Realizable Dicyclic Groups

by
Lindsey Wise

Honors Thesis

Appalachian State University

Submitted to the Department of Mathematical Sciences
and The Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Science
December 2020

Approved by:

William J. Cook, Ph.D., Thesis Director and
Honors Director, Department of Mathematical Sciences

Brooke Hester, Ph.D., Second Reader

Vicky Klima, Ph.D., Third Reader

Jefford Vahlbusch, Ph.D., Dean, The Honors College

Abstract

It is well-known that the units of a ring forms a group called the group of units. A group that is the group of units for some ring is said to be *realizable*. Fuchs' problem asks whether a given group is realizable by some ring. In this paper, we present the resolution of Fuchs' problem for dihedral groups as given in [CL1]. We then present partial results for dicyclic groups. For dicyclic groups of order 12 and smaller, our results are complete.

Contents

1 Introduction

It is well-known that the units of a ring form a group, and it is reasonable to determine this group of units from a given ring. Over 50 years ago, László Fuchs published *Abelian Groups* [Fu] where he posed his infamous inversion of this exercise, now known as Fuchs' problem: Given an Abelian group G, is it possible to construct a ring R such that $R^\times = G$; that is, G is the unit group of R?

Even half a century later, the solution eludes us. Partial results exist for certain types of groups, including cyclic groups [Gi, PS], symmetric and alternating groups [DO1], finite simple groups [DO2], p-groups [CL2, SW], and dihedral groups [CL1]. As demonstrated by this list of groups, Fuchs' problem has since been extended to consider non-Abelian groups as well. We intend to extend this list further by considering Fuchs' problem for dicyclic groups, a double cover of the dihedral groups. To do so, we rely heavily on technology from [CL1] and include most of their major results here.

In this paper, we begin by stating necessary group and ring theory background. Then, we introduce dihedral groups with some basic properties and solve Fuchs' problem for dihedral groups of every order as described by [CL1]. We conclude with a discussion of dicyclic groups. This includes a full resolution of Fuchs' problem for dicyclic groups of order 12 and smaller and partial results for larger orders.

2 Background

Before considering Fuchs' problem in general, we need to review some group and ring theory background.

2.1 Groups

First, we introduce some basic definitions and results from group theory. These will help us state and solve our proposed problem. For more details, we refer the reader to [DF] and [Fr].

Definition 2.1. *Let G be a nonempty set, and let $\cdot$ be a binary operation. A* **group** *is an ordered pair $(G, \cdot)$ with the following properties:*

(a) (Closed) Let $a, b \in G$. Then $a \cdot b \in G$.

(b) (Associative) For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(c) (Identity) There exists an $e \in G$ such that for any $a \in G$, we have $a \cdot e = e \cdot a = a$.

(d) (Inverse) For each $a \in G$, there exists an $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

We call a group **Abelian** if for every $a, b \in G$, $a \cdot b = b \cdot a$. The **order** of a group $|G|$ is defined as the number of distinct elements in the group. If G is an infinite set, we say G has infinite order.

We can consider several possible structures for groups in order to classify them. The distinction between Abelian and non-Abelian groups lies in the operation itself, dictating the way that the elements of the set interact with each other.

Definition 2.2. *A* **cyclic group** *G has an element $g \in G$ such that g generates the group. We denote g is a generator of G by $\langle g \rangle = \{g, g^2, g^3, \dots\} = G$.*

Any two cyclic groups of the same order are isomorphic, we will denote a cyclic group of order n by C_n.

Theorem 2.3. *Every cyclic group is Abelian.*

Proof. Let $\langle g \rangle = G$ be a cyclic group. Then every element $a, b \in G$ can be represented by a power of g. Take $a = g^n$, $b = g^m$. Then

$$a \cdot b = g^n \cdot g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n = b \cdot a.$$

Thus G is Abelian. □

One way of constructing groups G is via generators and relations. In particular, if

$$G = \langle S \mid R \rangle = \langle x_1, x_2, \dots, x_\ell \mid r_1, r_2, \dots, r_k \rangle$$

where $S = \{x_1, \ldots, x_\ell\}$ are called **generators** and $R = \{r_1, \ldots, r_k\}$ are called **relations**, we can construct **words** from the **alphabet** S by concatenating $x_1^{\pm 1}, \ldots, x_\ell^{\pm 1}$. For example, $x_2^{-3}x_5x_1^7$ is a word in our alphabet. We can multiply words together using the relations $r_1 = 1, r_2 = 1, \ldots, r_k = 1$ together with $x_i x_i^{-1} = 1$ and $x_i^{-1}x_i = 1$. This group G is then generated by S where elements of G are equivalence classes of words in this alphabet.

Example 2.4. *Take $G = \langle a \mid a^5 = 1 \rangle$. So our alphabet is $a^{\pm 1}$ and words are then powers of a. By our specified relation, we know that powers of a reduce to one of $\{1, a, a^2, a^3, a^4\}$, so this is our group G. In particular, $G = C_5$ is the cyclic group of order 5.*

Definition 2.5. *Let G be a group and $g \in G$. The* **order** *of g is given by $|g| = n$ where n is the smallest positive integer such that $g^n = 1$. If no such n exists, then g is said to have infinite order. Note this only occurs when G is an infinite group.*

Definition 2.6. *A* **subgroup** *$H \leq G$ is a non-empty subset of G that is closed with respect to the operation of G and closed under inverses.*

A subgroup N of a group G that is closed under conjugation, that is, $gxg^{-1} \in N$ for all $g \in G$ and $x \in N$, is called a **normal subgroup**, *denoted $N \triangleleft G$.*

We can then use normal subgroups to build **quotient groups**. Given N a subgroup of G, we let $G/N = \{gN \mid g \in G\}$ where $gN = \{gn \mid n \in N\}$ is the **left coset** of N represented by g. Moreover, if N is a normal subgroup then G/N becomes a group under the multiplication $xN\, yN = xyN$.

Definition 2.7. *Let G, H be groups and let $\varphi : G \to H$. We call φ a* **group homomorphism** *if φ is operation-preserving. That is, for all $a, b \in G$,*

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

If φ is also a bijection, then we call φ a **group isomorphism** *and write $G \cong H$. Furthermore, the* **kernel** *of φ is the set*

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = 1_H\}$$

where 1_H is the identity of the group H, and the **image** *(or range) of φ is the set*

$$\mathrm{im}(\varphi) = \{\varphi(g) \mid g \in G\}.$$

Theorem 2.8 (First Isomorphism Theorem)**.** *Let $\varphi : G \to H$ be a group homomorphism. Then $\ker(\varphi)$ is a normal subgroup of G and $G/\ker(\varphi) \cong \mathrm{im}(G)$.*

Proof. For a proof of this theorem, see [Ga]. □

Definition 2.9. *The* **center** *of a group G is the normal subgroup*

$$Z(G) = \{x \in G \mid ax = xa \text{ for all } a \in G\}.$$

Definition 2.10. *The* **centralizer** *of a subset S of a group G is*

$$C_G(S) = \{g \in G \mid gs = sg \text{ for all } s \in S\}.$$

Definition 2.11. *The* **torsion subgroup** G_T *of an Abelian group* G *is the subgroup of* G *containing all elements of* G *with finite order. For any prime number* p*, the* p**-torsion subgroup** *contains all elements of* G *that have order a power of* p*. The* p*-torsion subgroup is denoted* $G_{T_p} = \{g \in G \mid \exists n \in \mathbb{N},\, p^n g = 0\}$*, and* $G_T \cong \bigoplus_{p \in P} G_{T_p}$ *(see Chapter* 12 *of [DF]).*

Definition 2.12. *We say a group* G *is* **decomposable** *if* G *has proper, nontrivial, normal subgroups* H *and* K *where* $H \cap K = \{1\}$ *(*1 *is the identity of* G*) and*

$$G = HK = \{hk \mid h \in H \text{ and } k \in K\}.$$

If G decomposes as $G = HK$, then $G = HK \cong H \times K$ where

$$H \times K = \{(h, k) \mid h \in H \text{ and } k \in K\}$$

and we multiply as follows: $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$. In other words, the internal direct product is isomorphic to the external direct product. We will identify the canonically isomorphic internal and external products: $HK = H \times K$.

Every finite Abelian group G has a canonical decomposition as the product of cyclic groups of prime power order. The number of such factors is denoted $\mathrm{d}(G)$.

For example, the dihedral group of order 4, D_4, as defined in Definition 3.1, is finite Abelian and has the decomposition $D_4 = C_2 \times C_2$ and $\mathrm{d}(D_4) = 2$. Only a few dihedral groups are decomposable, as stated in Proposition 3.2. Similarly, a group is called **indecomposable** if no such direct product exists. We prove that dicyclic groups are indecomposable in Theorem 4.3.

2.2 Rings

In this section we introduce the basic definition of a ring as well as some properties of rings and constructions of certain types of rings. We then draw connections between rings and groups to set up our resolutions of Fuchs' problem. For more details, see [DF] and [Hu].

Definition 2.13. *A* **ring** *is a set* R *with two binary operations* $+$ *and* $\times$ *such that*

(a) $1 \in R$ *such that* $a \times 1 = a = 1 \times a$*.*

(b) $(R, +)$ *is an Abelian group.*

(c) $\times$ *is an associative operation.*

(d) Distributivity holds for all $a, b, c \in R$*. That is,* $(a + b) \times c = (a \times c) + (b \times c)$ *and* $a \times (b + c) = (a \times b) + (a \times c)$*.*

Note that some authors do not require a multiplicative identity in their definition of a ring; we do since the presence of 1 is necessary for our discussion of Fuchs' problem. Further, for brevity we write $a \times b = ab$ for the remainder of this paper.

We say a ring R is **commutative** if $ab = ba$ for every $a, b \in R$. For example, $\mathbb{Z}$ is a commutative ring since standard multiplication is commutative. However, $M_n(R)$, the ring of $n \times n$ matrices with entries in R, generally is noncommutative. Let n be a positive integer and R a ring. Given $A, B \in M_n(R)$ where the (i,j)-entries of A and B are a_{ij} and b_{ij} respectively, we define $A + B$ to be the matrix whose (i,j)-entry is $a_{ij} + b_{ij}$ and define AB to be the matrix whose (i,j)-entry is $\sum_{k=1}^{n} a_{ik}b_{kj}$. Under these operations, $M_n(R)$ becomes a ring. Since the operation of matrix multiplication is not commutative in general, this is a noncommutative ring.

Example 2.14. *Take the commutative ring R and adjoin an indeterminant x, denoted $R[x]$. In particular,*

$$R[x] = \left\{ f(x) \;\middle|\; \text{for some } n \in \mathbb{Z}_{>0},\ f(x) = \sum_{i=0}^{n} r_i x^i \text{ where } r_i \in R \right\}$$

is a **polynomial ring** *in indeterminant x and coefficients in R. Elements add and multiply as expected. The coefficients are added and multiplied according to the operations in R.*

Definition 2.15. *Let R be a commutative ring and let G be a multiplicative group. A* **group ring** *is defined as*

$$R[G] = \left\{ A \;\middle|\; \text{for some } n \in \mathbb{Z}_{>0},\ A = \sum_{i=0}^{n} r_i g_i \text{ where } r_i \in R,\ g_i \in G \right\}.$$

We add elements by adding coefficients of like terms. Multiplication of elements is defined according to the group operation and then extended linearly according to the distributive laws. Further, we require that the elements of R commute with all elements in $R[G]$.

As a concrete example, take $R = \mathbb{Z}_3$ and $G = \mathrm{Dic}_2$ as expressed in Definition 4.1. Then general elements of $\mathbb{Z}_3[\mathrm{Dic}_2]$ are of the form

$$c_1 1 + c_2 a + c_3 a^2 + c_4 a^3 + c_5 x + c_6 ax + c_7 a^2 x + c_8 a^3 x$$

where each $c_i \in \mathbb{Z}_3$. Let $A = 2 + a^2 + 2x + ax$ and $B = 2a + x$ in $\mathbb{Z}_3[\mathrm{Dic}_2]$. Then we add A and B as

$$\begin{aligned} A + B &= (2 + a^2 + 2x + ax) + (2a + x) \\ &= 2 + 2a + a^2 + 3x + ax \\ &= 2 + 2a + a^2 + ax \end{aligned}$$

where we combine like terms and reduce coefficients modulo 3 as described by the ring. We multiply A and B as

$$\begin{aligned}
AB =&(2 + a^2 + 2x + ax)(2a + x)\\
=&(2)(2a) + (a^2)(2a) + (2x)(2a) + (ax)(2a) + (2)(x)\\
&+ (a^2)(x) + (2x)(x) + (ax)(x)\\
=&4a + 2a^3 + 4xa + 2axa + 2x + a^2x + 2x^2 + ax^2\\
=&4a + 2a^3 + 4a^3x + 2x + 2x + a^2x + 2a^2 + a(a^2)\\
=&4a + 2a^3 + 4a^3x + 4x + a^2x + 2a^2 + a^3\\
=&a + 2a^2 + 3a^3 + 4x + a^2x + 4a^3x\\
=&a + 2a^2 + x + a^2x + a^3x
\end{aligned}$$

where first we distribute terms and then rewrite terms in their standard word representation in Dic_2. Note that coefficients are in our ring $R = \mathbb{Z}_3$ and thus commute with every element, so we can always pull them to the front of each term. We then combine like terms and reduce coefficients modulo 3.

Definition 2.16. *The* **characteristic** *of a ring R, denoted* $\mathrm{char}(R)$*, is given by the minimum number of times needed to add one to itself before the summation equals zero. That is, for $1 \in R$, if $\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0$ but $\underbrace{1 + \cdots + 1}_{n-1 \text{ times}} \neq 0$, then $\mathrm{char}(R) = n$. If no such n exists, that is, we always have $1 + 1 + \cdots + 1 \neq 0$, then $\mathrm{char}(R) = 0$.*

The integers modulo n, $\mathbb{Z}_n$, have characteristic n. In our most natural example for a ring, $\mathbb{Z}$, we can never add 1 to itself and get 0. Thus, $\mathrm{char}(\mathbb{Z}) = 0$.

Note that in a ring R of characteristic n, we have

$$nr = \underbrace{r + \cdots + r}_{n \text{ times}} = r1 + \cdots + r1 = r(1 + \cdots + 1) = r(n1) = r0 = 0.$$

Notice that in a ring R of characteristic 2, such as $\mathbb{Z}_2$, we have that odd property that $1 + 1 = 0$ so that $-1 = 1$ and thus $-r = r$ for all $r \in R$.

Definition 2.17. *Let R be a ring where* $\mathrm{char}(R) = n$*. We call the smallest subring of R its* **prime subring***. In particular, if $S = \{k1 \mid k \in \mathbb{Z}\}$ where $k1 = \underbrace{1 + \cdots + 1}_{k \text{ times}}$, then S is the prime subring of R.*

Definition 2.18. *Let R be a ring, and let $r \in R$. If there exists an $x \in R$ such that $rx = 1$, then r is a* **left unit** *with* **right inverse** *x. If $xr = 1$, then r is a* **right unit** *with* **left inverse** *x. If r is a left and a right unit, then r is a* **unit***.*

In $\mathbb{Z}$, it is obvious that ± 1 are the only units since $(-1)(-1) = 1 = (1)(1)$. As soon as we introduce an $a \neq \pm 1$, we no longer have equality with 1. However, in the rational numbers $\mathbb{Q}$, every nonzero element is a unit. Note that every non-zero element in $\mathbb{Q}$ can be written as $\frac{a}{b}$ where $a, b \in (\mathbb{Z} - \{0\})$. Then $(\frac{a}{b})(\frac{b}{a}) = 1$.

Proposition 2.19. *Let R be a ring. Then we call the set of all units in R the* **group of units***, denoted $R^\times = U(R)$.*

Proof. To show $R^\times$ is a group under multiplication, first note that $1 \in R^\times$, so our set is non-empty. Next, since all elements are units, for any $a, b \in R^\times$ we have $a^{-1}, b^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$ and $bb^{-1} = b^{-1}b = 1$. This implies $(a^{-1})^{-1} = a$ and $(b^{-1})^{-1} = b$, so $a^{-1}, b^{-1} \in R^\times$. Now, $(ab)(b^{-1}a^{-1}) = a(1)a^{-1} = 1$ and $(b^{-1}a^{-1})(ab) = b^{-1}(1)b = 1$. So the product of units gives a unit, and what's more, $(ab)^{-1} = b^{-1}a^{-1}$. Finally, we inherit associativity from R, so $R^\times$ is a group under multiplication. □

As mentioned above, the units of $\mathbb{Z}$ are ± 1, so $\mathbb{Z}^\times = U(\mathbb{Z}) = \{\pm 1\} \cong C_2$, the cyclic group of order 2. Further, the units of $\mathbb{Q}$ are $\mathbb{Q} - \{0\}$, so the group of units is just $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$ under multiplication.

Definition 2.20. *Let D be a ring with $1 \neq 0$. If $D^\times = D - \{0\}$, that is, every nonzero element is a unit, then D is called a* **division ring** *or* **skew field**. *Moreover, if D is commutative, then D is a* **field**.

This is one way to prove $\mathbb{Q}$ is a field, as demonstrated by the statement above of its group of units.

Definition 2.21. *A group is* **realizable** *if it is the group of units of a ring. In other words, a group G is realizable if there exists some ring R such that $R^\times \cong G$.*

Moreover, we say that G is realizable in characteristic n if there exists some ring R of characteristic n such that $R^\times \cong G$.

Given a commutative ring R and a group G, we have that $G \subseteq (R[G])^\times$. So any group can appear among the units of some ring in any characteristic. Fuchs' problem is asking if we can find a ring where the units are *exactly* G. This is much more difficult.

An element x of an algebraic structure R that satisfies the property $xy = yx$ for all $y \in R$ is said to be **central**. An element a that satisfies the property $a^2 = a$ is said to be **idempotent**. Notice this implies that $a^n = a$ for any integer n. A **nilpotent** element satisfies a similar property: if n is a positive integer, we say a is nilpotent of **index** n if $a^n = 0$ but $a^{n-1} \neq 0$. If $a, b \neq 0$, but $ab = 0$, then a and b are **zero-divisors**.

Definition 2.22. *We call a ring where $1 \neq 0$ with no zero-divisors a* **domain**. *A commutative domain is called an* **integral domain**. *An integral domain in which every element except the multiplicative and additive identity has a unique factorization of primes up to ordering is called a* **unique factorization domain**, *or UFD.*

It is easy to show that the characteristic of any domain, and thus any integral domain, must be prime or zero.

Definition 2.23. *Let R, S be rings and let $\varphi : R \to S$. Suppose $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$. If in addition $\varphi(1) = 1$, we say φ is a* **ring homomorphism**. *If φ is also a bijection, then φ is an* **isomorphism** *and R and S are* **isomorphic**; *that is, $R \cong S$.*

The kernel of φ is defined to be the kernel of φ thought of as a group homomorphism under addition. In particular,

$$\ker(\varphi) = \{x \in R \mid \varphi(x) = 0\}.$$

Definition 2.24. *Let R be a ring, and let $S \subseteq R$. We say S is a* **subring** *of R if $1 \in S$ and S is a ring under the addition and multiplication of R.*

Definition 2.25. *An* **ideal** *I of a ring R is a subset of R that is closed under subtraction and satisfies the multiplicative absorption properties: $x - y, xr, rx \in I$ for every $x, y \in I$ and $r \in R$.*

That is, multiplication absorbs elements from outside the ideal into the ideal. We can use ideals to make new rings by quotienting a ring by an ideal from the ring. For example, the integers $\mathbb{Z}$ modulo an ideal of the integers $n\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ produces a familiar ring. Such a ring is called a **quotient ring**. To show that this construction is truly a ring, let I be an ideal of a ring R. Since R is an Abelian group under addition, I's closure under subtraction guarantees that it is a subgroup of R under addition. Since R's addition is commutative, I is in fact a normal subgroup. Thus $R/I = \{r + I \mid r \in R\}$ is an Abelian group under coset addition, $(r + I) + (s + I) = (r + s) + I$. Moreover, since I is an ideal, coset multiplication, $(r + I)(s + I) = rs + I$, is well-defined and R/I is a ring.

Given ideals I and J of R, the **product ideal** is defined to be

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \;\middle|\; n \in \mathbb{Z}_{\geq 0} \text{ and } x_i \in I \text{ and } y_i \in J \right\}.$$

That is, IJ consists of finite sums of products of elements drawn from I and J. In particular, $I^1 = I$, $I^2 = II$, and more generally $I^{n+1} = I^n I$.

We say N is a **nilpotent ideal** if N is an ideal and there exists some positive integer n such that $N^n = \{0\}$.

Theorem 2.26 (First Isomorphism Theorem for Rings)**.** *Let $\varphi : R \to S$ be a ring homomorphism. Then $R/\ker(\varphi) \cong \text{im}(\varphi)$.*

Proof. This follows from the first isomorphism theorem for groups. For a full proof, see [Hu]. □

Notice that if we let $\varphi : \mathbb{Z} \to R$ be the map $\varphi(k) = k1$, then φ is a ring homomorphism. Its image $\text{im}(\varphi) = S$, the prime subring, and we get that $S \cong R/\ker(\varphi)$ by the first isomorphism theorem.

Finally, we note that there exists a unique non-negative integer n where $\ker(\varphi) = \{n\ell \mid \ell \in \mathbb{Z}\} = n\mathbb{Z}$ so that $S \cong \mathbb{Z}/n\mathbb{Z}$. In particular, R's prime subring is $S \cong \mathbb{Z}_n$ if $\text{char}(R) = n > 0$ and $S \cong \mathbb{Z}$ if $\text{char}(R) = 0$.

Going forward, we identify R's prime subring with $\mathbb{Z}_n$ when $\text{char}(R) = n$ or $\mathbb{Z}$ when $\text{char}(R) = 0$.

Proposition 2.27. *If G is a group realizable in characteristic m, then it is the group of units of $\mathbb{Z}_m[G]/I$ for some ideal I. In particular, G is the group of units of a finite ring if and only if it is finite and realizable in positive characteristic.*

Proof. Let R be a ring of characteristic m where $R^\times = G$. There exists a ring homomorphism $\varphi : \mathbb{Z}_m[G] \to R$ that extends the identity map on G.

Notice that $\mathrm{im}(\varphi)$ contains all of G since φ extends the identity map on G. Thus since the image of the homomorphism contains all of the units of R, we have $(\mathrm{im}(\varphi))^\times = R^\times = G$.

By the first isomorphism theorem, $\mathrm{im}(\varphi) \cong \mathbb{Z}_m[G]/I$, where $I = \ker(\varphi)$. Therefore, we have that $(\mathbb{Z}_m[G]/I)^\times \cong G$.

Note that if G is not finite, R must be infinite since it must at least contain G. Also, if G can only be realized in characteristic 0, then our ring must contain a copy of $\mathbb{Z}$, which forces R to be infinite. On the other hand, if G is both finite and realizable in characteristic $n > 0$, we have just shown that it is the group of units of some quotient of $\mathbb{Z}_n[G]$. Since this ring is finite, G is realizable by a finite ring. □

Theorem 2.28. *Suppose G is a finite group realizable in R and $\mathrm{char}(R) = m$. Then the subring of R defined by $S = \{\sum_{g\in G} k_g g \mid k_g \in \mathbb{Z}_m\}$ has the same units as R: $S^\times = R^\times = G$.*

Proof. It is obvious that S is nonempty and closed under subtraction. Now, since groups are closed under multiplication, using the distributive law and the fact $\mathbb{Z}_m$ is a central subring, the multiplication of two summations will again be in S. Next, a unit $u \in S^\times$ implies $u \in R^\times$ since $S^\times \subseteq G$. Further, $g, g^{-1} \in G$ implies $g, g^{-1} \in S$ by the construction of S, so $G \subseteq S^\times$. Thus $S^\times = G$. □

Theorem 2.29. *Suppose G is realizable by R and $\mathrm{char}(R) = m$. Then $\mathbb{Z}_m^\times \subseteq Z(G)$.*

Proof. First, observe $\mathbb{Z}_m$ is a central subring of R. Further, $\mathbb{Z}_m^\times \subseteq G$ by the definition of units and each element in $\mathbb{Z}_m^\times$ is central. Then $\mathbb{Z}_m^\times \subseteq Z(G)$. □

Next, let R be a ring with prime characteristic p whose group of units has an element of order p^r. There is a ring homomorphism $\varphi : \mathbb{F}_p[x]/(x^{p^r} - 1) \to R$ sending x to a unit of order p^r. By sending $x \mapsto x + 1$, we can see the domain of φ is isomorphic to $\mathbb{F}_p[x]/(x^{p^r})$. Then there is some subring S of R such that $S = \mathrm{Im}\,(\varphi) \cong \mathbb{F}_p[x]/(x^n)$ for some $n \leq p^r$.

We now present some ring theory results compiled in [CL1].

Proposition 2.30. *The group of units of $R = \mathbb{F}_p[x]/(x^n)$ is isomorphic to*

$$U(n) = C_{p-1} \oplus \left(\bigoplus_{1\leq k<1+\log_p(n)} C_{p^k}^{\lceil \frac{n}{p^{k-1}} \rceil - 2\lceil \frac{n}{p^k} \rceil + \lceil \frac{n}{p^{k+1}} \rceil} \right).$$

Proof. This result is presented in [CL1] Proposition 2.4. Let $f(x), g(x) \in \mathbb{F}_p[x]$. If $f(x)g(x) = 1 \mod x^n$, then $fg = 1 + x^n\ell$. So $fg - x^n\ell = 1$ implies $\gcd(f, x^n) = 1$. That is, f must have a nonzero constant term since $\mathbb{F}_p[x]$ is a UFD. Let $B \leq R^\times$ be the subgroup of units with constant term 1 such that $R^\times = \mathbb{F}_p^\times \cdot B$. Then $f(x) = h(x) + c = c(c^{-1}h(x) + 1)$ where $c \in \mathbb{F}_p^\times$ and $c^{-1}h(x) + 1 \in B$. Now,

$$h(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x$$

has p choices for each of the $n - 1$ coefficients, so $|B| = p^{n-1}$. So by Lagrange's theorem every element of B has order a power of p.

Let α_{p^k} denote the number of units in B with an order dividing p^k. Consider the non-identity element $g(x) = 1 + c_j x^j + \cdots$ reduced modulo x^n. If $jp^k \geq n$, we lose those terms. Hence $\alpha_{p^k} = p^{n-\lceil n/p^k \rceil}$ is the number of units in B of an order dividing p^k.

Take β_{p^k} to be the number of factors in the canonical decomposition of B isomorphic to C_{p^k}. Since C_{p^k} has $\varphi(p^k) = p^k - p^{k-1}$ generators, we find

$$\alpha_{p^k} = p^{\beta_p} \cdot (p^2)^{\beta_{p^2}} \cdot \vdots \cdot (p^{k-1})^{\beta_{p^{k-1}}} \cdot (p^k)^{\beta_{p^k} + \beta_{p^{k+1}} + \cdots}.$$

Solving for β_{p^k} gives

$$\beta_{p^k} = \log_p \left(\frac{\alpha_{p^k}^2}{a_{p^{k-1}} \alpha_{p^{k+1}}} \right).$$

The formula then follows. □

Recall in Definition 2.12 we defined $\mathrm{d}(G)$ as the number of factors in the canonical decomposition of G as a direct product of cyclic groups of prime power order. The following proposition provides a lower bound on $\mathrm{d}(G)$ for some finite Abelian subgroup of a group of units.

Theorem 2.31. *Let R be a ring of prime characteristic p where $R^\times$ contains an element of order p^r for $r \geq 2$.*

(a) If $p > 2$, then $R^\times$ has a noncyclic finite Abelian subgroup G such that $\mathrm{d}(G) \geq 1 + (p-1)p^{r-2}$.

(b) If $p = 2$, then $R^\times$ has a finite Abelian subgroup G such that $\mathrm{d}(G) \geq 2^{r-2}$. If $r \geq 3$, then G is noncyclic.

Proof. This proposition is as stated in [CL1] Proposition 2.5. Let φ be as defined before Proposition 2.30. Since the domain of φ is isomorphic to $\mathbb{F}_p[x]/(x^{p^r})$, we have a subring of R given by $S = \mathrm{Im}\,(\varphi) \cong \mathbb{F}_p[x]/(x^n)$ for some $n \leq p^r$. We also must have an element of order $p^r \in S$. Then using the decomposition from Proposition 2.30, we must have $1 \leq r < 1 + \log_p(n)$ and $n \geq p^{r-1} + r$. Further, the quotient map $S \to \mathbb{F}_p[x]/(x^{p^{r-1}+1})$ is surjective since its kernel $(x^{p^{r-1}+1})$ is a nilpotent ideal in S. Thus $U_{p^{r-1}+1}$ is a quotient of a subgroup G of $R^\times$. Since taking quotients cannot increase the number of factors in the canonical decomposition of a finite Abelian group, $\mathrm{d}(G) \geq \mathrm{d}(U_{p^{r-1}+1})$. Next, note

$$U_{p^{r-1}+1} = C_{p-1} \times C_{p^{r-1}}^{p-1} \times C_{p^{r-2}}^{(p-1)^2} \times C_{p^{r-3}}^{p(p-1)^2} \times \cdots \times C_{p^2}^{p^{r-4}(p-1)^2} \times C_p^{p^{r-3}(p-1)^2}.$$

If $p > 2$, $\mathrm{d}(U_{p^{r-1}+1}) = 1 + (p-1)p^{r-2}$. If $p = 2$, $\mathrm{d}(U_{p^{r-1}+1}) = 2^{r-2}$. Moreover, when $p > 2$, $\mathrm{d}(U_{p^{r-1}+1}) \geq 3$ and if $p = 2$ and $r \geq 3$, then $\mathrm{d}(U_{p^{r-1}+1}) \geq 2$. In both cases, $\mathrm{d}(H) \geq 2$ where H is the p-torsion summand of $U_{p^{r-1}+1}$. It follows that G is a noncyclic Abelian subgroup. □

Definition 2.32. *The* **Jacobson radical** *of a ring R is given by*

$$J = \{x \in R \mid 1 + RxR \subseteq R^\times\}.$$

There are several alternative characterizations of the Jacobson radical, but this is the most relevant for our work. In particular, elements in the Jacobson radical can be used to create units. This following proposition is stated in [CL1] Proposition 2.6.

Proposition 2.33. *Let R be a ring with a finite group of units and let I be a two-sided ideal of R contained in the Jacobson radical. Then*

(a) The quotient map $\varphi : R \to R/I$ induces a surjective group homomorphism

$$\varphi^\times : R^\times \to (R/I)^\times.$$

(b) The set $1 + I = \ker(\varphi^\times)$ is a normal subgroup of $R^\times$, and I is finite since $R^\times$ is finite.

(c) We have $|R^\times| = |(R/I)^\times||\ker(\varphi^\times)| = |(R/I)^\times||I|$ and hence $|I|$ divides both $|R|$ and $|R^\times|$.

Theorem 2.34. *If R is a ring and I is a nilpotent two-sided ideal contained in the Jacobson radical of R, then there is a bijection between the set of central idempotent elements of R and the central idempotent elements of R/I^2.*

Corollary 2.35. *If R is a ring and I is a nilpotent two-sided ideal contained in the Jacobson radical of R, then R is indecomposable if and only if R/I^2 is indecomposable.*

See [CL1] Proposition 2.7 for more details.

The **descending chain condition** (DCC) states that there is no infinite descending sequence of ideals $I_1 \supseteq I_2 \supseteq \cdots$. We call a ring that satisfies the DCC an **Artinian ring**. Further, a **semiprimitive ring** is a ring with a trivial Jacobson radical, and any Artinian semiprimitive ring is **semisimple**.

Theorem 2.36. *Let $\mathbb{F}$ be a finite field. Then $|\mathbb{F}|$ is p^m for some prime p and positive integer m where $\mathrm{char}(\mathbb{F}) = p$. Moreover, not only must finite fields be of prime power order, but for each prime power there is a unique field of that size up to isomorphism. If $q = p^m$ is a prime power, we call this field $\mathbb{F}_q$.*

Proof. For a proof, see [DF]. □

Theorem 2.37 (Artin-Wedderburn Theorem)**.** *An Artinian semisimple ring R is isomorphic to the product of finitely many $M_{n_i}(D_i)$ where the division rings D_i and the matrix rings are uniquely determined up to permutation of i.*

Theorem 2.38 (Wedderburn's Little Theorem)**.** *Every finite domain is a field.*

Corollary 2.39. *Let R be a finite ring of prime characteristic p. If R has a trivial Jacobson radical, then it is a finite product of matrix rings of the form $M_m(\mathbb{F}_{p^k})$ where $m, k \in \mathbb{Z}_{>0}$.*

Proof. This is an application of Theorems 2.37 and 2.38. □

Example 2.40. *Let A, B be rings, and let*

$$f, g : A \to Z(B)$$

be ring homomorphisms from A into the center of B such that f and g have central values. Then the **semi-direct product** *$B \rtimes A$ is a ring if $B \rtimes A = B \oplus A$ as an additive group; that is,*

$$(b, a) + (d, c) = (b + d, a + c),$$

and if we define multiplication by

$$(b, a)(y, x) = (bf(x) + yg(a), ax).$$

The multiplicative identity of $B \rtimes A$ is $1 = (0, 1)$ since

$$\begin{aligned}(0, 1)(b, a) &= (0f(a) + bg(1), 1a) = (b, a)\\ (b, a)(0, 1) &= (bf(1) + 0g(a), a1) = (b, a).\end{aligned}$$

Further, $(b, a) \in (B \rtimes A)^\times$ if and only if $a \in A^\times$. Moreover, the inverse of a unit (b, a) is given by $(b, a)^{-1} = (-bg(a^{-1})f(a^{-1}), a^{-1})$.

Notice that if we are to have $(b, a)(y, x) = (0, 1) = (y, x)(b, a)$, we must have $ax = 1 = xa$ so that a must be a unit of A. Next, a simple calculation shows that

$$\begin{aligned}(b, a)(-bg(a^{-1})f(a^{-1}), a^{-1}) &= (bf(a^{-1}) - bg(a^{-1})f(a^{-1})g(a), aa^{-1})\\ &= (bf(a^{-1}) - bf(a^{-1})g(a^{-1})g(a), 1)\\ &= (bf(a^{-1}) - bf(a^{-1})g(a^{-1}a), 1)\\ &= (bf(a^{-1}) - bf(a^{-1}), 1)\\ &= (0, 1)\end{aligned}$$

and similarly $(-bg(a^{-1})f(a^{-1}), a^{-1})(b, a) = (0, 1)$.

Observe that because f and g preserve multiplication, they send 1 to 1, and their outputs are central.

Since we already have that $B \rtimes A$ is an Abelian group under addition, it only remains to check that its multiplication is associative and that the distributive laws hold.

To confirm associativity, suppose $(b, a), (y, x), (q, p) \in B \rtimes A$. Then

$$\begin{aligned}((b, a)(y, x))(q, p) &= (bf(x) + yg(a), ax)(q, p)\\ &= ((bf(x) + yg(a))f(p) + qg(ax), axp)\\ &= (bf(x)f(p) + yg(a)f(p) + qg(a)g(x), axp)\end{aligned}$$

matches

$$\begin{aligned}(b, a)((y, x)(q, p)) &= (b, a)(yf(p) + qg(x), xp)\\ &= (bf(xp) + (yf(p) + qg(x))g(a), axp)\\ &= (bf(x)f(p) + yf(p)g(a) + qg(x)g(a), axp)\end{aligned}$$

since f and g preserve multiplication and have central values in B.

Now, the distributive laws hold since

$$\begin{aligned}((b,a)+(y,x))(q,p) &= (b+y,a+x)(q,p) = ((b+y)f(p)+qg(a+x),(a+x)p)\\ &= (bf(p)+yf(p)+qg(a)+qg(x),ap+xp)\end{aligned}$$

matches

$$\begin{aligned}(b,a)(a,p)+(y,x),(q,p) &= (bf(p)+qg(a),ap)+(yf(p)+qg(x),xp)\\ &= (bf(p)+qg(a)+yf(p)+qg(x),ap+xp)\end{aligned}$$

and

$$\begin{aligned}(b,a)((y,x)+(q,p)) &= (b,a)(y+q,x+p) = (bf(x+p)+(y+q)g(a),a(x+p))\\ &= (bf(x)+bf(p)+yg(a)+qg(a),ax+ap)\end{aligned}$$

matches

$$\begin{aligned}(b,a)(y,x)+(b,a)(q,p) &= (bf(x)+yg(a),ax)+(bf(p)+qg(a),ap)\\ &= (bf(x)+yg(a)+bf(p)+qg(a),ax+ap)\end{aligned}$$

where we used the fact that f and g preserve addition.

Hence $B \rtimes A$ is a ring and $(B \rtimes A)^\times = \{(b,a) \mid b \in B \text{ and } a \in A^\times\}$

Example 2.41. *We define the* **quaternions**

$$\mathbb{H} = \{a+bi+cj+dk \mid a,b,c,d \in \mathbb{R}\}.$$

Take

$$\overline{a+bi+cj+dk} = a-bi-cj-dk$$

to be the **conjugate** *of the quaternion $a+bi+cj+dk$. Furthermore, we say*

$$\Re(a+bi+cj+dk) = a$$

is the real part of $a+bi+cj+dk$.

Definition 2.42. *We call a function $N : R \to \mathbb{R}$ a* **multiplicative norm** *if*

$$N(xy) = N(x)N(y)$$

and $N(x) = 0$ if and only if $x = 0$.

Proposition 2.43. *Let $v, w \in \mathbb{H}$ where $v = a+bi+cj+dk$ and $a,b,c,d \in \mathbb{R}$. We define $N(v) = v\overline{v} = \overline{v}v = a^2+b^2+c^2+d^2$.*

1. *$\overline{ab} = \overline{a}\overline{b}$, $\overline{a+b} = \overline{a}+\overline{b}$, and $\overline{\overline{a}} = a$.*
2. *N is a multiplicative norm. That is, $N(vw) = N(v)N(w)$ and $N(v) = 0$ if and only if $v = 0$. Moreover, $N(v) \geq 0$ for all v.*
3. *If $N(v) = 1$ and $N(v-1) = 0$, then $\Re(v) = 1$.*

Proof. These properties all follow from straightforward calculations. □

3 Dihedral Groups

This section introduces the dihedral group using the generator-relations construction and presents some basic properties of the dihedral group. For more information on dihedral groups, see Chapter 1 in both [DF] and [Ga].

After our discussion of dihedral groups in general, we state and prove results presented in [CL1] that resolve Fuchs' problem for dihedral groups entirely. Analogous results for dicyclic groups using similar approaches appear in Section 4.2.

Definition 3.1. *Let the* **dihedral group** *of order* $2n$ *be given by*

$$D_{2n} = \langle r, s \mid r^n = 1,\ s^2 = 1,\ rsrs = 1 \rangle,$$

Note that since $s^2 = 1$, that is, $s = s^{-1}$, and $rsrs = 1$, we have $rs = sr^{-1}$ and $sr = r^{-1}s$. This means any word over the alphabet $r^{\pm 1}$ and $s^{\pm 1}$ can be rewritten as $r^k s^\ell$. Moreover, since $r^n = 1$ and $s^2 = 1$, we can make sure $k = 0, 1, \ldots,$ or $n-1$ and $\ell = 0$ or 1. Thus $D_{2n} = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$.

If we construct D_{2n} as a symmetry group of a regular n-gon, then r generates the subgroup of rotations and $s, rs, \ldots, r^{n-1}s$ are the reflections. This guarantees that D_{2n} does indeed consist of exactly $2n$ distinct elements.

Proposition 3.2. *Dihedral groups satisfy the following properties.*

(a) We have $D_2 \cong C_2$ *and* $D_4 \cong D_2 \times D_2 \cong C_2 \times C_2$.

(b) For $n > 2$, *the center of* D_{2n} *is* $\{1\}$ *if* n *is odd and* $\langle r^{n/2} \rangle = \{1, r^{n/2}\}$ *if* n *is even.*

(c) For $n > 2$, *the dihedral group is indecomposable unless* $n = 2k$ *where* k *is odd, in which case* $D_{2n} \cong C_2 \times D_{2k}$, *where both factors are indecomposable. This direct product decomposition is unique up to the order of the factors.*

(d) For $n > 2$ *and* n *odd, the only proper normal subgroups of* D_{2n} *are subgroups of* $\langle r \rangle$. *For* $n > 2$ *and* n *even, there are two additional proper normal subgroups,* $\langle r^2, s \rangle$ *and* $\langle r^2, rs \rangle$, *both of order* n *and isomorphic to* D_n.

Proof. This is [CL1] Proposition 2.1. Its proof is a straightforward exercise in basic group theory. □

3.1 Realizing D_{2n}

Rather than checking each individual dihedral group for a possible ring to be realized in, Chebolu and Lockridge [CL1] showed the rings must have specific properties, namely, specific characteristics. Here we present restrictions on which dihedral groups are realizable in which ring characteristics and give examples of rings for each characteristic that realize each dihedral group.

Theorem 3.3. *Let R be a ring with a dihedral group of units $R^\times$. Then*

$$\mathrm{char}(R) = 0, 2, 3, 4, 6, 8, \text{ or } 12.$$

This is the main result of [CL1] given in Theorem 1.1. The following table also from [CL1] gives examples of rings and their corresponding dihedral group of units in $\mathrm{char}(R) = 0, 2, 3, 4, 6, 8,$ *and* 12*. Moreover, this is a complete list of dihedral groups realizable in the characteristics specified below. That is, if D_{2n} can be realized in characteristic m, then it is listed in the table below.*

$\mathrm{char}(R) = c$	$R^\times$	R
$c = 0$	D_2	$\mathbb{Z}$
	D_{4k}, k *odd*	$\mathbb{Z}_k \rtimes \mathbb{Z}[C_2]$
$c = 2$	D_2	$\mathbb{F}_2[D_2]$
	D_4	$\mathbb{F}_2[D_2] \times \mathbb{F}_2[D_2]$
	D_6	$M_2(\mathbb{F}_2)$
	D_8	$U_3(\mathbb{F}_2)$
	D_{12}	$\mathbb{F}_2[D_6]$
$c = 3$	D_2	$\mathbb{F}_3$
	D_4	$\mathbb{F}_3 \times \mathbb{F}_3$
	D_{12}	$U_2(\mathbb{F}_3)$
$c = 4$	D_2	$\mathbb{Z}_4$
	D_4	$\mathbb{Z}_4 \times \mathbb{Z}_4$
	D_8	$\mathrm{End}_{\mathbb{Z}}(C_4 \times C_2)$
	D_{12}	$\mathbb{Z}_4 \times M_2(\mathbb{F}_2)$
$c = 6$	D_2	$\mathbb{F}_2 \times \mathbb{F}_3$
	D_4	$\mathbb{F}_2 \times \mathbb{F}_3 \times \mathbb{F}_3$
	D_{12}	$\mathbb{F}_2 \times U_2(\mathbb{F}_3)$
$c = 8$	D_4	$\mathbb{Z}_8$
$c = 12$	D_4	$\mathbb{Z}_{12}$

We define the rings of this table in the following manner. Of course $\mathbb{Z}$ and $\mathbb{Z}_n$ denote the rings of integers and integers modulo n. As mentioned previously, the finite field of order q is denoted by $\mathbb{F}_q$, and the group ring composed of $R = \mathbb{F}_2$ and $G = D_{2n}$ is defined as in Definition 2.15. The matrix rings $M_n(R)$ and $U_n(R)$ denote the $n \times n$ matrices and upper triangular matrices with entries in R, respectively. Finally, $\mathrm{End}_{\mathbb{Z}}(C_4 \times C_2)$ is the endomorphism ring over the integers comprised of group homomorphisms from $C_4 \times C_2$ to $C_4 \times C_2$.

All that remains is our construction of the ring formed by the semi-direct product $\mathbb{Z}_k \rtimes \mathbb{Z}[C_2]$. First, recall that $\mathbb{Z}[C_2]$ is the group ring of the cyclic group of order 2 with integer coefficients. Let $C_2 = \{1, s\}$ so that $s^2 = 1$. Thus $\mathbb{Z}[C_2] = \{a + bs \mid a, b \in \mathbb{Z}\}$. Define

$$f, g : \mathbb{Z}[C_2] \to \mathbb{Z}_k$$

by $f(a+bs) = a+b \mod k$ and $g(a+bs) = a-b \mod k$. It is obvious f and g are ring homomorphisms, and since $\mathbb{Z}_k$ is a commutative ring, the values of f and g are central. Then by Example 2.40, $\mathbb{Z}_k \rtimes \mathbb{Z}[C_2]$ is a ring.

It is relatively straightforward to verify that each of the above rings give the claimed group as its group of units. One simply finds elements to call r and s among each ring's units. Then checks the requisite relations: $r^n = 1$, $s^2 = 1$, and $rsrs = 1$ and finally one must make sure there are exactly $2n$ units. For example, $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$. If $r = 3$ and $s = 5$ then $r^2 = 1$, $s^2 = 1$, and $rsrs = 1$. There are $2 \cdot 2 = 4$ units in $\mathbb{Z}_8$. Thus $\mathbb{Z}_8^\times = D_{2\cdot 2} = D_4$. We skip this verification in all other cases.

Now, finding examples is useful to grasp the effect of a unit group's structure on a ring, but it does not confirm that other characteristics of rings are impossible to generate. Hence we will prove Theorem 3.3 with the help of several propositions. We begin by constraining possible ring characteristics.

Proposition 3.4. *If R is a ring such that $R^\times \cong D_{2n}$, then* $\mathrm{char}(R) = 0, 2, 3, 4, 6, 8,$ *or* 12. *If $n > 1$ is odd, then* $\mathrm{char}(R) = 2$.

Proof. This is Proposition 2.3 from [CL1]. First, suppose R is a ring of characteristic $m > 0$ with $R^\times = D_{2n}$. Since $m > 0$, we have a central subring $\mathbb{Z}_m$ of R. This implies $\mathbb{Z}_m^\times$ is a subgroup of the center of D_{2n}. Now, this center is trivial if $n > 2$ is odd, is isomorphic to C_2 if $n = 1$ or $n > 2$ is even, and is isomorphic to $C_2 \times C_2$ if $n = 2$. Also note that $|\mathbb{Z}_m^\times| = \varphi(n)$ where $\varphi(n)$ is the Euler totient function. Now, if $m > 12$, we have $|\mathbb{Z}_m^\times| > 4$. Therefore, we must have that $\mathrm{char}(R) \leq 12$.

$m =$	1	2	3	4	5	6	7	8	9	10	11	12
$\lvert\mathbb{Z}_m^\times\rvert =$	1	1	2	2	4	2	6	4	6	4	10	4

Since $m = 1$ implies $R = \{0\}$, that we only have one unit, characteristic $m = 1$ can be ruled out immediately. If the center has order at most 2, we know $m = 2, 3, 4,$ or 6. Note that D_4 is Abelian of order 4, but $D_4 \cong C_2 \times C_2$, the noncyclic Klein 4-group. Since $\mathbb{Z}_5^\times$ and $\mathbb{Z}_{10}^\times$ are cyclic, we can rule out characteristics 5 and 10 even when considering D_4. However, for D_4, the ring may have characteristic 8 or 12, as we can see from Table 3.3. For $m > 2$, note that $-1 \in R$ is a central element with multiplicative order 2, since $-1 \neq 1$ and $(-1)^2 = 1$, but if n is odd there is no such element of D_{2n}. Hence for odd n the $\mathrm{char}(R) = 2$. □

3.1.1 Finite Rings

First, we constrain ourselves to positive ring characteristics. Here we detail restrictions on ring characteristics for each dihedral group of order $2n$.

Proposition 3.5. *Let $n \in \mathbb{Z}_{>0}$ such that n is not divisible by 8. If R is a finite ring of* $\mathrm{char}(R) = 2$ *with trivial Jacobson radical and $R^\times = D_{2n}$, then $n = 3$.*

Proof. This is [CL1] Proposition 3.1. Let R be as described. By Corollary 2.39, R is a product of matrix rings of the form $M_m(\mathbb{F}_{2^k})$. We know D_{2n} is indecomposable unless $n = 2r$ for r odd, when $D_{4r} = C_2 \times D_{2r}$ as stated in Proposition 3.2, part (c). Further,

the direct product decomposition is unique up to ordering and C_2 is not the group of units of any $M_m(\mathbb{F}_{2^k})$, we know $D_{2n} \cong \mathrm{GL}_m(\mathbb{F}_{2^k})$, the $m \times m$ invertible matrices with entries in $\mathbb{F}_{2^k}$. Since D_{2n} is a multiplicative group, we must have matrices closed under inverses, thus forcing this subset of $M_m(\mathbb{F}_{2^k})$. It is well known that

$$|\mathrm{GL}_m(\mathbb{F}_{p^k})| = (p^{mk} - 1)(p^{mk} - p) \dots (p^{mk} - p^{(m-1)k}).$$

If we distribute all the terms of this product, the power of p is $km(m-1)/2$. Further, since $p = 2$ and $8 \nmid n$, we know $km(m-1) \leq 6$.

If we take $m = 1$, then $\mathrm{GL}_m(\mathbb{F}_{2^k}) = \mathbb{F}_{p^k}$ has odd order, a contradiction since D_{2n} has even order.

If $k = 3$, then $m = 2$ and the $Z(\mathrm{GL}_2(\mathbb{F}_8)) = \mathbb{F}_8^\times$, which is not the center of any D_{2n}.

Similarly, if $k = 2$ then $m = 2$ and $Z(\mathrm{GL}_2(\mathbb{F}_4)) = \mathbb{F}_4^\times$ is not the center of any D_{2n}. If $k = 1$, then $m = 2$ or 3.

If $m = 2$, then $\mathrm{GL}_2(\mathbb{F}_2) = D_6$. If $m = 3$, then $\mathrm{GL}_3(\mathbb{F}_2)$ has a trivial center and order 168, but $Z(D_{168})$ has order 2. Hence only D_6 satisfies the criteria. □

Proposition 3.6. *If D_{2n} is realizable in characteristic 2, then n is divisible by 12.*

Proof. This is [CL1] Proposition 3.2. Let R be a ring of characteristic 2 with $R^\times = D_{2n}$. If 8 divides n, then since D_{2n} has a cyclic subgroup of order n given by the rotations $\langle r \rangle$, it has an element of order 8. Thus there exists a unit of order 8. By Proposition 2.31 (b), we know that D_{2n} contains a noncyclic Abelian subgroup when $n \neq 2$. Thus 8 must not divide n. From Proposition 2.27, without loss of generality we can assume that R is finite, and that R and its Jacobson radical J have orders which are powers of 2. Since $|J|$ divides $|R^\times|$, we can limit the possible orders of J to $|J| = 1, 2, 4$, or 8.

If we take $|J| = 1$, then Proposition 3.5 tells us $D_{2n} = D_6$ so $n = 3$.

If $|J| = 2$, then $1 + J \lhd D_{2n}$ has order 2 since the order does not change by adding 1. If $1 + J$ is in the rotation subgroup of D_{2n}, then we must have n is divisible by 2 and $D_n = (R/J)^\times$ is realizable in characteristic 2 by a ring with trivial Jacobson radical, again by Proposition 3.5 forcing $n = 3$ and $D_{2n} = D_6$. Otherwise, $1 + J$ has order n. The only order n subgroups of D_{2n} are $\langle r^2, s \rangle$ and $\langle r^2, rs \rangle$. This forces $n = 2$ and $D_{2n} = D_4$. If $1 + J = D_{2n}$, then we must have $n = 1$ and $D_{2n} = D_2$.

If $|J| = 4$, then $1 + J \lhd D_{2n}$ has order 4 since again the order does not change by adding 1. If $1 + J$ is in the rotation subgroup, then n is divisible by 4 and we have that $D_{n/2} = (R/J)^\times$ is realizable in characteristic 2 by a ring with trivial Jacobson radical, again using Proposition 3.5 to force $n = 12$ such that $D_{n/2} = D_6$. Otherwise, n must be even and $1 + J = \langle r^2, s \rangle$ or $\langle r^2, rs \rangle$. Both subgroups have order n, so $n = 4$ and $D_{2n} = D_8$. If $1 + J = D_{2n}$, then $n = 2$ to match orders.

If $|J| = 8$, since n cannot be divisible by 8 the only possibility is $1 + J = D_{2n}$ for $n = 4$. Hence the only possibilities in all cases are those where n is divisible by 12. □

Lemma 3.7. *If R is a characteristic 2 ring generated by $R^\times = D_{2n}$, then R is decomposable.*

Proof. For a proof of this lemma, see [CL1] Proposition 3.3. □

Proposition 3.8. *There is no characteristic 2 ring R for which $R^\times = D_{24}$.*

Proof. This is Proposition 3.4 from [CL1]. By Proposition 2.27, if D_{24} is realized by a characteristic 2 ring R then R is finite. Since D_{24} is indecomposable, we can also assume R is indecomposable. If we take $R = R_1 \times R_2$, then D_{24} must be the unit group for either R_1 or R_2. Hence we can replace R with one of R_1 or R_2.

Now, let J be the Jacobson radical of R. By Lagrange's theorem, we must have $|J| = 1, 2$, or 4. Note we can rule out $|J| = 8$ since D_{24} has no subgroup of order 8. Further, we can rule out $|J| = 1$ by Proposition 3.5. If $|J| = 2$, then $1 + J = \langle r^6 \rangle$ and R/J has trivial Jacobson radical with unit group D_{12}, a contradiction to Proposition 3.5. If $|J| = 4$, then $1 + J = \langle r^3 \rangle$. Since J is a nilpotent ideal and R is indecomposable, by Proposition 2.34 we know R/J^2 is indecomposable. Now, since $1 + J^2 = \langle r^6 \rangle$ and the map $R \to R/J^2$ is surjective on units, by the previous case $|J| = 2$ we have R/J^2 is an indecomposable ring generated by its unit group D_{12}. This is impossible by Proposition 3.7. □

This concludes our discussion of characteristic 2 rings. The next proposition completely resolves which dihedral groups are realizable in characteristic 3.

Proposition 3.9. *If $n \neq 1, 2,$ or 6, then D_{2n} is not realizable in characteristic 3.*

Proof. This is [CL1] Proposition 3.5. Suppose R is a characteristic 3 ring with $R^\times = D_{2n}$. If n is divisible by 9, then since D_{2n} has a cyclic subgroup of order n, it must have an element of order 9. Thus R contains a unit of order $3^2 = 9$. So by Theorem 2.31 (a), D_{2n} must contain a noncyclic Abelian subgroup, but no such group exists if $n \neq 2$. Hence n must not be divisible by 9.

Without loss of generality, we can assume that by Proposition 2.27, R is a finite ring, and we know the Jacobson radical of R is of order 1 or 3 since n is not divisible by 9. If $|J| = 1$, Corollary 2.35 tells us that R can be represented as the product of matrix rings of the form $M_m(\mathbb{F}_{3^k})$. Suppose in particular that the group of units is $\mathrm{GL}_m(\mathbb{F}_{3^k})$, which must be isomorphic to D_{2n} by assumption. Using the well-known order of $\mathrm{GL}_m(\mathbb{F}_n)$ described in the proof of Proposition 3.5, we know that the exponent of 3 in the prime factorization of $|\mathrm{GL}_m(\mathbb{F}_{3^k})|$ is $km(m-1)/2$. Further, since n is not divisible by 9, we have $km(m-1) \leq 2$. If we take $m = 1$, then $D_{2n} = \mathbb{F}_{3^k}^\times$ is cyclic, which is only true when $n = k = 1$. If $m = 2$, then $k = 1$, but $\mathrm{GL}_2(\mathbb{F}_3)$ has multiple subgroups of order 3 and $|\mathrm{GL}_2(\mathbb{F}_3)| = 48$. But D_{48} only has one subgroup of order 3, $\langle r^8 \rangle$. Hence if D_{2n} is indecomposable and realizable in characteristic 3 by a ring with trivial Jacobson radical, then $n = 1$. If D_{2n} is decomposable, then $n = 2k$ where k is odd and $D_{2n} = D_2 \times D_{2k}$ where D_{2k} is indecomposable. That is, if D_{2n} is decomposable and realizable in characteristic 3 by a ring with trivial Jacobson radical, then $n = 2$ so $D_{2n} = D_2 \times D_2 = D_4$.

If $|J| = 3$, then $(R/J)^\times \cong D_{2n/3}$ where R/J has trivial Jacobson radical. Hence $n = 3$ or 6 to ensure a viable order for a dihedral group. It remains to eliminate $n = 3$. If $R^\times \cong D_6$, then R has a subring isomorphic to a quotient of $\mathbb{F}_3[r]/(r^3)$. By Proposition 2.30, we know the unit group of this subring is $C_2 \times B$, where B is a finite Abelian 3-group. This must be a nontrivial group since the subring contains an element of order 3. But D_6 has no elements of order 3, so D_6 is not realizable in characteristic 3. □

We can now use our results about characteristics 2 and 3 to resolve which D_{2n} are realizable in characteristic 6.

Proposition 3.10. *If D_{2n} is the group of units of a characteristic 6 ring R, then one of the following must hold:*

(a) $D_{2n} = (\mathbb{F}_2 \times S)^\times$ where $\mathrm{char}(S) = 3$,

(b) $2n = 4k$ for k odd, and $D_{2n} = (S \times \mathbb{F}_3)^\times$ where $\mathrm{char}(S) = 2$, or

(c) $2n = 4k$ for k odd, and $D_{2n} = (\mathbb{F}_2[x]/(x^2) \times S)^\times$ where $\mathrm{char}(S) = 3$.

Proof. This is [CL1] Proposition 3.6. Suppose R is a characteristic 6 ring with unit group D_{2n}. Then $R = R_1 \times R_2$ where R_1 has characteristic 2 and R_2 has characteristic 3. Further, we must have $D_{2n} = R_1^\times \times R_2^\times$. We know that $R_2^\times$ cannot be trivial, so we could have $R_2^\times = D_{2n}$ and (a) holds when we set $S = R_2$. Otherwise, D_{2n} must be decomposable. Then $n = 2k$ for k odd and D_{2k} is indecomposable by Proposition 3.2. We can take $D_{2k} = R_1^\times$ or $D_{2k} = R_2^\times$. In the first case, $D_{2n} = (R_1 \times \mathbb{F}_3)^\times$ and (b) holds. In the second case, $D_{2n} = (\mathbb{F}_2[x]/(x)^2 \times R_2)^\times$ and (c) holds. □

The lone remaining positive characteristic is characteristic 4, which we resolve with the following two propositions.

Proposition 3.11. *If D_{2n} is realizable in characteristic 4, then $n = 1, 2, 4, 6$ or 8.*

Proof. This is [CL1] Proposition 3.7. Suppose R is a ring of characteristic 4 with $R^\times = D_{2n}$. For $t \in R$, we have $(1+2t)^2 = 1$. So the order of $1+2t$ must divide 2 in D_{2n}. Thus,

$$1 + (2) \subseteq \{g \in D_{2n} \mid |g| \leq 2\}.$$

Consider the quotient map $\varphi : R \to R/(2)$. Since quotient maps send units to units, we also have the map $\varphi^\times : R^\times \to (R/(2))^\times$, which is surjective since (2) is a nilpotent ideal and $1 + (2) = \ker(\varphi^\times)$. If we take the kernel to be trivial, then $2 = 0$, a contradiction since R has characteristic 4. Thus $\ker(\varphi^\times) \triangleleft D_{2n}$ is nontrivial and contains exclusively elements of order dividing 2. If $n \neq 1, 2$, or 4, then n must be even and $\ker(\varphi^\times) = \langle r^{n/2} \rangle$. So $(R/(2))^\times \cong D_n$. Then by Propositions 3.6 and 3.8, we know $n = 8$ or an even divisor of 12.

If $n = 12$, using Proposition 3.8 we know that R must be finite, indecomposable, and generated by D_{24}. We also know the Jacobson radical J of R contains the nilpotent ideal (2). Further, $R/(2)$ is a ring of characteristic 2 such that $(R/(2))^\times \cong D_{12}$ By Proposition 3.6, the Jacobson radical of $R/(2)$ must have size 2, so $|J| = 4$. Next, since $1 + J$ is a normal order 4 subgroup of D_{24}, we must have $1 + J = \langle r^3 \rangle$ and $1 + J^2 = \langle r^6 \rangle$ as they are the only elements of order 4 and order 2 respectively. Then $J^2 = (2)$. Since R is indecomposable, $R/J^2 = R/(2)$ by Proposition 2.34. But this contradicts Proposition 3.7 so we are finished. □

Proposition 3.12. *The dihedral group D_{16} is not realizable in characteristic 4.*

Proof. This is Proposition 3.8 in [CL1]. Assume to the contrary that there is a characteristic 4 ring R such that $R^\times = D_{16}$. Note that -1 is a central element of order 2, so $r^4 = -1$ in R since this is the unique element of order 2 in D_{16}. Thus there is a ring homomorphism

$$\varphi : \mathbb{Z}_4[x]/(x^4+1) \to R$$

which sends $x \mapsto r$. Let $S = \text{im}(\varphi)$. We will show that $2 = 0$ in S, forcing $\text{char}(S) = 2$. This then forces $\text{char}(R) = 2$, a contradiction.

Since S is a commutative subring of R and $\langle r \rangle = C_8 \subseteq S$, it must be that $S^\times = C_8$ since this is the only Abelian subgroup of D_{16} that contains C_8. Then ± 1 are the only units in S whose orders divide 2. Since $(1+2r)^2 = 1$, we must either have $1 + 2r = 1$, forcing $2 = 0$ since r is a unit, or $1 + 2r = -1$, forcing $2 + 2r = 0$.

Now, using $x^4 + 1 = 0$ and $2 + 2r = 0$, we have $(1 + (1 + r)^3)^2 = 1$. Then either $1 + (1 + r)^3 = 1$ forces $0 = (1 + r)^4 + 2 = 2$, or $1 + (1 + r)^3 = -1$ forces a similar contradiction $0 = (1 + r)^4 + 2 = 2(1 + r) + 2 = 2$. □

Thus we have proven Theorem 3.3 for positive ring characteristics.

3.1.2 Infinite Rings

All that remains to resolve dihedral groups are rings of characteristic 0. In this subsection we address all dihedral groups that are realizable in characteristic 0 to complete the proof of Theorem 3.3.

Suppose $n > 1$ and D_{2n} is realizable in characteristic 0. We know n is even by Proposition 3.4. Now, take $C_2 = \langle s \rangle$. Note $\mathbb{Z}[C_2] \cong \mathbb{Z}[s]/(s^2 - 1)$ has unit group $\{\pm 1, \pm s\} \cong D_4$.

Proposition 3.13. *For $k \in \mathbb{Z}_{>0}$, the semi-direct product $\mathbb{Z}_k \rtimes \mathbb{Z}[C_2]$ has unit group isomorphic to $C_2 \times D_{2k}$. In particular, if k is odd then D_{4k} is realizable in* $\text{char}(R) = 0$.

Proof. This proof is of Proposition 4.1 in [CL1]. We want to show

$$(\mathbb{Z}_k \rtimes \mathbb{Z}[C_2])^\times \cong \langle -1 \rangle \times D_{2k}$$

where $D_{2k} = \langle r, s \rangle$. Let $\pm 1 = (0, \pm 1)$, $r = (1, 1)$, and $s = (0, s)$. Note that $r^i = (i, 1)$ for any $i \in \mathbb{Z}$, so $|r| = k$ and r is a unit with inverse $r^{-i} = (-i, 1)$. Observe

$$sr = (0, s)(1, 1) = (1, s) = (-1, 1)(0, s) = r^{-1}s.$$

Then we have satisfied the relations $s^2 = 1$, $r^k = 1$,and $sr = r^{-1}s$. Hence $\pm D_{2k} = \pm\langle r, s \rangle$ is a subgroup of $(\mathbb{Z}_k \rtimes \mathbb{Z}[C_2])^\times$. Further, if $(t, u) \in (\mathbb{Z}_k \rtimes \mathbb{Z}[C_2])^\times$, then $u \in (\mathbb{Z}[s]/(s^2-1))^\times$, which is of order 4. So $(\mathbb{Z}_k \rtimes \mathbb{Z}[C_2])^\times$ has at most order $4k$. Therefore

$$(\mathbb{Z}_k \rtimes \mathbb{Z}[C_2])^\times \cong \langle -1 \rangle \times D_{2k}.$$

□

Now we must show that no other dihedral group is realizable in characteristic 0. First, we need a new ring.

Definition 3.14. *Let Q be the* **split quaternion** *ring over $\mathbb{Z}$. In particular,*

$$Q = \{a + bi + cs + dis \mid a, b, c, d \in \mathbb{Z}\}$$

where $i^2 = -1$, $s^2 = 1$, and $si = -is$.

Proposition 3.15. *If 8 divides $|D_{2n}|$, then D_{2n} is not realizable in characteristic 0.*

Proof. We sketch the proof here. See [CL1] for more details. Assume towards contradiction that a ring R exists where $R^\times \cong D_{8k}$. There exists a ring homomorphism

$$\varphi : Q \to R$$

where $i \mapsto r^k = i$ and $s \mapsto s$. Consider the element

$$z = (1 + 4i) + (3 + 3i)s \in Q.$$

There exists a multiplicative norm on Q such that $N(z) = 17 - 18 = -1$, so $z \in Q^\times$. Thus z maps to a unit in R. Then

$$0 = \varphi(z)^{8k} - 1 = \varphi(z^{8k} - 1)$$

since $|R^\times| = 8k$ and φ is a ring homomorphism. Then

$$0 = \varphi\left((z^{8k} - 1)\overline{(z^{8k} - 1)}\right) = \varphi\left(N(z^{8k} - 1)\right).$$

Then if $N(z^{8k} - 1) \neq 0$ we have a contradiction since the norms values are integers and $\mathbb{Z}$ has no zero divisors. Now, $z^2 = 2z + 1$ implies that $z^j = 2z^{j-1} + z^{j-2}$ for all $j \geq 2$. It follows that

$$\Re(z^j) = 2\Re(z^{j-1}) + \Re(z^{j-2}).$$

By induction, we can see that $\Re(z^j) > 2$ for all $j \geq 2$. In particular, $\Re(z^{8k}) \neq 1$ and $N(z^{8k}) = (-1)^{8k} = 1$ so $N(z^{8k} - 1) \neq 0$, a contradiction. □

Thus we have completely resolved Fuchs' problem for dihedral groups.

4 Dicyclic Groups

We now turn our attention to the primary purpose of this paper: to solve Fuchs' problem for dicyclic groups. First, we introduce the definition of dicyclic groups and some basic properties. Then, a complete resolution of Fuchs' problem is given for dicyclic groups of order 12 or less, and partial results are given for larger orders.

4.1 Dicyclic Group Basics

In this section we collect necessary facts about dicyclic groups in order to investigate Fuchs' problem.

Definition 4.1. *The* **dicyclic group** *of order* $4n$ *is given by*

$$\mathrm{Dic}_n = \langle a, x \mid a^{2n} = 1,\, a^n = x^2,\, x^{-1}ax = a^{-1} \rangle.$$

Using the third relation, multiplying on the left by x and multiplying on the right by a simplifies to $axa = x$. Then multiplying on the left by a^{-1} gives us the relation $xa = a^{-1}x$, and similarly, multiplying on the right by a^{-1} gives $ax = xa^{-1}$. Thus in Dic_n, any word in powers of a and x can be rewritten in the form $a^k x^\ell$. Using the second relation $a^n = x^2$, we can reduce the power ℓ to 0 or 1. Finally, the first relation $a^{2n} = 1$ allows us to simplify powers of a modulo $2n$. Hence we have at most

$$\mathrm{Dic}_n = \{1, a, a^2, \ldots, a^{2n-1}, x, ax, \ldots, a^{2n-1}x\}$$

distinct elements.

To show these elements are all distinct, consider the quaternion construction. In $\mathbb{H}$ we have $a = e^{\pi i/n}$, a primitive $2n^{\text{th}}$ root of unity, and $x = j$. Then $a^{2n} = 1$ and $a^n = -1 = x^2$. That is, $|a| = 2n$ and $|x| = 4$. Now, observe

$$\begin{aligned} x^{-1}ax &= -j\left(\cos\left(\frac{\pi}{n}\right) + i\sin\left(\frac{\pi}{n}\right)\right)j \\ &= \cos\left(\frac{\pi}{n}\right) + i\sin\left(\frac{\pi}{n}\right)(-jij) \\ &= \left(\cos\left(\frac{\pi}{n}\right) + i\sin\left(\frac{\pi}{n}\right)\right)(-i) \\ &= \cos\left(-\frac{\pi}{n}\right) + i\sin\left(-\frac{\pi}{n}\right) \\ &= a^{-1}. \end{aligned}$$

Thus we must have at least and at most $4n$ elements and $|G| = 4n$.

Proposition 4.2. *Let* $G = \mathrm{Dic}_n$.

(a) $|G| = 4n$. *Further,* $|a| = 2n$ *and* $|x| = 4$.

(b) $G\big/\langle x^2 \rangle = D_{2n}$.

(c) $Z(G) = \{1, a^n\}$.

Proof. (a) This is shown in the preceding paragraph.

(b) Note

$$\begin{aligned} \frac{G}{\langle x^2 \rangle} &= \langle a, x \mid a^{2n} = 1, a^n = x^2 = 1, x^{-1}ax = a^{-1} \rangle \\ &= \langle a, x \mid a^n = 1, x^2 = 1, axax = 1 \rangle \\ &= D_{2n}. \end{aligned}$$

(c) First, 1 and $a^n = -1$ are units of G so $\{1, a^n\} \subseteq Z(G)$. Assume there is another element $g \in Z(G)$. Let $g = a^k x^m$. But by definition, $xa^m = a^{-m}x$, so $gx = a^k x^{m+1}$ and $xg = xa^k x^m = a^{-k}x^{m+1}$. Hence $g \notin Z(G)$. □

To compute conjugates we can focus on the action of the generators of Dic_n: a and x.

Fix some $0 \leq k < 2n$. Then $aa^k a^{-1} = a^k$ and $xa^k x^{-1} = a^{-k}xx^{-1} = a^{-k}$. Therefore, the only conjugates of a^k are a^k and a^{-k}. So the conjugacy class of a^k is $\{a^k, a^{-k}\}$. Notice that since a is of order $2n$, $a^k = a^{-k}$ if and only if $2k = 0 \mod 2n$; that is, $k = 0 \mod n$. So these conjugacy classes are of order 2 for $0 < k < n$ or $n < k < 2n$ and of order 1 for $k = 0$ and $k = n$.

Next, fix some $0 \leq k < 2n$ and consider $a(a^k x)a^{-1} = a^{k+1}ax = a^{k+2}x$. Thus if k is even, then $a^k x$ is conjugate to any $a^\ell x$ where ℓ is even. If k is odd, then $a^k x$ is conjugate to any $a^\ell x$ where ℓ is odd. Also, notice that $x(a^k x)x^{-1} = a^{-k}x$. But since $a^{-k}x = a^{2n-k}x$ and $2n-k$ is even (respectively odd) precisely when k is even (respectively odd), conjugation by x does not give us any additional conjugates. Therefore, we have the following additional conjugacy classes: $\{ax, a^3x, \dots\}$ and $\{x, a^2x, \dots\}$. In summary, the dicyclic group decomposes into conjugacy classes as follows:

$$\mathrm{Dic}_n = \{1\} \cup \{a^{\pm 1}\} \cup \cdots \cup \{a^{\pm(n-1)}\} \cup \{a^n\} \cup \{x, ax^2, \dots\} \cup \{ax, a^3x, \dots\}.$$

Further, since $(a^k x)^2 = a^n$, we know that for any subgroup H of Dic_n either $H \subseteq \langle a \rangle$ or $a^n \in H$.

Theorem 4.3. *For all $n > 0$, Dic_n is indecomposable.*

Proof. Suppose $H, K \triangleleft \mathrm{Dic}_n$ with $H \cap K = \{1\}$ and $H \times K = \mathrm{Dic}_n$. Note that either H or K must contain an element other than merely powers of a since otherwise we have $HK \subseteq \langle a \rangle \neq \mathrm{Dic}_n$. Therefore, without loss of generality, assume H contains some element of the form $a^\ell x$. Now H is a normal subgroup and thus it is a union of conjugacy classes. Therefore, H contains either $E = \{x, a^2x, \dots, a^k x\}$ or $O = \{ax, a^3x, \dots, a^m x\}$ where we let k and m be the largest even (respectively odd) integer less than $2n$. Either way, we have $1 \in H$ and $(a^\ell x)^2 = a^n \in H$ since $a^\ell x \in H$. Thus since both $|E|$ and $|O|$ have n elements respectively, H must contain at least $n + 2$ elements.

Case 1: Assume n is odd. Then $a^{n+\ell}x = a^n a^\ell x \in H$ and so since $n + \ell$ is even if ℓ is odd and vice-versa and H is normal hence is the union of conjugacy classes, H must

contain both E and O. Therefore, $|H| \geq 2n+2$ so $|H| = 4n$ since the only divisor of $4n$ greater than $2n$ is $4n$ itself. Thus $H = \mathrm{Dic}_n$ and $K = \{1\}$.

Case 2: Assume n is even. If $E \subseteq H$ (respectively $O \subseteq H$), we have $x \in H$ (respectively $ax \in H$). Thus we have $a^\varepsilon x \in H$ for either $\varepsilon = 0, 1$. Now for any ℓ, we have $a^{\varepsilon+2\ell}x \in H$. Notice

$$a^{\varepsilon+2\ell}xa^\varepsilon x = a^{(\varepsilon+2\ell)-\varepsilon+n} = a^{2\ell+n} \in H.$$

Since n is even, $2\ell + n$ forces $\langle a^2 \rangle \subseteq H$. Thus $|H| \geq 2n$.

Assume $|H| = 2n$. Then $|K| = 2$. That is, for $b \in K$, $b \neq 1$, then $b^2 = 1$. If $b = a^p$, then $a^p a^p = 1$ implies that $p \equiv 0 \mod n$. That is, p is even and $a^p \in H$, a contradiction since $H \cap K = \{1\}$. Otherwise, if $b = a^p x a^p x = a^{p-p}a^n = a^n \neq 1$, so no K exists. Hence Dic_n is indecomposable. □

4.2 Realizability

With these properties in hand, we can now begin to postulate on the existence of realizable dicyclic groups. For $\mathrm{Dic}_1 \cong C_4$ and $\mathrm{Dic}_2 \cong Q_8$, the quaternion group of order 8, we can use results from [PS] and [SW] respectively. Then by Theorem 2.29, we can limit possible ring characteristics for $n \geq 2$ using the fact that $\mathbb{Z}_m^\times \subseteq Z(\mathrm{Dic}_n)$. Recall from Proposition 4.2 that $Z(\mathrm{Dic}_n) = \{1, x^2\}$. That is, we need $|\mathbb{Z}_m^\times| \leq 2$ in order to realize Dic_n for $n \geq 2$. This is only true for $m = 0, 2, 3, 4$, or 6. However, we can further condense this list using the following results.

Proposition 4.4. *Let R be a ring, let $n \geq 1$, and let $\mathrm{Dic}_n = R^\times$. Then $\mathrm{char}(R) \neq 3$ or 6.*

Proof. Note that in $\mathrm{char}(R) > 2$, we have $-1 \neq 1$ and $(-1)^2 = 1$. Therefore, we must have that $x^2 = a^n = -1$ since Dic_n has one element of order 2. First, suppose $\mathrm{char}(R) = 3$. Then

$$(1+x)^4 = 1 + 4x + 6x^2 + 4x^3 + x^4 = 1 + x + 0 + (-1)x + 1 = 2 = -1.$$

Therefore $(1+x)^8 = (-1)^2 = 1$ but we have just shown $(1+x)^4 = -1 \neq 1$. Hence by Lagrange's theorem $1 + x$ is a unit of order 8. But $x, ax, \ldots, a^{2n-1}x$ are all of order 4. Thus $1 + x = a^k$ for some k, and $a(1+x) = a^{k+1} = (1+x)a$ implies $a + ax = a + xa$ so that $ax = xa$. However, our relation from the definition of the dicyclic group $ax = a^{-1}x$ implies $a = a^{-1}$ and thus $a^2 = 1$.

Then $n = 1$, but Dic_1 has no elements of order 8, a contradiction. Therefore we cannot realize Dic_n in characteristic 3.

Now, suppose $\mathrm{char}(R) = 6$. Then

$$(2+x)^4 = 2^4 + 4 \cdot 2^3 x + 6 \cdot 2^2 x^2 + 4 \cdot 2x^3 + x^4 = 4 + 2x + 2(-1)x + 1 = 5 = -1.$$

Thus $(2+x)^8 = (-1)^2 = 1$ so as before we have, $2 + x$ is a unit of order 8. Again, this means $2 + x = a^k$ for some k, so $a(2+x) = a^{k+1} = (2+x)a$ implies $2a + ax = 2a + xa$ so that $ax = xa$. However, $ax = a^{-1}x$ implies $a = a^{-1}$ and thus $a^2 = 1$.

Once again we force $n = 1$ but Dic_1 has no element of order 8. Thus we cannot realize Dic_n in characteristic 6. □

Theorem 4.5. *Let $|G| = 2^k$ and let $g \in G$ such that $|g| \geq 0$ with $C_G(g) = \langle g \rangle$. Then G cannot be realized in characteristic 2^m for any $m \geq 1$.*

Proof. For a proof of this theorem, see [SW]. □

Now, note that $|\mathrm{Dic}_{2^k}| = 2^{k+2}$ and $|a| = 2^{k+1}$, which is greater than or equal to 8 if $k \geq 2$. Further, $C_{\mathrm{Dic}_{2^k}}(a) = \{y \in \mathrm{Dic}_{2^k} \mid ay = ya\} = \langle a \rangle$ since the set contains only powers of a. Therefore, we have the following partial result:

Theorem 4.6. Dic_{2^k} *for $k \geq 2$ cannot be realized in characteristic 2 or 4.*

4.2.1 Realizing Dic_1

Note that $\mathrm{Dic}_1 = \langle x \rangle$ since $x^1 = x$, $x^2 = a$, $x^3 = ax$, and $x^4 = 1$. Then we know $\mathrm{Dic}_1 \cong C_4$. Citing our previous discussion about $\mathbb{Z}_n^\times$ being contained in the center of our group of units, we get that the characteristic is limited to $m = 0, 2, 3, 4, 5, 6$, and 10. Recall $\mathbb{Z}_5^\times$ and $\mathbb{Z}_{10}^\times$ are cyclic order 4 whereas $\mathbb{Z}_8^\times$ and $\mathbb{Z}_{12}^\times$ are non-cyclic order 4. Theorem 4.4 rules out 3 and 6. This confirms results from [PS]. The following constructions then show that Dic_1 is realizable exactly when the characteristic is $m = 0, 2, 4, 5$, or 10.

Note the Gaussian integers $\mathbb{Z}[i]$ have units $\{\pm 1, \pm i\}$ which can be cyclically generated by i. That is, $(\mathbb{Z}[i])^\times \cong \langle i \rangle \cong C_4 \cong \mathrm{Dic}_1$. Hence Dic_1 is realizable in a ring of characteristic 0.

Consider the ring $\mathbb{Z}_2[x]/(x^3) = \{a + bx + cx^2 + (x^3) \mid a, b, c \in \mathbb{Z}_2\}$. An element is a unit if and only if the constant term is a unit, so $a = 1$ for all units. Observe

$$\begin{aligned}(1 + x + (x^3))^2 &= 1 + x^2 + (x^3)\\ (1 + x + (x^3))^3 &= 1 + x + x^2 + (x^3)\\ (1 + x + (x^3))^4 &= 1 + (x^3).\end{aligned}$$

Hence $\left(\mathbb{Z}_2[x]/(x^3)\right)^\times = \langle 1 + x + (x^3) \rangle \cong C_4 \cong \mathrm{Dic}_1$ and thus Dic_1 is realizable in a characteristic 2 ring.

Let $I = (2x, x^2 - 2)$. Take the characteristic 4 ring

$$R = \mathbb{Z}_4[x]/I = \{ax + b + I \mid a = 1 \text{ or } 3,\ b = 0, 1, 2, \text{ or } 3\}.$$

Since we have 2 choices for a and 4 choices for b, $|R| = 4 \times 2 = 8$. Now,

$$\begin{aligned}(1 + x + I)^2 &= 1 + 2x + x^2 + I = 1 + 2 + I = 3 + I\\ (1 + x + I)^3 &= (1 + x) \cdot 3 + I = 3 + 3x + I = 3 + x + I\\ (1 + x + I)^4 &= (3 + x)(1 + x) + I = 3 + 4x + x^2 + I = 5 + I = 1 + I.\end{aligned}$$

So $R^\times = \langle 1 + x + I \rangle \cong \mathbb{Z}_4 \cong \mathrm{Dic}_1$.

Since $\mathrm{Dic}_1 \cong C_4$, the cyclic group of order 4, we know Dic_1 is realized by $\mathbb{Z}_5$ and $\mathbb{Z}_{10}$ with characteristic 5 and 10 respectively.

4.2.2 Realizing Dic_2

Recall that the quaternion group of order 8 is given by $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. We can create an isomorphism between Dic_2 and Q_8 by $1 \mapsto 1$, $a \mapsto i$, $a^2 \mapsto -1$, $a^3 \mapsto -i$, $x \mapsto j$, $ax \mapsto ij = k$, $a^2x \mapsto -j$, $a^3x \mapsto -ij = -k$. Using Propositions 4.2 and 4.4, we can limit the possible ring characteristics for Dic_2 to $m = 0, 2$, and 4.

Take the characteristic 0 ring $\mathbb{Z}[i, j] = \mathbb{Z}[i, j, k]$, a subring of the quaternions $\mathbb{H}$. We have the norm $N(a+bi+cj+dk) = a^2+b^2+c^2+d^2$ where $N(a+bi+cj+dk) \in \mathbb{Z}_{\geq 0}$ for $a + bi + cj + dk \in \mathbb{Z}[i, j, k]$. Recall that the units $u \in \mathbb{Z}[i, j, k]$ are precisely the elements such that $N(u) = 1$. Thus each integer solution of $a^2 + b^2 + c^2 + d^2 = 1$ is a unit. The only possible integer solutions require one of the squares to be 1 and the rest to be 0. There are eight such solutions. We get that

$$\mathbb{Z}[i, j, k]^\times = \{\pm 1, \pm i, \pm j, \pm k\} = Q_8 = \mathrm{Dic}_2.$$

We can confirm Dic_2 is the unit group for the characteristic 2 ring $\mathbb{Z}_2[\mathrm{Dic}_2]/(1 + x + a + ax)$ using the GAP code in Appendix 6.1. Similarly, we can confirm Dic_2 is realizable in the characteristic 4 ring $\mathbb{Z}_4[\mathrm{Dic}_2]/(1 + x + a + ax, 1 + x^2)$ using the GAP code in Appendix 6.2.

4.2.3 Realizing Dic_3

In addition to the characteristic restrictions from Propositions 4.2 and 4.4, we also have the following two restrictions for Dic_3.

Proposition 4.7. *There is no characteristic 2 ring R for which $R^\times = \mathrm{Dic}_3$.*

Proof. Suppose $R^\times = \mathrm{Dic}_3$ where $\mathrm{char}(R) = 2$. First, note

$$(a^3 + a^k x)^4 = (a^3)^4 + (a^k x)^4 = 1 + 1 = 0$$

but

$$(a^3 + a^k x)^2 = (a^3)^2 + (a^k x)^2 = 1 + a^3 \neq 0.$$

Then $(1 + a^3 + a^k x)^4 = 1^4 + (a^3 + a^k x)^4 = 1$ but

$$(1 + a^3 + a^k x)^2 = 1^2 + (a^3 + a^k x)^2 = 1 + 1 + a^3 = a^3.$$

Thus $(1 + a^3 + a^k x)$ has order 4 for $k = 0, \ldots, 5$. Now, order 4 elements in Dic_3 are $a^\ell x$ for $\ell = 0, \ldots, 5$. If we assume $\ell = k$, then $1 + a^3 + a^k x = a^k x$. That is, $1 = a^3$, a contradiction since $|a^3| = 2$. If $\ell \neq k$, $1 + a^3 = a^k x + a^\ell x$ so $a = (1 + a^3)^2 = (a^k x + a^\ell x)^2$. Then

$$\begin{aligned}(a^k x)^2 + a^k x a^\ell x + a^k x a^\ell x + (a^k x)^2 &= 0\\ x a^{\ell-k} x &= x a^{k-\ell} x\\ a^{\ell-k} &= a^{k-\ell}\end{aligned}$$

implies $k \equiv \ell \mod 3$ and $k \neq \ell$. This gives us the equality $1 + a^3 = a^k x + a^{k+3} x$ for $k = 0, 1, 2$. We can further simplify to $a^j + a^{j+3} = 1 + a^3$.

Consider the element $x = 1 + a + a^2 + ax + a^2 x$. A simple calculation shows that $x^2 = 1 + ax + a^4 x + a^2 x + a^5 x$. But from our previous relations, we know that $ax + a^4 x = 1 + a^3$ and $a^2 x + a^5 x = 1 + a^3$, so $x^2 = 1 + ax + a^4 x + a^2 x + a^5 x = 1 + 1 + a^3 + 1 + a^3 = 3 + 2a^3 = 1$. Therefore, x is a unit of order 1 or 2. So either $x = 1$ or $x = a^3$. In other words, either $0 = x - 1 = a + a^2 + ax + a^2 x$ or $0 = x - a^3 = 1 + a + a^2 + a^3 + ax + a^2 x$.

Without loss of generality, by Theorem 2.28, we can assume that R is a quotient of $\mathbb{Z}_2[\mathrm{Dic}_3]$. In fact, given the above relations, we have that R must be a quotient of $\mathbb{Z}_2[\mathrm{Dic}_3]/I$ where $I = (1 + a^3 + a + a^4,\ 1 + a^3 + x + a^3 x,\ a + a^2 + ax + a^2 x)$ or $I = (1 + a^3 + a + a^4,\ 1 + a^3 + x + a^3 x,\ 1 + a + a^2 + a^3 + ax + a^2 x)$.

Using the GAP code in Appendix 6.3, we consider the quotients of $\mathbb{Z}_2[\mathrm{Dic}_3]$ by each of these ideals. However, both of these quotients have less than 12 elements and thus cannot realize Dic_3. Therefore, no quotient of $\mathbb{Z}_2[\mathrm{Dic}_3]$ realizes Dic_3 and thus Dic_3 cannot be realized in characteristic 2. □

Proposition 4.8. *There is no characteristic 4 ring R such that $R^\times = \mathrm{Dic}_3$.*

Proof. Suppose that R is a ring of characteristic 4 that realizes Dic_3. Moreover, as before, we can assume R is a quotient of the group ring $\mathbb{Z}_4[\mathrm{Dic}_3]$. Note that $a^3 = x^2 = -1$ and thus $a^3 + 1 = 0$ since we only have one unit of order 2 and in $\mathrm{char}(R) \neq 2$ this is -1.

First, observe $(1 + 2x)^2 = 1 + 4x + 4x^2 = 1$. So $1 + 2x$ is a unit of order 1 or 2. If the order of $1 + 2x$ is 1, then $1 + 2x = 1$ implies $2x = 0$. Thus $2 = 2xx^{-1} = 0x^{-1} = 0$, a contradiction (since our characteristic is 4). Hence $1 + 2x = -1$ and likewise $1 + 2a = -1$. Thus, in order to realize Dic_3 in $\mathrm{char}(R) = 4$, we must have $2 + 2x = 0$ and $2 + 2a = 0$. Now we can construct a nilpotent index 2 element $n = a + a^2 + ax + a^2 x$. Then

$$(1 + n)^2 = 1 + 2n = 1 + 2a + 2a^2 + 2ax + 2a^2 x = 1$$

since $a(2 + 2a) = 0$ and $(2 + 2a)ax = 0$. Thus $1 + n$ is a unit of order 1 or 2. If the order of $1 + n$ is 1, then $1 + n = 1$ and $n = 0$. If the order of $1 + n$ is 2, then $1 + n = -1$ so $2 + n = 0$.

Therefore, we must have $a^3 + 1 = 0$, $2 + 2a = 0$, $2 + 2x = 0$, and either $n = 0$ or $2 + n = 0$. Using the GAP code found in Appendix 6.4 we check the units of $\mathbb{Z}_4[\mathrm{Dic}_3]/(a^3 + 1, 2 + 2a, 2 + 2x, n)$ and $\mathbb{Z}_4[\mathrm{Dic}_3]/(a^3 + 1, 2 + 2a, 2 + 2x, 2 + n)$. Since neither of these quotient rings have enough units to contain Dic_3, we cannot realize Dic_3 in a ring of characteristic 4. □

Corollary 4.9. *Therefore,* Dic_3 *cannot be realized as the unit group of a finite ring.*

That leaves one final characteristic for which Dic_3 may be realizable.

Proposition 4.10. *It is possible to realize* Dic_3 *in a characteristic 0 ring.*

Proof. Let $\alpha = e^{2\pi i/6} = \frac{1+i\sqrt{3}}{2}$ be a primitive sixth root of unity. Consider the subring $R = \mathbb{Z}[\alpha, j]$ of the quaternions $\mathbb{H}$.

First, note that $\alpha^2 = \frac{-1+i\sqrt{3}}{2} = \alpha - 1$, so powers of α can be expressed in terms of linear combinations of 1 and α (with integer coefficients). This includes

$$\alpha^{-1} = \alpha^5 = \overline{\alpha} = 1 - \alpha = \frac{1 - i\sqrt{3}}{2}.$$

Also, $\alpha j = \frac{1+i\sqrt{3}}{2} j = \frac{j+k\sqrt{3}}{2} = j\frac{1-i\sqrt{3}}{2} = j\overline{\alpha}$ and likewise $\overline{\alpha} j = j\alpha$. Since $\overline{\alpha} = 1 - \alpha$, we can express all elements in terms of integer coefficient linear combinations of $1, \alpha, j$, and αj. Therefore,

$$R = \{n_1 + n_2\alpha + n_3 j + n_4 \alpha j \mid n_1, n_2, n_3, n_4 \in \mathbb{Z}\}.$$

Also, notice that if $q = n_1 + n_2\alpha + n_3 j + n_4 \alpha j \in R$, then

$$\begin{aligned} \overline{q} = n_1 + n_2\overline{\alpha} + n_3\overline{j} + n_4\overline{\alpha j} &= n_1 + n_2(1-\alpha) + n_3(-j) + n_4(1-\alpha)(-j) \\ &= (n_1 + n_2) - n_2\alpha - (n_3 + n_4)j + n_4\alpha j \qquad \in R. \end{aligned}$$

Therefore, R is closed under conjugation. Further,

$$\begin{aligned} N(n_1 + n_2\alpha) = N\left(\left(n_1 + \frac{n_2}{2}\right) + \left(\frac{n_2\sqrt{3}}{2}\right) i\right) &= \left(n_1 + \frac{n_2}{2}\right)^2 + \left(\frac{n_2\sqrt{3}}{2}\right)^2 \\ = n_1^2 + n_1 n_2 + \frac{n_2^2}{4} + \frac{3n_2^2}{4} &= n_1^2 + n_1 n_2 + n_2^2. \end{aligned}$$

Therefore, $N(n_1 + n_2\alpha + n_3 j + n_4\alpha j) = n_1^2 + n_1 n_2 + n_2^2 + n_3^2 + n_3 n_4 + n_4^2$ (which is an integer). Therefore, since we know that the norm of any quaternion is a non-negative real number, we have $N(q) \in \mathbb{Z}_{\geq 0}$ for any $q \in R$.

Consider $q \in R^\times$. Then since the norm is multiplicative, $N(q)N(q^{-1}) = N(qq^{-1}) = 1$. But since $N(q), N(q^{-1}) \in \mathbb{Z}_{\geq 0}$, we must have that $N(q) = 1$. Conversely, suppose $q \in R$ and $N(q) = 1$. Then by definition, $1 = N(q) = q\overline{q} = \overline{q}q$. Thus $q^{-1} = \overline{q}$ and since R is closed under conjugation, $q^{-1} = \overline{q} \in R$. Therefore, $q \in R^\times$ if and only if $N(q) = 1$.

Thus to determine the units of R we need to find all integer solutions of the equation:

$$n_1^2 + n_1 n_2 + n_2^2 + n_3^2 + n_3 n_4 + n_4^2 = 1.$$

Suppose $N(q) = 1$. We have $N(q) = \left(n_1 + \frac{n_2}{2}\right)^2 + \left(\frac{n_2\sqrt{3}}{2}\right)^2 + \left(n_3 + \frac{n_4}{2}\right)^2 + \left(\frac{n_4\sqrt{3}}{2}\right)^2$. If $|n_2| \geq 2$, then $\left(\frac{n_2\sqrt{3}}{2}\right)^2 = \frac{3}{4}n_2^2 > 1$, so $N(q) \neq 1$. Likewise, if $|n_4| \geq 2$, then $N(q) \neq 1$. So we must have $n_2, n_4 \in \{0, \pm 1\}$. Next, notice that if $|n_1| \geq 2$, then $\left|n_1 + \frac{n_2}{2}\right| > 1$, so $\left(\frac{n_2\sqrt{3}}{2}\right)^2 > 1$. Thus $N(q) \neq 1$ and $|n_1| \leq 1$. Likewise, $|n_3| \leq 1$. Therefore, we must have $n_1, n_2, n_3, n_4 \in \{0, \pm 1\}$.

Among these possible values of n_1, n_2, n_3, n_4 we have exactly 12 which give us an element of norm 1:

$$R^\times = \{\pm 1, \pm\alpha, \pm\alpha^2, \pm j, \pm\alpha j, \pm\alpha^2 j\}.$$

Notice that $\alpha^6 = 1$, $j^2 = \alpha^3 = -1$, and

$$j^{-1}\alpha j = -j\alpha j = -jj\overline{\alpha} = \overline{\alpha} = \alpha^{-1}.$$

Therefore, $R^\times = \mathrm{Dic}_3$. □

4.2.4 Realizing Dic_n

With Fuchs' problem for Dic_3 resolved, the first dicyclic group not isomorphic to a group for which Fuchs' problem is already known, we now turn to generalizing our results for Dic_n where $n > 3$.

Note that if $p = 1 \mod 4$, then $p^k - p^{k-1} = 1 - 1 = 0 \mod 4$ for any positive integer k. That is, $p^k - p^{k-1}$ is divisible by 4. If $p = 3 = -1 \mod 4$, then

$$p^k - p^{k-1} = (-1)^k - (-1)^{k-1} = 2(-1)^k = 2 \mod 4.$$

Proposition 4.11. *Let $m \in \mathbb{Z}_{>0}$ and suppose every prime factor of m is congruent to 1 modulo 4. Then $(\mathbb{Z}_m \rtimes \mathbb{Z}[i])^\times = \mathrm{Dic}_m$.*

Proof. First, note that if $m = 1$, then $\mathrm{Dic}_1 \cong C_4 \cong (\mathbb{Z}[i])^\times = (\{0\} \rtimes \mathbb{Z}[i])^\times$. We now assume $m > 1$. Next, note that since $2 \neq 1 \bmod 4$, $p = 2$ is not a factor of m and so m is odd.

Let $m = p_1^{k_1} \cdots p_n^{k_n}$ be the prime factorization of m where we have $p_i = 1 \bmod 4$ for each $i = 1, \ldots, n$. Notice that $p_i = 1 \bmod 4$ implies that 4 divides $p_i^{k_i} - p_i^{k_i - 1}$.

Since $(\mathbb{Z}_{p_i^{k_i}})^\times$ is cyclic and its order $p_i^{k_i} - p_i^{k_i-1}$ is divisible by 4, it must have an element of order 4, say τ_i. Moreover, $(\mathbb{Z}_{p_i^{k_i}})^\times$ has exactly one element of order 2 since it is cyclic, namely -1. Thus $\tau_i^2 = -1$.

Considering $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$ and $(\tau_1, \ldots, \tau_n)$ has order $\mathrm{lcm}\{4, \ldots, 4\} = 4$ and $(\tau_1, \ldots, \tau_n)^2 = (-1, \ldots, -1)$, we have that there exists a $\tau \in (\mathbb{Z}_m)^\times$ such that $|\tau| = 4$ and $\tau^2 = -1$. Consider $f : \mathbb{Z}[i] \to \mathbb{Z}_m$ defined by $f(a + bi) = a + b\tau$. Then $f(1) = 1$ and f preserves addition. We can confirm f preserves multiplication:

$$\begin{aligned} f((a+bi)(c+di)) &= f((ac-bd)+(ad+bc)i) \\ &= (ac-bd)+(ad+bc)\tau \\ &= (a+b\tau)(c+d\tau) \\ &= f(a+bi)f(c+di). \end{aligned}$$

Hence f is a ring homomorphism. Further, $Z(\mathbb{Z}_m) = \mathbb{Z}_m$ since $\mathbb{Z}_m$ is a commutative ring, so we map into the center of our ring. Similarly define a ring homomorphism $g : \mathbb{Z}[i] \to \mathbb{Z}_m$ as $g(a + bi) = a - b\tau$. We can then construct $\mathbb{Z}_m \rtimes \mathbb{Z}[i]$ using f and g such that

$$(m, a+bi)(n, c+di) = (m(c+d\tau) + n(a-b\tau), (a+bi)(c+di)).$$

Take $(-1, -1) \in \mathbb{Z}_m \rtimes \mathbb{Z}[i]$. Using induction,

$$\begin{aligned} (-1,-1)^k &= (-1,-1)^{k-1}(-1,-1) \\ &= ((-1)^{k-1}(k-1), (-1)^{k-1})(-1,-1) \\ &= ((-1)^{k-1}(k-1)(-1) + (-1)(-1)^{k-1}, (-1)^{k-1}(-1)) \\ &= ((-1)^k k, (-1)^k). \end{aligned}$$

So $(-1,-1)^k = ((-1)^k k, (-1)^k)$. In particular, since m is odd, we have

$$(-1,-1)^m = ((-1)^m m, (-1)^m) = (0,-1) = (0,i)(0,i).$$

Then $(-1,-1)^m = (0,i)^2$ and $(-1,-1)^{2m} = (0,1)$.

Next, observe

$$(-1,-1)^{-1} = (-1,-1)^{2m-1} = ((-1)^{2m-1}(2m-1), (-1)^{2m-1}) = (1,-1).$$

Now,

$$\begin{aligned}(-1,-1)(0,i) &= ((-1)\tau + 0(-1), (-1)i) = (-\tau, -i)\\ (0,i)(1,-1) &= (0(-1) + 1(-\tau), i(-1)) = (-\tau,-i).\end{aligned}$$

If we let $a = (-1,-1)$ and $x = (0,i)$, we just showed $a^{2m} = 1$, $a^m = x^2$, and $ax = xa^{-1}$. Further, we have $|(\mathbb{Z}_m \rtimes \mathbb{Z}[i])^\times| = |\mathbb{Z}_m| \cdot |(\mathbb{Z}[i])^\times| = m \cdot 4 = 4m$. Therefore

$$(\mathbb{Z}_m \rtimes \mathbb{Z}[i])^\times = \mathrm{Dic}_m.$$

□

5 Conclusion

We can construct the following table describing when Dic_n can be realized in various characteristics where $n = 1, 2, 3$, or m as defined in Proposition 4.11.

$\mathrm{char}(R) = c$	$R^\times$	R
$c = 0$	Dic_1	$\mathbb{Z}[i]$
	Dic_2	$\mathbb{Z}[i, j]$
	Dic_3	$\mathbb{Z}[e^{2\pi i/6}, j]$
	Dic_m for m in Prop. 4.11	$\mathbb{Z}_m \rtimes \mathbb{Z}[i]$
$c = 2$	Dic_1	$\mathbb{Z}_2[x] \big/ (x^3)$
	Dic_2	$\mathbb{Z}_2[\mathrm{Dic}_2] \big/ (1 + x + a + ax)$
$c = 4$	Dic_1	$\mathbb{Z}_4[x] \big/ (2x, x^2 - 2)$
	Dic_2	$\mathbb{Z}_4[\mathrm{Dic}_2] \big/ (1 + x^2, 1 + x + a + ax)$
$c = 5$	Dic_1	$\mathbb{Z}_5$
$c = 10$	Dic_1	$\mathbb{Z}_{10}$

We showed that Dic_n can only be realized in characteristics $0, 2, 4, 5$, and 10. In particular, Dic_1 is the only dicyclic group realizable in characteristics 5 and 10. Thus our table in complete for $c = 5$ and $c = 10$.

We conjecture this table is similarly complete for characteristics 2 and 4. For characteristic 0, we are less sure of the completeness of this table.

6 Appendix

6.1 Realizing Dic_2 in Characteristic 2

This is GAP code [GAP] that constructs a ring of characteristic 2 whose group of units is Dic_2 (i.e., the quaternion group of order 8). In particular, $R = \mathbb{Z}_2[\mathrm{Dic}_2]$, $I = (1 + a + x + ax)$, and $S = R/I$ has Dic_2 as its group of units.

```
# GAP CODE BEGINS HERE.
T := EmptySCTable(8,0);;

for i in [1..8] do
   # 1*Y = Y and Y*1 = Y
   SetEntrySCTable(T,1,i,[1,i]);
   SetEntrySCTable(T,i,1,[1,i]);
od;;

# i*Y = ...
SetEntrySCTable(T,2,2,[1,5]);
SetEntrySCTable(T,2,3,[1,4]);
SetEntrySCTable(T,2,4,[1,7]);
SetEntrySCTable(T,2,5,[1,6]);
SetEntrySCTable(T,2,6,[1,1]);
SetEntrySCTable(T,2,7,[1,8]);
SetEntrySCTable(T,2,8,[1,3]);

# j*Y = ...
SetEntrySCTable(T,3,2,[1,8]);
SetEntrySCTable(T,3,3,[1,5]);
SetEntrySCTable(T,3,4,[1,2]);
SetEntrySCTable(T,3,5,[1,7]);
SetEntrySCTable(T,3,6,[1,4]);
SetEntrySCTable(T,3,7,[1,1]);
SetEntrySCTable(T,3,8,[1,6]);

# k*Y = ...
SetEntrySCTable(T,4,2,[1,3]);
SetEntrySCTable(T,4,3,[1,6]);
SetEntrySCTable(T,4,4,[1,5]);
SetEntrySCTable(T,4,5,[1,8]);
SetEntrySCTable(T,4,6,[1,7]);
SetEntrySCTable(T,4,7,[1,2]);
SetEntrySCTable(T,4,8,[1,1]);

# -1*Y = ...
```

```
SetEntrySCTable(T,5,2,[1,6]);
SetEntrySCTable(T,5,3,[1,7]);
SetEntrySCTable(T,5,4,[1,8]);
SetEntrySCTable(T,5,5,[1,1]);
SetEntrySCTable(T,5,6,[1,2]);
SetEntrySCTable(T,5,7,[1,3]);
SetEntrySCTable(T,5,8,[1,4]);

# -i*Y = ...
SetEntrySCTable(T,6,2,[1,1]);
SetEntrySCTable(T,6,3,[1,8]);
SetEntrySCTable(T,6,4,[1,3]);
SetEntrySCTable(T,6,5,[1,2]);
SetEntrySCTable(T,6,6,[1,5]);
SetEntrySCTable(T,6,7,[1,4]);
SetEntrySCTable(T,6,8,[1,7]);

# -j*Y = ...
SetEntrySCTable(T,7,2,[1,4]);
SetEntrySCTable(T,7,3,[1,1]);
SetEntrySCTable(T,7,4,[1,6]);
SetEntrySCTable(T,7,5,[1,3]);
SetEntrySCTable(T,7,6,[1,8]);
SetEntrySCTable(T,7,7,[1,5]);
SetEntrySCTable(T,7,8,[1,2]);

# -k*Y = ...
SetEntrySCTable(T,8,2,[1,7]);
SetEntrySCTable(T,8,3,[1,2]);
SetEntrySCTable(T,8,4,[1,1]);
SetEntrySCTable(T,8,5,[1,4]);
SetEntrySCTable(T,8,6,[1,3]);
SetEntrySCTable(T,8,7,[1,6]);
SetEntrySCTable(T,8,8,[1,5]);

# Additive orders of elements
TO := [2,2,2,2,2,2,2,2];;

# Denote 1 as e, -1 as ne, -i as ni, etc.
TL := ["e","i","j","k","ne","ni","nj","nk"];;

# This is Z_2[Dic_2]
R := RingByStructureConstants(TO,T,TL);

GN := GeneratorsOfRing(R);
```

```
G := Units(R);

Print("R has size ");
Print(Size(R));
Print(" and there are ");
Print(Size(G));
Print(" units of R.\n\n");

# S = Z_2[Dic_2]/(1+a+x+ax)
I := Ideal(R,[GN[1]+GN[2]+GN[3]+GN[4]]);
S := R/I;

G := Units(S);

# Print out information about our ring S.
Print("S has size ");
Print(Size(S));
Print(" and there are ");
Print(Size(G));
Print(" units in S.\n\n");

# Print out the order of each unit.
for u in Elements(S) do
   if IsUnit(S,u) then
      Print(" ");
      Print(Order(u));
      Print(" ");
   fi;
od;

# [size,GAP group id] https://groupprops.subwiki.org/wiki/Groups_of_order_8
# We want (and get) group id [8,4].
Print("\n\n Group ID: ");
Print(IdGroup(G));
Print(" is the quaternions.");
```

6.2 Realizing Dic_2 in Characteristic 4

This is GAP code [GAP] that constructs a ring of characteristic 4 whose group of units is Dic_2 (i.e., the quaternion group of order 8). In particular, $R = \mathbb{Z}_4[\mathrm{Dic}_2]$, $I = (1 + a + x + ax, 1 + x^2)$, and $S = R/I$ has Dic_2 as its group of units.

```
# GAP CODE BEGINS HERE.
T := EmptySCTable(8,0);;
```

```
# 1=1, 2=i, 3=j, 4=k, 5=-1, 6=-i, 7=-j, 8=-k
for i in [1..8] do
   # 1*Y = Y and Y*1 = Y
   SetEntrySCTable(T,1,i,[1,i]);
   SetEntrySCTable(T,i,1,[1,i]);
od;;

# i*Y = ...
SetEntrySCTable(T,2,2,[1,5]);
SetEntrySCTable(T,2,3,[1,4]);
SetEntrySCTable(T,2,4,[1,7]);
SetEntrySCTable(T,2,5,[1,6]);
SetEntrySCTable(T,2,6,[1,1]);
SetEntrySCTable(T,2,7,[1,8]);
SetEntrySCTable(T,2,8,[1,3]);

# j*Y = ...
SetEntrySCTable(T,3,2,[1,8]);
SetEntrySCTable(T,3,3,[1,5]);
SetEntrySCTable(T,3,4,[1,2]);
SetEntrySCTable(T,3,5,[1,7]);
SetEntrySCTable(T,3,6,[1,4]);
SetEntrySCTable(T,3,7,[1,1]);
SetEntrySCTable(T,3,8,[1,6]);

# k*Y = ...
SetEntrySCTable(T,4,2,[1,3]);
SetEntrySCTable(T,4,3,[1,6]);
SetEntrySCTable(T,4,4,[1,5]);
SetEntrySCTable(T,4,5,[1,8]);
SetEntrySCTable(T,4,6,[1,7]);
SetEntrySCTable(T,4,7,[1,2]);
SetEntrySCTable(T,4,8,[1,1]);

# -1*Y = ...
SetEntrySCTable(T,5,2,[1,6]);
SetEntrySCTable(T,5,3,[1,7]);
SetEntrySCTable(T,5,4,[1,8]);
SetEntrySCTable(T,5,5,[1,1]);
SetEntrySCTable(T,5,6,[1,2]);
SetEntrySCTable(T,5,7,[1,3]);
SetEntrySCTable(T,5,8,[1,4]);

# -i*Y = ...
```

```
SetEntrySCTable(T,6,2,[1,1]);
SetEntrySCTable(T,6,3,[1,8]);
SetEntrySCTable(T,6,4,[1,3]);
SetEntrySCTable(T,6,5,[1,2]);
SetEntrySCTable(T,6,6,[1,5]);
SetEntrySCTable(T,6,7,[1,4]);
SetEntrySCTable(T,6,8,[1,7]);

# -j*Y = ...
SetEntrySCTable(T,7,2,[1,4]);
SetEntrySCTable(T,7,3,[1,1]);
SetEntrySCTable(T,7,4,[1,6]);
SetEntrySCTable(T,7,5,[1,3]);
SetEntrySCTable(T,7,6,[1,8]);
SetEntrySCTable(T,7,7,[1,5]);
SetEntrySCTable(T,7,8,[1,2]);

# -k*Y = ...
SetEntrySCTable(T,8,2,[1,7]);
SetEntrySCTable(T,8,3,[1,2]);
SetEntrySCTable(T,8,4,[1,1]);
SetEntrySCTable(T,8,5,[1,4]);
SetEntrySCTable(T,8,6,[1,3]);
SetEntrySCTable(T,8,7,[1,6]);
SetEntrySCTable(T,8,8,[1,5]);

# Additive orders of elements
TO := [4,4,4,4,4,4,4,4];;

# Denote 1 as e, -1 as ne, -i as ni, etc.
TL := ["e","i","j","k","ne","ni","nj","nk"];;

# This is Z_4[Dic_2]
R := RingByStructureConstants(TO,T,TL);

GN := GeneratorsOfRing(R);

G := Units(R);

Print("R has size ");
Print(Size(R));
Print(" and there are ");
Print(Size(G));
Print(" units of R.\n\n");
```

```
# S = Z_4[Dic_2]/(e+ne,e+i+j+k) - we force e+ne = 1+(-1) = 0  and 1+i+j+k = 0
I := Ideal(R,[GN[1]+GN[5],GN[1]+GN[2]+GN[3]+GN[4]]);
S := R/I;

G := Units(S);

Print("S has size ");
Print(Size(S));
Print(" and there are ");
Print(Size(G));
Print(" units of S.\n\n");

# Print out the order of each unit.
for u in Elements(S) do
   if IsUnit(S,u) then
      Print(" ");
      Print(Order(u));
      Print(" ");
   fi;
od;

# [size,GAP group id] https://groupprops.subwiki.org/wiki/Groups_of_order_8
# We want (and get) group id [8,4].
Print("\n\n Group ID: ");
Print(IdGroup(G));
Print(" is the quaternions.");
```

6.3 Realizing Dic_3 in Characteristic 2 is Impossible

This is GAP code [GAP] that constructs the group ring of characteristic 2, $\mathbb{Z}_2[\mathrm{Dic}_3]$. We then consider relations that must hold along with an arbitrary additional relation. No such relation yields Dic_3 as the group of units. Therefore, Dic_3 cannot be realized in characteristic 2.

```
#
# Use "Read("./Desktop/FILENAME.XXX");"
# to read in code.
#

# GAP CODE BEGINS HERE.
T := EmptySCTable(12,0);;

# 1=1, 2=a, 3=a^2, ..., 7=x, 8=ax, ..., 12=a^5x
# so i=1,...,6 is a^{i-1} and i=7,...,12 is a^{i-7}x
for i in [1..6] do
```

```
   for j in [1..6] do
      # a^(i-1)*a^(j-1) = a^{i+j-2 mod 6}
      SetEntrySCTable(T,i,j,[1,((i+j-2) mod 6)+1]);
      # +1 to go from 0..5 to 1..6 = a's

      # a^(i-1)*a^(j-1)x = a^{i+j-2 mod 6}x
      SetEntrySCTable(T,i,j+6,[1,((i+j-2) mod 6)+7]);
      # +7 to go from 0..5 to 7..12 = ax's

      # a^{i-1}x*a^{j-1} = a^{6+(i-1)-(j-1) mod 6}x since xa^{-1}=ax implies
      xa^k=xa^{k-6}=a^{6-k}x
      SetEntrySCTable(T,i+6,j,[1,((6+(i-1)-(j-1)) mod 6)+7]);

      # a^{i-1}x*a^{j-1}*x = a^{6+(i-1)-(j-1) mod 6}x^2
      = a^{6+(i-1)-(j-1)+3 mod 6} since x^2=a^3
      SetEntrySCTable(T,i+6,j+6,[1,((6+(i-1)-(j-1)+3) mod 6)+1]);
   od;;
od;;

# Additive orders of elements
TO := [2,2,2,2,2,2,2,2,2,2,2,2];;

TL := ["e","a","a2","a3","a4","a5","x","ax","a2x","a3x","a4x","a5x"];;

# This is Z_2[Dic_3]
R := RingByStructureConstants(TO,T,TL);

GN := GeneratorsOfRing(R);

# The elements of Z_2[Dic_3]...
ElementsR := Elements(R);

# Our known relations...
REL1 := GN[1]+GN[2]+GN[4]+GN[5];
REL2 := GN[1]+GN[4]+GN[7]+GN[10];

I := Ideal(R,[REL1,REL2]);
S := R/I;

G := Units(S);

Print("We must have 1+a+a^3+a^4=0 and 1+a^3+x+a^3x=0 in our ring.\n\n");
Print("If I=(these two elements), then S=R/I has ");
Print(Size(S));
Print(" elements and there are ");
```

```
Print(Size(G));
Print(" units in S.\n");

# Gives [24,5] = [size,GAP group id]
# https://groupprops.subwiki.org/wiki/Groups_of_order_12 we want [12,1].
Print("The units of S have group id: ");
Print(IdGroup(G));
Print(", but we are looking for id: [12,1] (Dic_3).\n\n");

# New helper element.
x := GN[1]+GN[2]+GN[3]+GN[8]+GN[9];

REL3a := x+GN[1];
REL3b := x+GN[4];

Ja := Ideal(R,[REL1,REL2,REL3a]);
Jb := Ideal(R,[REL1,REL2,REL3b]);

Print("Consider x = 1+a+a^2+ax+a^2x. We compute x^2 and get: ");
Print(x^2);
Print("\n");
Print("Notice that since ax+a^4x=1+a^3 and a^2x+a^5x=1+a^3 this is
1+1+a^3+1+a^3=1.\n");
Print("Thus since x^2=1, x must be an element of order 1 or 2. Therefore,
x=1 or x=a^3.\n\n");

Print("Case 1: x=1. Then we get an additional relation x=1 so
a+a^2+ax+a^2x=0.\n");
Print("We create an ideal Ja = I + (this new relation) and check out R/Ja.\n");

Print("R/Ja has ");
Print(Size(R/Ja));
Print(" elements and thus is too small to accomodate Dic_3.\n\n");

Print("Case 2: x=a^3. Then we get an additional relation x=a^3 so
1+a+a^2+a^3+ax+a^2x=0.\n");
Print("We create an ideal Jb = I + (this new relation) and check out R/Jb.\n");

Print("R/Jb has ");
Print(Size(R/Jb));
Print(" elements and thus is too small to accommodate Dic_3.\n\n");

Print("Since Dic_3 would have to be realized by a quotient of one of
these\n");
Print("quotient rings, we cannot realize Dic_3 as the group of units in
```

```
char 2!\n");
```

6.4 Realizing Dic_3 in Characteristic 4 is Impossible

This is GAP code [GAP] that constructs the group ring of characteristic 2, $\mathbb{Z}_4[\mathrm{Dic}_3]/(a^3+1)$. We then consider relations that must hold along with a final pair of relations (one of which must hold). Both alternatives fail to yield Dic_3 as the group of units of our ring. Therefore, Dic_3 cannot be realized in characteristic 4.

```
# GAP CODE BEGINS HERE.
T := EmptySCTable(6,0);;

# 1=1, 2=a, 3=a^2, 4=x, 5=ax, 6=a^2x
for i in [1..6] do
   # 1*Y = Y and Y*1 = Y
   SetEntrySCTable(T,1,i,[1,i]);
   SetEntrySCTable(T,i,1,[1,i]);
od;;

# a*Y = ...
SetEntrySCTable(T,2,2,[1,3]);
SetEntrySCTable(T,2,3,[-1,1]);
SetEntrySCTable(T,2,4,[1,5]);
SetEntrySCTable(T,2,5,[1,6]);
SetEntrySCTable(T,2,6,[-1,4]);

# a^2*Y = ...
SetEntrySCTable(T,3,2,[-1,1]);
SetEntrySCTable(T,3,3,[-1,2]);
SetEntrySCTable(T,3,4,[1,6]);
SetEntrySCTable(T,3,5,[-1,4]);
SetEntrySCTable(T,3,6,[-1,5]);

# x*Y = ...
SetEntrySCTable(T,4,2,[-1,6]);
SetEntrySCTable(T,4,3,[-1,5]);
SetEntrySCTable(T,4,4,[-1,1]);
SetEntrySCTable(T,4,5,[1,3]);
SetEntrySCTable(T,4,6,[1,2]);

# ax*Y = ...
SetEntrySCTable(T,5,2,[1,4]);
SetEntrySCTable(T,5,3,[-1,6]);
SetEntrySCTable(T,5,4,[-1,2]);
SetEntrySCTable(T,5,5,[-1,1]);
```

```
SetEntrySCTable(T,5,6,[1,3]);

# a^2x*Y = ...
SetEntrySCTable(T,6,2,[1,5]);
SetEntrySCTable(T,6,3,[1,4]);
SetEntrySCTable(T,6,4,[-1,3]);
SetEntrySCTable(T,6,5,[-1,2]);
SetEntrySCTable(T,6,6,[-1,1]);

# Additive orders of elements
TO := [4,4,4,4,4,4];;

TL := ["e","a","a2","x","ax","a2x"];;

# This is Z_4[Dic_3]/(a^3+1)
# So we've already forced the a^3=x^2=-1 relation.
R := RingByStructureConstants(TO,T,TL);

GN := GeneratorsOfRing(R);

# Must have 2+2x=0
I := Ideal(R,[2*GN[1]+2*GN[4]]);

S := R/I;

G := Units(S);

Print("We must have 2+2x=0 in our ring. If I=(2+2x), then S=R/I has size ");
Print(Size(S));
Print(" and there are ");
Print(Size(G));
Print(" units of S.\n\n");

Print("(a+a^2+ax+a^2x)^2 = ");
Print((GN[2]+GN[3]+GN[5]+GN[6])^2);
Print(", so subject to the required relation 2+2a=0, this is 0.\n\n");

J := Ideal(R,[2*GN[1]+2*GN[4],GN[2]+GN[3]+GN[5]+GN[6]]);
S := R/J;
G := Units(S);

Print("We must have 2+2x=0 in our ring. What if we also have a+a^2+ax+a^2x?
J=(2+2x,a+a^2+ax+a^2x), then S=R/J has size ");
Print(Size(S));
Print(" and there are ");
```

```
Print(Size(G));
Print(" units of S.\n\n");


J := Ideal(R,[2*GN[1]+2*GN[4],2*GN[1]+GN[2]+GN[3]+GN[5]+GN[6]]);
S := R/J;
G := Units(S);

Print("We must have 2+2x=0 in our ring. What if we also have 2+a+a^2+ax+a^2x?
J=(2+2x,2+a+a^2+ax+a^2x), then S=R/J has size ");
Print(Size(S));
Print(" and there are ");
Print(Size(G));
Print(" units of S.\n\n");

Print("Since either a+a^2+ax+a^2x=0 or 2+a+a^2+ax+a^2x=0 and we do not
realize\n");
Print("Dic_3 either way, we have that Dic_3 cannot be realized in
characteristic 4.\n");
```

7 Bibliography

References

[CL1] S. Chebolu, K. Lockridge, "Fuchs' problem for dihedral groups", *Journal of Pure and Applied Algebra*, Vol. 221, Iss. 4 (2016).

[CL2] S. Chebolu, K. Lockridge, "Fuchs' problem for p-groups", *Journal of Pure and Applied Algebra*, Vol. 223, Iss. 11 (2019).

[DO1] Christopher Davis and Tommy Occhipinti, "Which alternating and symmetric groups are unit groups?" *Journal of Algebra and Its Applications*. Vol. 13, No. 3 (2014).

[DO2] Christopher Davis and Tommy Occhipinti, "Which finite simple groups are unit groups?" *Journal of Pure and Applied Algebra*. Vol. 13, No. 3 (2014).

[D] S. Z. Ditor, "On the group of units of a ring," Amer. Math. Monthly 78 (1971). 522–523.

[DF] D. S. Dummit, R. M. Foote, *Abstract Algebra*, 3^{rd} ed., John Wiley & Sons, 2004.

[Fr] J.B. Fraleigh, *A First Course in Abstract Algebra*, 7^{th} ed., Addison Wesley, 2003.

[Fu] L. Fuchs, "Abelian groups", *International Series of Monographs on Pure and Applied Mathematics*, Pergamon Press, New York-Oxford-London-Paris, 1960.

[Ga] J. Gallian, *Contemporary Abstract Algebra*, 8^{th} ed., Cengage Learning, 2012.

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.0*; 2020, `https://www.gap-system.org`.

[Gi] R. Gilmer, "Finite rings having a cyclic multiplicative group of units," *American Jounral of Mathematics*, 1963, 447-452.

[Hu] T. W. Hungerford. *Algebra*, Springer-Verlag, 1974.

[PS] K. R. Pearson and J. E. Schneider, "Rings with a cyclic group of units," *Journal of Algebra*. Vol. 16 (1970).

[SW] E. Swartz and N. Werner, "Fuchs' problem for 2-groups," *Journal of Algebra* Vol. 556 (2020).