$$\text{ord}_n N(p) = \text{ord}_m p^{\text{ord}_n p} = \frac{\text{ord}_m p}{\text{gcd}(\text{ord}_m p, \text{ord}_n p)} = \frac{\text{lcm}(\text{ord}_n p, \text{ord}_m p)}{\text{ord}_n p} = \frac{\text{ord}_{\text{lcm}(n_0,m)} p}{\text{ord}_n p}.$$

Therefore by Theorem 2.2 that $R[G]$ is clean if and only if

$$\text{for every divisor } m \text{ of } n_2, \text{ we have } \frac{\varphi(\text{lcm}(n_0,m))}{\varphi(n_0)} = \frac{\text{ord}_{\text{lcm}(n_0,m)} p}{\text{ord}_n p}.$$

1. We first suppose that $R[G]$ is clean. Since $n_1$, $n_3$ and $n_2$ are divisors of $n_2$, we obtain

$$\frac{\varphi(\text{lcm}(n_0, n_1))}{\varphi(n_0)} = \frac{\text{ord}_{\text{lcm}(n_0,n_1)} p}{\text{ord}_n p},$$

$$\frac{\varphi(\text{lcm}(n_0, n_3))}{\varphi(n_0)} = \frac{\text{ord}_{\text{lcm}(n_0,n_3)} p}{\text{ord}_n p},$$

and

$$\frac{\varphi(\text{lcm}(n_0, n_2))}{\varphi(n_0)} = \frac{\text{ord}_{\text{lcm}(n_0,n_2)} p}{\text{ord}_n p}.$$

Since $\gcd(n_1, n_0) = 1$, we obtain

$$\varphi(n_1) = \frac{\varphi(\text{lcm}(n_0, n_1))}{\varphi(n_0)} = \frac{\text{ord}_{\text{lcm}(n_0,n_1)} p}{\text{ord}_n p} = \frac{\text{lcm}(\text{ord}_n p, \text{ord}_1 p)}{\text{ord}_n p} \leq \frac{\text{ord}_n p}{\text{ord}_n p} = \text{ord}_n p \leq \varphi(n_1).$$

Then $\text{ord}_n p = \varphi(n_1)$.

Since

$$m' = \frac{\varphi(n_0m')}{\varphi(n_0)} = \frac{\varphi(\text{lcm}(n_0, n_3))}{\varphi(n_0)} = \frac{\text{ord}_{\text{lcm}(n_0,n_3)} p}{\text{ord}_n p} = \frac{\text{ord}_{n_0m'} p}{\text{ord}_n p} \leq \frac{m' \text{ord}_n p}{\text{ord}_n p} = m',$$

we obtain $\text{ord}_{n_0m'} p = m' \text{ord}_n p$. 


Proposition 3.3. Let

\[ m' \varphi(n_1) = \varphi(n_0 m' n_1) = \varphi(\text{lcm}(n_0, n_2)) = \frac{\text{ord}_{\text{lcm}(n_0, n_2)} p}{\text{ord}_{n_0} p} = \frac{\text{ord}_{n_0 m' n_1} p}{\text{ord}_{n_0} p} = \frac{\text{ord}_{n_0} p \varphi(n_1)}{\text{ord}_{n_0} p} = m' \varphi(n_1), \]

we obtain \( \text{lcm}(\text{ord}_{n_0 m' p}, \text{ord}_{n_1} p) = \text{ord}_{n_0 m' p} \text{ord}_{n_1} p \). Thus \( \gcd(\text{ord}_{n_0 m' p}, \text{ord}_{n_1} p) = 1 \).

2. Conversely, suppose that \( \text{ord}_{n_1} p = \varphi(m_1) \), \( \text{ord}_{n_0 m' p} = m' \text{ord}_{n_0} p \), and \( \gcd(\text{ord}_{n_1} p, \text{ord}_{n_0 m' p}) = 1 \). Then for every \( m \mid n_2 \), we let \( m_1 = \gcd(m_1, n_1) \) and \( m_2 = \frac{\text{lcm}(m_1, m_0)}{n_0} \). Then \( \text{ord}_{m_1} p = \varphi(m_1) \). It follows by \( n_0 m_2 \mid n_0 m' \) that \( \gcd(\text{ord}_{m_1} p, \text{ord}_{n_0 m_2} p) = 1 \) and

\[ \text{ord}_{n_0 m_2} p = \text{ord}_{n_0 m_2} m' \leq \frac{m'}{m_2} \text{ord}_{n_0 m_2} p = \frac{m'}{m_2} m_2 \text{ord}_{n_0} p = \frac{m'}{m_2} \text{ord}_{n_0} p = \text{ord}_{n_0 m' p}. \]

Thus \( \text{ord}_{n_0 m_2} p = m_2 \text{ord}_{n_0} p \). It follows that

\[ \frac{\text{ord}_{\text{lcm}(n_0, m)} p}{\text{ord}_{n_0} p} = \frac{\text{ord}_{m_1, n_0 m_2} p}{\text{ord}_{n_0} p} = \frac{\text{ord}_{\text{lcm}(m_1, \text{ord}_{n_0 m_2} p)} p}{\text{ord}_{n_0} p} = \frac{m_2 \text{ord}_{m_1} p \text{ord}_{n_0} p}{\text{ord}_{n_0} p} = \frac{m_2 \text{ord}_{m_1} p}{\frac{m'}{m_2} \text{ord}_{n_0} p} = \frac{\varphi(m_1)}{\frac{\varphi(n_0)}{\varphi(\text{gcd}(m_0, n_1))}}. \]

Therefore \( R[G] \) is clean.

3. In particular, if \( \exp(G) \) is a divisor of \( n \), then \( n_1 = m' = 1 \) and hence \( \mathcal{O}_p[G] \) is clean. \( \square \)

Next we characterize when a group ring of a finite abelian group over a local ring \( \mathcal{O}_p \) is \( * \)-clean. We need the following two propositions.

**Proposition 3.2.** Let \( m, n \in \mathbb{N} \). Then \( Q(\zeta_m + \zeta_m^{-1})(\zeta_n) = Q(\zeta_m)(\zeta_n) \) if and only if \( \gcd(m, n) \geq 3 \) or \( m \leq 2 \).

**Proof.** If \( m \leq 2 \), then it is obvious that \( Q(\zeta_m + \zeta_m^{-1})(\zeta_n) = Q(\zeta_m)(\zeta_n) \). We suppose \( m \geq 3 \).

Let \( K = Q(\zeta_m + \zeta_m^{-1}) \). Then \( K \subset Q(\zeta_m)(\zeta_n) = Q(\zeta_{\text{lcm}(m, n)}) \). Thus \( K(\zeta_n) = Q(\zeta_m)(\zeta_n) \) if and only if \( [K(\zeta_n) : K] = [Q(\zeta_{\text{lcm}(m, n)}) : K] \).

Since \( [Q(\zeta_{\text{lcm}(m, n)}) : K] = \frac{[Q(\zeta_{\text{lcm}(m, n)}) : Q(\zeta_n)]}{[Q(\zeta_n) : K]} = \frac{2\varphi(\text{lcm}(m, n))}{\varphi(m)} = \frac{2\varphi(n)}{\varphi(\text{gcd}(m, n))} \) and

\[ [K(\zeta_n) : K] = [Q(\zeta_n) : K \cap Q(\zeta_n)] = [Q(\zeta_n) : Q(\zeta_{\text{gcd}(m, n)})] [Q(\zeta_{\text{gcd}(m, n)}) : K \cap Q(\zeta_n)] \]

\[ = \frac{\varphi(n)}{\varphi(\text{gcd}(m, n))} [Q(\zeta_{\text{gcd}(m, n)}) : K \cap Q(\zeta_{\text{gcd}(m, n)})] \]

\[ = \frac{\varphi(n)}{\varphi(\text{gcd}(m, n))} [K(\zeta_{\text{gcd}(m, n)}) : K], \]

we obtain \( [K(\zeta_{\text{gcd}(m, n)}) : K] \leq 2 \). Moreover, \( K(\zeta_n) = Q(\zeta_m)(\zeta_n) \) if and only if \( [K(\zeta_{\text{gcd}(m, n)}) : K] = 2 \) if and only if \( \zeta_{\text{gcd}(m, n)} \notin K \).

If \( \gcd(m, n) \geq 3 \), then \( \zeta_{\text{gcd}(m, n)} \notin \mathbb{R} \) and hence \( \zeta_{\text{gcd}(m, n)} \notin K \subset \mathbb{R} \). It follows that \( K(\zeta_n) = Q(\zeta_m)(\zeta_n) \).

If \( \gcd(m, n) \leq 2 \), then \( \zeta_{\text{gcd}(m, n)} \in Q \subset K \) and hence \( K(\zeta_n) \neq Q(\zeta_m)(\zeta_n) \). \( \square \)

**Proposition 3.3.** Let \( G \) be a finite abelian group and let \( n \in \mathbb{N} \). Then \( Q(\zeta_n)[G] \) is \( * \)-clean if and only if \( \exp(G) \geq 3 \) and \( \gcd(\exp(G), n) \leq 2 \).

**Proof.** This follows from [4, Theorem 1.2] and Proposition 3.2. \( \square \)
Theorem 3.4. Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field for some $n \in \mathbb{N}$, $\mathcal{O} = \mathbb{Z}[\zeta_n]$ its rings of integers, $p \subset \mathcal{O}$ a nonzero prime ideal with $p\mathbb{Z} = p \cap \mathbb{Z}$, where $p$ is a prime, and $G$ a finite abelian group with $p \not| \exp(G)$. Let $n_0$ be the maximal positive divisor of $n$ with $p \nmid n_0$ and let $n_1$ be the maximal divisor of $\exp(G)$ with $\gcd(n_1,n_0) = 1$. Then the group ring $\mathcal{O}_p[G]$ is $\ast$-clean if and only if $\ord_{n_1}p = \varphi(n_1)$, $3 \leq \exp(G) \leq 2n_1$, and $\gcd(\ord_{n_1}p, \ord_{n_0}p) = 1$.

Proof. 1. Suppose $\ord_{n_1}p = \varphi(n_1)$, $3 \leq \exp(G) \leq 2n_1$, and $\gcd(\varphi(n_1), \ord_{n_0}p) = 1$. Since every prime divisor of $\exp(G)/n_1$ is a divisor of $n_0$, it follows from $\exp(G)/n_1 \leq 2$ that $(\exp(G)/n_1)$ divides $n_0$. Hence

$$\frac{\lcm(\exp(G), n_0)}{n_0n_1} = \frac{\lcm(\exp(G)/n_1, n_0)}{n_0} = 1.$$ 

Thus by Theorem 1.1 $\mathcal{O}_p[G]$ is clean. Since $p \nmid \exp(G)$, we have $\gcd(n, \exp(G)) = \gcd(n_0, \exp(G)/n_1) \leq 2$. Thus it follows from Proposition 3.3 that $\mathbb{Q}(\zeta_n)[G]$ is $\ast$-clean and hence by Theorem 2.3 $\mathcal{O}_p[G]$ is $\ast$-clean.

2. Suppose $\mathcal{O}_p[G]$ is $\ast$-clean. Let $m' = \frac{\lcm(\exp(G), n_0)}{n_0n_1}$. Since $\mathcal{O}_p[G]$ is clean, it follows from Theorem 1.1 that

$$\ord_{n_1}p = \varphi(n_1), \quad \ord_{n_0m'}p = m'\ord_{n_0}p, \quad \text{and} \quad \gcd(\varphi(n_1), m'\ord_{n_0}p) = 1.$$ 

By Theorem 2.3 and Proposition 3.3, we have $\exp(G) \geq 3$ and $\gcd(n, \exp(G)) \leq 2$. Thus $\gcd(n_0, \exp(G)/n_1) \leq 2$. Since every prime divisor of $\exp(G)/n_1$ is a divisor of $n_0$, we obtain

$$\exp(G) = 2^\ell n_1$$ 

for some $\ell \in \mathbb{N}_0$.

If $\ell \geq 2$, then $n_0 = 2n_0'$ with $n_0'$ is odd which implies that $m' = 2^{\ell-1}$. Thus

$$2^{\ell-1}\ord_{n_0}p = m'\ord_{n_0}p = \ord_{n_0m'}p = \lcm(\ord_{n_0}p, \ord_{n_0'}p) \leq 2^{\ell-2}\ord_{n_0}p = 2^{\ell-2}\ord_{n_0}p,$$

a contradiction. Thus $\exp(G) \leq 2n_1$ and $m' = 1$. The assertion follows. $\square$

Next, we provide some ($\ast$-clean or non-$\ast$-clean) clean group rings in each case of the characterizations of Theorems 1.1 and 3.3.

Example 3.5. Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field for some $n \in \mathbb{N}$, $\mathcal{O} = \mathbb{Z}[\zeta_n]$ its rings of integers, and $G$ a finite abelian group with $\exp(G) \geq 3$.

1. If $p$ is a primitive root of unity of $\exp(G)$, then $\mathcal{O}_p[G]$ is $\ast$-clean.

2. Suppose $\gcd(\exp(G), n) = 1$ and $\exp(G)$ has a primitive root. If there is a prime divisor $q$ of $\varphi(n)$ such that $q \nmid \varphi(\exp(G))$, then there exists $x, y \in \mathbb{N}$ with $\gcd(x, n) = 1$ and $\gcd(y, \exp(G)) = 1$ such that $\ord_{n}x = q$ and $\ord_{\exp(G)}y = \varphi(\exp(G))$. By Chinese Reminder Theory, there exists $z \in \mathbb{N}$ with $\gcd(z, n \exp(G)) = 1$ such that $\ord_{n}z = q$ and $\ord_{\exp(G)}z = \varphi(\exp(G))$. By Dirichlet prime number theorem, there is a prime $p$ such that $p \equiv z \pmod{n \exp(G)}$. Let $p \subset \mathcal{O}$ be a prime ideal such that $p \cap \mathbb{Z} = p\mathbb{Z}$. Then by Theorem 3.4 $\mathcal{O}_p[G]$ is $\ast$-clean.

3. Suppose $\gcd(\exp(G), n) \geq 3$, $\gcd\left(\frac{\exp(G)}{\gcd(\exp(G), n)}, n\right) = 1$, and $\frac{\exp(G)}{\gcd(\exp(G), n)}$ has a primitive root. If there is a prime divisor $q$ of $\varphi(n)$ such that $q \nmid \varphi\left(\frac{\exp(G)}{\gcd(\exp(G), n)}\right)$, then there exists a prime $p$ such that $\gcd(\ord_{n}p, \ord_{\frac{\exp(G)}{\gcd(\exp(G), n)}}p) = 1$. Let $p \subset \mathcal{O}$ be a prime ideal such that $p \cap \mathbb{Z} = p\mathbb{Z}$. Then by Theorems 1.1 and 3.4 $\mathcal{O}_p[G]$ is clean but not $\ast$-clean.

4. Let $n = 7$, $\exp(G) = 49 \times 3$, and let $p \subset \mathcal{O}$ be a prime ideal such that $p \cap \mathbb{Z} = 23\mathbb{Z}$. Since $\ord_{23}23 = 3$, $\ord_{23}23 = 2 = \varphi(3)$, and $\ord_{149}23 = 21 = 7\ord_{23}$, it follows from Theorems 1.1 and 3.4 $\mathcal{O}_p[G]$ is clean but not $\ast$-clean.
4. Group rings over local subrings of quadratic fields

In this section, we investigate when a group ring over a local subring of a quadratic field is clean. Let $d$ be a non-zero square-free integer with $d \neq 1$, $K = \mathbb{Q}(\sqrt{d})$ a quadratic number field, \[
\omega = \begin{cases} 
\sqrt{d} & \text{if } d \equiv 2, 3 \pmod{4}, \\
1 + \sqrt{d} & \text{if } d \equiv 1 \pmod{4},
\end{cases}
\]
and $\Delta = \begin{cases} 
4d & \text{if } d \equiv 2, 3 \pmod{4}, \\
d & \text{if } d \equiv 1 \pmod{4}.
\end{cases}$

Then $\mathcal{O}_K = \mathbb{Z}[\omega]$ is the ring of integers and $\Delta$ is the discriminant of $K$.

For an odd prime $p$ and an integer $a$, we denote by $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$ the Legendre symbol of $a$ modulo $p$.

We first provide two useful lemmas.

**Lemma 4.1.** Let $d \neq 1$ be a non-zero square-free integer and let $\Delta$ be the discriminant of $\mathbb{Q}(\sqrt{d})$. Then $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_n)$ if and only if $n$ is a multiple of $\Delta$.

**Proof.** This follows from [13, Corollary 4.5.5] \[ \square \]

**Lemma 4.2.** Let $d \neq 1$ be a non-zero square-free integer and let $I$ be a prime ideal of $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{d})$. Suppose $\Delta$ is the discriminant of $K$ and $\mathcal{O}_K/I = p$, where $p$ is a prime.

1. If $p = 2$, then $N(I) = p$ if and only if $\Delta \not\equiv 5 \pmod{8}$.
2. If $p$ is odd, then $N(I) = p$ if and only if $\left(\frac{\Delta}{p}\right) = 1$ or 0.

**Proof.** This follows by [1] Theorem 22, III.2.1, and V.1.1.] \[ \square \]

**Proof of Theorem 1.3** Let $R = \mathcal{O}_p$. By Theorem 2.2, we have $R[G] = \mathcal{O}_p[G]$ is clean if and only if $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\sqrt{d})] = \text{ord}_m(N(p))$ for every divisor $m$ of $n$.

1. Since $\Delta \mid n$, it follows by Lemma 4.1 that $\mathbb{Q}(\sqrt{d}) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ for every positive divisor $m$ of $n$.

2. Suppose the item 1.(a) or 1.(b) holds. By Lemma 4.2, we have $N(p) = p$. Therefore for every divisor $m$ of $n$, we obtain that $p$ is a primitive root of unity of $m$ and hence

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\sqrt{d})] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \text{ord}_m p = \text{ord}_m(N(p)).$$

Thus $R[G]$ is clean.

2. Conversely, suppose $R[G]$ is clean. Then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\sqrt{d})] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \text{ord}_m(N(p))$ implies that $\varphi(n) = \text{ord}_m(N(p))$. Thus $N(p) = p$ is a primitive root of unity of $n$. The assertions follow by Lemma 4.12.

2.1. Suppose that $R[G]$ is clean. Since $\Delta = 4d \equiv 4 \pmod{4}$, we have $[\mathbb{Q}(\zeta_4) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\sqrt{d})] = [\mathbb{Q}(\zeta_4) : \mathbb{Q}] = \text{ord}_4(N(p))$. Thus $\varphi(4) = \text{ord}_4(N(p))$ and hence $N(p) = p \equiv 3 \pmod{4}$. If $p \mid d$, then $p \mid n$, a contradiction. Thus $p \not\mid d$ and hence by Lemma 4.2, $\left(\frac{\Delta}{p}\right) = 1$.

Since $[\mathbb{Q}(\zeta_4) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\sqrt{d})] = [\mathbb{Q}(\zeta_4) : \mathbb{Q}(\sqrt{d})] = \text{ord}_4(N(p))$, we obtain that $\varphi(n)/2 = \text{ord}_4(N(p)) = \text{ord}_4 p$. Since $4 \mid n$, we may assume that $n = 2^r n'$ with $\ell \geq 2$ and $n'$ is odd. Thus $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/2^\ell \mathbb{Z})^* \times (\mathbb{Z}/n'\mathbb{Z})^*$. Since $(\mathbb{Z}/n\mathbb{Z})^*$ has an element of order $\varphi(n)/2$, we obtain that $n' = 1$ if $\ell \geq 3$ and $n'$ is a prime power if $\ell = 2$. Thus $n = 4q^2$ and $d = q^2$, where $q$ is a prime.

If $d \equiv 2 \pmod{4}$, then $|d| = q = 2$ is a prime. Suppose $d \equiv 3 \pmod{4}$. Then $q \equiv 3$. If $|d| = q^2$ with $t \geq 2$, then $4d \mid q$ and $4d \not\mid q^2$. Thus $q - 1 = \text{ord}_4 p$ and $2(q - 1) = \text{ord}_4 p$. Since $p^{(q-1)/2} \equiv -1 \pmod{q}$ and $q^2 \equiv 1 \pmod{4}$, we have $p^{q-1} \equiv 1 \pmod{4q}$, a contradiction to $2(q - 1) = \text{ord}_4 p$. Therefore $|d| = q$ is a prime.

2.2. Conversely, $\left(\frac{\Delta}{p}\right) = 1$ implies that $N(p) = p$. Suppose $|d| = 2$ and $n = 2^\ell$ with $\ell \geq 3$. Let $m$ be a positive divisor of $n$. If $m = 4$, then $[\mathbb{Q}(\zeta_4) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\sqrt{d})] = 2$ and $\text{ord}_4 p = 2$ by $p \equiv 3 \pmod{4}$. Thus $[\mathbb{Q}(\zeta_4) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\sqrt{d})] = \text{ord}_4 p$. If $m = 2^r$ with $t \geq 3$, then $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\sqrt{d})] = 2^{t-2}$
and $\text{ord}_m p = m/4 = 2^{t-2}$ by $2^{t-2} = \varphi(p)/2 = \text{ord}_p p$. Thus $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \text{ord}_m (N(p))$.

Putting all these together, we obtain that $R[G]$ is clean.

Suppose $|d| \geq 3$ is a prime and $n = 4|d|^\ell$. Let $m$ be a positive divisor of $n$. If $m = |d|^\ell$ for some $1 \leq t \leq \ell$, then $4d \nmid m$ and hence $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \varphi(m) = |d|^{t-1}(|d| - 1)$. Since $p$ is a primitive root of unity of $|d|^\ell$, we obtain $\varphi(m) = \text{ord}_m p$. Therefore $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \text{ord}_m (N(p))$. If $m = 2|d|^\ell$ for some $1 \leq t \leq \ell$, then $4d \nmid m$ and hence $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \varphi(m) = |d|^{t-1}(|d| - 1)$. Since $p$ is a primitive root of unity of $|d|^\ell$, we obtain $\varphi(m) = \text{ord}_m p$. Therefore $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \text{ord}_m (N(p))$. If $m = 4|d|^\ell$ for some $1 \leq t \leq \ell$, then $4d \mid m$ and hence $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \varphi(m) = |d|^{t-1}(|d| - 1)$. Since $p$ is a primitive root of unity of $|d|^\ell$, we obtain $\varphi(m) = \text{ord}_m p$. Therefore $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \text{ord}_m (N(p))$.

Putting all these together, we obtain that $R[G]$ is clean.

3. If $p \mid d$, then $p \mid n$, a contradiction. Therefore $\left(\frac{d}{p}\right) = 1$ or $-1$.

3.1. Let $R[G]$ be clean. Suppose $|d| = m$ is a prime and $n = |d|^\ell$ or $n = 2|d|^\ell$ for some $\ell \in \mathbb{N}$. If $\left(\frac{d}{p}\right) = -1$, then $N(p) = p^2$ and hence $[Q(\zeta_m) : Q(\zeta_n) \cap Q(\sqrt{d})] = \text{ord}_n p^2$ implies that $\varphi(n) = \text{ord}_n p$. If $\left(\frac{d}{p}\right) = 1$, then $N(p) = p$ and hence $[Q(\zeta_m) : Q(\zeta_n) \cap Q(\sqrt{d})] = \text{ord}_n p$ implies that $\varphi(n)/2 = \text{ord}_n p$. Putting all these together, we have $\text{ord}_n p = 2\left(\frac{d}{p}\right)$.

Otherwise, there exists a $m \mid n$ with $m \geq 3$ such that $d \nmid m$. Therefore $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \varphi(m) = \text{ord}_m (N(p))$. Since $\varphi(m)$ be must be even, we obtain that $N(p) = p$ and hence $\left(\frac{d}{p}\right) = 1$. Since $d \mid n$, we have $\varphi(n)/2 = \text{ord}_n p$. Therefore $(\mathbb{Z}/n\mathbb{Z})^\times \cong C_{\varphi(n)}$ or $C_2 \oplus C_{\varphi(n)/2}$, which implies that $n = q_1^i \ell_1^j q_2^k \ell_2^j$ or $2q_1^i q_2^k \ell_1^j q_2^l$ or $2q_1^i \ell_1^j q_2^k \ell_1^j$, where $q_1, q_2$ are distinct odd primes.

Since $d \equiv 1 \pmod{4}$, we have $n \neq 2i^i$. If $|d| = q_1^i$ with $t \geq 2$, then choose $m = q_1$ and hence $d \nmid m$, $\varphi(m) = q_1 - 1 = \text{ord}_m p$. Thus $p^{m-1}/2 \equiv -1 \pmod{m}$ and hence $p^{\varphi(m)-1}/2 \equiv -1 \pmod{|d|}$, a contradiction to $\varphi(|d|)/2 = \text{ord}_d p$.

Suppose $|d| = q_1$. Then $n = q_1^i q_2^j q_3^k$ or $q_1^i q_2^j q_3^k$ or $4q_1^i q_2^j q_3^k$ with $q_1 \equiv 1 \pmod{4}$. If $n = q_1^i q_2^j q_3^k$, then $p$ is a primitive root of unity of $q_2$ and $(q_1 - 1)/2 = \text{ord}_q q_2$, $|q_1 - 1)/2 = \text{ord}_q q_2$. Since $p^{\varphi(q_2)-1}/2 \equiv -1 \pmod{q_2}$, and hence $|q_1 - 1)/2 = \text{ord}_q q_2$. Therefore $p^{\varphi(q_2)-1}/2 \equiv 1 \pmod{q_2}$, a contradiction to $(q_1 - 1)/2 = \text{ord}_q q_2$. Since $n = q_1^i q_2^j q_3^k$, we have that $p^{\varphi(q_2)-1}/2 \equiv 1 \pmod{q_2}$, and hence $p^{\varphi(q_2)-1}/2 \equiv 1 \pmod{q_2}$. Since $p^{\varphi(q_2)-1}/2 \equiv 1 \pmod{q_2}$, $q_1, q_2$ are distinct odd primes.

Suppose $|d| = q_1^i q_2^j q_3^k$ with $t_1, t_2 \in \mathbb{N}$. Then $p$ is a primitive root of unity of $q_1^i$ and $q_2^j q_3^k$. If $t_1 + t_2 \geq 3$, then $d \nmid q_1 q_2$ and hence $\varphi(q_1 q_2) = \varphi(q_1) q_2 = \text{ord}_q q_2$, a contradiction (as $q_1 q_2$ has no primitive root). Thus $t_1 + t_2 = 1$. If $q_1 \equiv 1 \pmod{4}$ and $q_2 \equiv 1 \pmod{4}$, then there is a subgroup $H$ of $\mathbb{Z}/n\mathbb{Z}$ such that $H \cong C_1 \oplus C_4$, a contradiction. Since $d = q_1 q_2 \equiv 1 \pmod{4}$, we have $q_1 \equiv 3 \pmod{4}$ and $q_2 \equiv 3 \pmod{4}$ and $q_1, q_2, (q_1 - 1)/2, (q_2 - 1)/2$ are pairwise co-prime integers.

3.2. Conversely, suppose that (a) holds. Let $m$ be a positive divisor of $n$ with $m \geq 3$. Then $d \mid m$. If $\left(\frac{d}{p}\right) = 1$, then $N(p) = p$ and hence $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \varphi(m)/2 = \text{ord}_m p = \text{ord}_n (N(p))$, implying that $R[G]$ is clean. If $\left(\frac{d}{p}\right) = -1$, then $N(p) = p^2$ and hence $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \varphi(m)/2 = \text{ord}_m p^2 = \text{ord}_n (N(p))$, implying that $R[G]$ is clean.

Suppose that (b) holds. Then $N(p) = p$. Let $m$ be a positive divisor of $n$ with $m \geq 3$. If $m = q_1^i$ or $q_2^j$ or $4q_1^i q_2^j q_3^k$, then $d \mid m$ and hence $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \varphi(m) = \text{ord}_m p = \text{ord}_n (N(p))$. If $m = q_1^i q_2^j q_3^k$ or $2q_1^i q_2^j q_3^k$, then $d \mid m$ and hence $[Q(\zeta_m) : Q(\zeta_m) \cap Q(\sqrt{d})] = \varphi(m)/2 = \text{ord}_m p = \text{ord}_n (N(p))$. Therefore $R[G]$ is clean.

$\square$
Next we characterize when such a group ring is *-clean. We first prove the following lemma.

**Lemma 4.3.** Let $d \neq 1$ be a non-zero square free integer. Then $\mathbb{Q}(\sqrt{d})(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\sqrt{d})(\zeta_n)$ if and only if either (1) $d < 0$ and $\Delta \mid n$ or $n \leq 2$, where $n \in \mathbb{N}$ and $\Delta$ is the discriminant of $\mathbb{Q}(\sqrt{d})$.

*Proof.* If $n \leq 2$, it is obvious that $\mathbb{Q}(\sqrt{d})(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\sqrt{d})(\zeta_n)$. Now we let $n \geq 3$.

Suppose that $d < 0$ and $\Delta \mid n$. Then by Lemma 4.1 $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_n)$ and hence $\mathbb{Q}(\sqrt{d})(\zeta_n + \zeta_n^{-1}) \subset \mathbb{Q}(\zeta_n)$. Since $n \geq 3$ and $d < 0$, we have

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = [\mathbb{Q}(\sqrt{d})(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2.$$ 

Therefore $\mathbb{Q}(\sqrt{d})(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt{d})(\zeta_n)$.

Suppose that $d < 0$ and $\Delta \nmid n$. Then $\mathbb{Q}(\sqrt{d})(\zeta_n + \zeta_n^{-1}) \not\subset \mathbb{R}$ and by $n \geq 3$, we have $\mathbb{Q}(\sqrt{d})(\zeta_n) \not\subset \mathbb{R}$. Hence $\mathbb{Q}(\sqrt{d})(\zeta_n + \zeta_n^{-1}) \neq \mathbb{Q}(\sqrt{d})(\zeta_n)$.

Suppose that $d < 0$ and $\Delta \nmid n$. Thus by Lemma 4.1 $\sqrt{d} \not\in \mathbb{Q}(\zeta_n)$. Therefore $[\mathbb{Q}(\sqrt{d})(\zeta_n) : \mathbb{Q}] = 2\varphi(n)$ and $\mathbb{Q}(\sqrt{d})(\zeta_n + \zeta_n^{-1}) : \mathbb{Q} = \varphi(n)$. It follows that $\mathbb{Q}(\sqrt{d})(\zeta_n + \zeta_n^{-1}) \neq \mathbb{Q}(\sqrt{d})(\zeta_n)$.

**Proposition 4.4.** Let $G$ be a finite abelian group with exponent $n$. Then $\mathbb{Q}(\sqrt{d})[G]$ is *-clean if and only if $n \geq 3$ and either $d < 0$ or $\Delta \nmid n$, where $\Delta$ is the discriminant of $\mathbb{Q}(\sqrt{d})$.

*Proof.* This result follows from [3, Theorem 1.2] and Lemma 4.3.

**Theorem 4.5.** Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field for some non-zero square-free integer $d \neq 1$, $\mathcal{O}$ its ring of integers, $p \subset \mathcal{O}$ a nonzero prime ideal with $p\mathbb{Z} = p \cap \mathcal{O}$, and $G$ a finite abelian group with $p \mid \exp(G)$. Let $\Delta$ be the discriminant of the field extension $K/\mathbb{Q}$. Then

1. if $d > 0$, then $\mathcal{O}_p[G]$ is *-clean if and only if $\mathcal{O}_p[G]$ is clean and $\exp(G) \geq 3$.
2. if $d < 0$, then $\mathcal{O}_p[G]$ is *-clean if and only if $\Delta \nmid \exp(G)$, $p$ is a primitive root of unity of $\exp(G)$, $\exp(G) \geq 3$, and $\frac{\varphi(n)}{2} = 1$ or 0.

*Proof.* 1. Let $d > 0$. Suppose $\mathcal{O}_p[G]$ is clean and $\exp(G) \geq 3$. Then by Proposition 4.4 $\mathbb{Q}(\sqrt{d})[G]$ is *-clean. It follows from Theorem 2.3 that $\mathcal{O}_p[G]$ is *-clean.

Conversely, suppose $\mathcal{O}_p[G]$ is *-clean. Then by Theorem 2.3 $\mathbb{Q}(\sqrt{d})[G]$ is *-clean. It follows from Proposition 1.4 that $\exp(G) \geq 3$.

2. Let $d < 0$. Suppose that $\Delta \nmid \exp(G)$, $p$ is a primitive root of unity of $\exp(G)$, $\exp(G) \geq 3$, and $\frac{\varphi(n)}{2} = 1$ or 0. Then by Theorem 1.3 $\mathcal{O}_p$ is clean and by Proposition 4.4 $\mathbb{Q}(\sqrt{d})[G]$ is *-clean. It follows from Theorem 2.3 that $\mathcal{O}_p[G]$ is *-clean.

Conversely, suppose $\mathcal{O}_p[G]$ is *-clean. Then by Theorem 2.3 $\mathbb{Q}(\sqrt{d})[G]$ is *-clean and hence by Proposition 4.4 $\exp(G) \geq 3$ and $\Delta \nmid \exp(G)$. It follows from Theorem 1.3 that $p$ is a primitive root of unity of $\exp(G)$ and $\frac{\varphi(n)}{2} = 1$ or 0.

We close the paper by the following example which provide some (*-clean or non *-clean) clean group rings for each case of the characterizations of Theorems 1.3 and 1.5.

**Example 4.6.**

1. Let $\mathcal{O}$ be the ring of integer of $\mathbb{Q}(\sqrt{d})$ and let $G$ be a finite abelian group with $\gcd(\exp(G), d) = 1$, where $d \neq 1$ is a square free integer and $\exp(G) \neq 4$ has a primitive root. Suppose that $d = \delta d_0$ such that $d_0$ is the maximal odd positive divisor of $d$. Then $\delta \in \{-1, 2, -2\}$.

For every prime $p$ with $p \equiv 1 \pmod{8d_0}$, we have $\left(\frac{d}{p}\right) = \left(\frac{d_0}{p}\right) = 1$. Since there exists $x \in \mathbb{N}$ with $\gcd(x, \exp(G)) = 1$ such that $\text{ord}_{p\exp(G)} x = \varphi(\exp(G))$, for every prime $p$ with $p \equiv x \pmod{\exp(G)}$, we have $\text{ord}_{p\exp(G)} x = \varphi(\exp(G))$. Note that $\text{ord}_{\exp(G)} p = \varphi(\exp(G))$. By Dirichlet prime number theorem, there is a prime $p$ such that $p \equiv 1 \pmod{8d_0}$ and $p \equiv x \pmod{\exp(G)}$. Let $\mathfrak{p} \subset \mathcal{O}$ be a prime ideal such that $p\mathcal{O} = \mathfrak{p}$. Then by Theorem 1.3 $\mathcal{O}_p[G]$ is clean. If $\exp(G) \geq 3$, then by Theorem 4.5 $\mathcal{O}_p[G]$ is *-clean.
2. Let $\mathcal{O}$ be the ring of integer of $\mathbb{Q}(\sqrt{-2})$, let $p \subset \mathcal{O}$ be a prime ideal with $p \cap \mathbb{Z} = 3\mathbb{Z}$, and let $G$ be a finite abelian group with $\exp(G) = 8$. Then Theorem 1.3.2 and Theorem 4.5.2 imply that $\mathcal{O}_p[G]$ is clean but not $\ast$-clean.

3. Let $\mathcal{O}$ be the ring of integer of $\mathbb{Q}(\sqrt{3})$, let $p \subset \mathcal{O}$ be a prime ideal with $p \cap \mathbb{Z} = 11\mathbb{Z}$, and let $G$ be a finite abelian group with $\exp(G) = 12$. Then Theorem 1.3.2 and Theorem 4.5.1 imply that $\mathcal{O}_p[G]$ is clean as well as $\ast$-clean.

4. Let $\mathcal{O}$ be the ring of integer of $\mathbb{Q}(\sqrt{5})$, let $p \subset \mathcal{O}$ be a prime ideal with $p \cap \mathbb{Z} = 19\mathbb{Z}$, and let $G$ be a finite abelian group with $\exp(G) = 5$. Then Theorem 1.3.3.a and Theorem 4.5.1 imply that $\mathcal{O}_p[G]$ is clean as well as $\ast$-clean.

5. Let $\mathcal{O}$ be the ring of integer of $\mathbb{Q}(\sqrt{-3})$, let $p \subset \mathcal{O}$ be a prime ideal with $p \cap \mathbb{Z} = 5\mathbb{Z}$, and let $G$ be a finite abelian group with $\exp(G) = 6$. Then Theorem 1.3.3.b and Theorem 4.5.2 imply that $\mathcal{O}_p[G]$ is clean but not $\ast$-clean.

6. Let $\mathcal{O}$ be the ring of integer of $\mathbb{Q}(\sqrt{33})$, let $p \subset \mathcal{O}$ be a prime ideal with $p \cap \mathbb{Z} = 2\mathbb{Z}$, and let $G$ be a finite abelian group with $\exp(G) = 33$. Then Theorem 1.3.3.b and Theorem 4.5.1 imply that $\mathcal{O}_p[G]$ is clean as well as $\ast$-clean.

References


Department of Mathematics and Statistics, Brock University, 1812 Sir Isaac Brock Way, St. Catharines, Ontario, Canada L2S 3A1

E-mail address: yli@brocku.ca

Institute for Mathematics and Scientific Computing, University of Graz, NAWI Graz, Heinrichstrasse 36, 8010 Graz, Austria

E-mail address: qinghai.zhong@uni-graz.at