Illinois State University Undergraduate Colloquium in Mathematics – March 23, 2022

Fuchs' Problem for Dicyclic Groups

Bill Cook $\Longleftrightarrow$ cookwj@appstate.edu
Appalachian State University
Boone, North Carolina

Joint work with Joshua Carr and Lindsey Wise.

Thursday, March 23rd, 2021

Every ring with identity has an associated group of units. Fuchs' problem seeks to determine which group structures can appear as groups of units. In this talk, we will discuss Fuchs' problem in general and then focus on groups of small orders and Dicyclic groups.

Background:

A ring R is an Abelian group under addition equipped with an associative multiplication and obeys distributive laws.

We assume that all of our rings are rings with 1.

- Closure: If $a, b \in R$, then $a + b, ab \in R$
- Associativity: If $a, b, c \in R$, then $(a + b) + c = a + (b + c)$ and $a(bc) = (ab)c$.
- Identity: There are $0, 1 \in R$ such that if $a \in R$, then $a + 0 = a = 0 + a$ and $1a = a = a1$.
- (Additive) Inverses: For all $a \in R$ there is some $-a \in R$ such that $a + (-a) = 0 = (-a) + a$.
- Commutativity (Addition): If $a, b \in R$, then $a + b = b + a$.
- Distributivity: If $a, b, c \in R$, then $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Background:

Let R be a ring. We say $u \in R$ is a unit if it has a multiplicative inverse: there exists some $b \in R$ such that $\boxed{uu^{-1} = 1 = u^{-1}u}$.

Let $\boxed{R^\times} = \{u \in R \mid u \text{ is a unit in } R\}$ be the group of units. This is a group under multiplication since...

- Closure – A unit times a unit is a unit: $(ab)^{-1} = b^{-1}a^{-1}$.
- Associativity – Multiplication is associative: $a(bc) = (ab)c$.
- Identity – The multiplicative identity, 1, is a unit: $1^{-1} = 1$.
- Inverses – The inverse of a unit is a unit: $(u^{-1})^{-1} = u$.

Background:

Let R be a ring. We say $u \in R$ is a unit if it has a multiplicative inverse: there exists some $b \in R$ such that $\boxed{uu^{-1} = 1 = u^{-1}u}$.

Let $\boxed{R^\times} = \{u \in R \mid u \text{ is a unit in } R\}$ be the group of units. This is a group under multiplication since...

- Closure – A unit times a unit is a unit: $(ab)^{-1} = b^{-1}a^{-1}$.
- Associativity – Multiplication is associative: $a(bc) = (ab)c$.
- Identity – The multiplicative identity, 1, is a unit: $1^{-1} = 1$.
- Inverses – The inverse of a unit is a unit: $(u^{-1})^{-1} = u$.

Examples: $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{R}[x]^\times = \mathbb{R}^\times = \mathbb{R}_{\neq 0}$, $(\mathbb{R}^{n \times n})^\times = \mathrm{GL}_n(\mathbb{R})$,

Background:

Let R be a ring. We say $u \in R$ is a unit if it has a multiplicative inverse: there exists some $b \in R$ such that $\boxed{uu^{-1} = 1 = u^{-1}u}$.

Let $\boxed{R^\times} = \{u \in R \mid u \text{ is a unit in } R\}$ be the group of units.
This is a group under multiplication since...

- Closure – A unit times a unit is a unit: $(ab)^{-1} = b^{-1}a^{-1}$.
- Associativity – Multiplication is associative: $a(bc) = (ab)c$.
- Identity – The multiplicative identity, 1, is a unit: $1^{-1} = 1$.
- Inverses – The inverse of a unit is a unit: $(u^{-1})^{-1} = u$.

Examples: $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{R}[x]^\times = \mathbb{R}^\times = \mathbb{R}_{\neq 0}$, $(\mathbb{R}^{n \times n})^\times = \mathrm{GL}_n(\mathbb{R})$,
$\mathbb{Z}_n^\times = U(\mathbb{Z}_n) = U(n) = \{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$

Background:

Let R be a ring. We say $u \in R$ is a unit if it has a multiplicative inverse: there exists some $b \in R$ such that $\boxed{uu^{-1} = 1 = u^{-1}u}$.

Let $\boxed{R^\times} = \{u \in R \mid u \text{ is a unit in } R\}$ be the group of units.
This is a group under multiplication since...

- Closure – A unit times a unit is a unit: $(ab)^{-1} = b^{-1}a^{-1}$.
- Associativity – Multiplication is associative: $a(bc) = (ab)c$.
- Identity – The multiplicative identity, 1, is a unit: $1^{-1} = 1$.
- Inverses – The inverse of a unit is a unit: $(u^{-1})^{-1} = u$.

Examples: $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{R}[x]^\times = \mathbb{R}^\times = \mathbb{R}_{\neq 0}$, $(\mathbb{R}^{n\times n})^\times = \mathrm{GL}_n(\mathbb{R})$,
$\mathbb{Z}_n^\times = U(\mathbb{Z}_n) = U(n) = \{k \in \mathbb{Z}_n \mid \gcd(k,n) = 1\}$

$U(10) = \{1, 3, 7, 9\}$
where $1^{-1} = 1$, $3^{-1} = 7$, $7^{-1} = 3$, and $9^{-1} = 9$.

Fuchs' Problem:

Which group structures can appear as unit groups? (Fuchs ≈1960)

Given a group G, is there a ring R such that $R^\times = G$?

We say the G is realizable as a unit group if there is some ring R such that $R^\times = G$.

Fuchs' Problem:

Which group structures can appear as unit groups? (Fuchs ≈1960)

Given a group G, is there a ring R such that $R^\times = G$?

We say the G is realizable as a unit group if there is some ring R such that $R^\times = G$.

Careful! This is not asking if G can appear among the units. For example, let R be any commutative ring. We can form the group ring, $R[G]$, and we have that $G \subseteq R[G]^\times$.

Fuchs' Problem:

Which group structures can appear as unit groups?

Given a group G, is there a ring R such that $R^\times = G$?

We say the G is realizable as a unit group if there is some ring R such that $R^\times = G$.

Examples: Notice $\{0\}^\times = \{0\}$ and $\mathbb{Z}_2^\times = \{1\}$ both realize the trivial group. Also, $\mathbb{Z}_3^\times = \{1, 2\} = \langle 2 \rangle \cong C_2$ realizes the cyclic group of order 2. Likewise, $\mathbb{Z}_5^\times = \{1, 2, 3, 4\} = \langle 2 \rangle \cong C_4$, $\mathbb{Z}_7^\times \cong C_6$, and $\mathbb{Z}_8^\times = \{1, 3, 5, 7\} \cong C_2 \times C_2$.

Fuchs' Problem:

Which group structures can appear as unit groups?

Given a group G, is there a ring R such that $R^\times = G$?

We say the G is realizable as a unit group if there is some ring R such that $R^\times = G$.

Examples: Notice $\{0\}^\times = \{0\}$ and $\mathbb{Z}_2^\times = \{1\}$ both realize the trivial group. Also, $\mathbb{Z}_3^\times = \{1, 2\} = \langle 2 \rangle \cong C_2$ realizes the cyclic group of order 2. Likewise, $\mathbb{Z}_5^\times = \{1, 2, 3, 4\} = \langle 2 \rangle \cong C_4$, $\mathbb{Z}_7^\times \cong C_6$, and $\mathbb{Z}_8^\times = \{1, 3, 5, 7\} \cong C_2 \times C_2$.

Finite Fields: There is a unique (up to isomorphism) field of order $q = p^k$ where p is prime and k is a positive integer. Call such a field $\mathbb{F}_q$.

Any finite subgroup of the multiplicative group of a field is cyclic, so $\mathbb{F}_q^\times = \mathbb{F}_q - \{0\} \cong C_{q-1}$. For example, $\mathbb{F}_4^\times \cong C_3$, $\mathbb{F}_8^\times \cong C_7$, and $\mathbb{F}_9^\times \cong C_8$.

Characteristic of a Ring:

For convenience, we let $\mathbb{Z}_0 = \mathbb{Z}$.

For any ring R, there exists some $n \in \mathbb{Z}_{\geq 0}$ such that R contains an isomorphic copy of $\mathbb{Z}_n$ called the prime subring of R.

$$\boxed{\mathrm{char}(R) = n}$$ is the characteristic of R

Examples: $\mathrm{char}(\mathbb{Z}) = 0$ and $\mathrm{char}(\mathbb{Z}_n) = n$

Characteristic of a Ring:

For convenience, we let $\mathbb{Z}_0 = \mathbb{Z}$.

For any ring R, there exists some $n \in \mathbb{Z}_{\geq 0}$ such that R contains an isomorphic copy of $\mathbb{Z}_n$ called the prime subring of R.

$$\boxed{\mathrm{char}(R) = n}$$ is the characteristic of R

Examples: $\mathrm{char}(\mathbb{Z}) = 0$ and $\mathrm{char}(\mathbb{Z}_n) = n$

Important Observation: Since 1 commutes with all R, so do additive powers of 1. Thus

the prime subring of R lies in the center of R.

Characteristic of a Ring:

For convenience, we let $\mathbb{Z}_0 = \mathbb{Z}$.

For any ring R, there exists some $n \in \mathbb{Z}_{\geq 0}$ such that R contains an isomorphic copy of $\mathbb{Z}_n$ called the prime subring of R.

$\boxed{\mathrm{char}(R) = n}$ is the characteristic of R

Examples: $\mathrm{char}(\mathbb{Z}) = 0$ and $\mathrm{char}(\mathbb{Z}_n) = n$

Important Observation: Since 1 commutes with all R, so do additive powers of 1. Thus

the prime subring of R lies in the center of R.

This implies that $\boxed{Z(R^\times) \text{ must contain a copy of } \mathbb{Z}_n^\times}$.

Characteristic of a Ring:

For convenience, we let $\mathbb{Z}_0 = \mathbb{Z}$.

For any ring R, there exists some $n \in \mathbb{Z}_{\geq 0}$ such that R contains an isomorphic copy of $\mathbb{Z}_n$ called the prime subring of R.

$$\boxed{\mathrm{char}(R) = n} \text{ is the characteristic of } R$$

Examples: $\mathrm{char}(\mathbb{Z}) = 0$ and $\mathrm{char}(\mathbb{Z}_n) = n$

Important Observation: Since 1 commutes with all R, so do additive powers of 1. Thus

the prime subring of R lies in the center of R.

This implies that $\boxed{Z(R^\times) \text{ must contain a copy of } \mathbb{Z}_n^\times}$.

Example: If $Z(R^\times) = \{1\}$, then either $R = \{0\}$ or $\mathrm{char}(R) = 2$ since $|\mathbb{Z}_n^\times| > 1$ for $n > 2$.

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.

Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ ($R = \{0\}$) and $n = 2$.

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.
Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ ($R = \{0\}$) and $n = 2$.
Proof #2: If $u \neq -u$, then units come in pairs.

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.
Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ ($R = \{0\}$) and $n = 2$.
Proof #2: If $u \neq -u$, then units come in pairs.

Example: We cannot realize C_5.

Suppose R realizes C_5 and say $R^\times = \langle u \rangle \cong C_5$. Since $|R^\times| = 5$ is odd, the characteristic of R must be 2 so that $x = -x$ for all $x \in R$.

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.

Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ ($R = \{0\}$) and $n = 2$.

Proof #2: If $u \neq -u$, then units come in pairs.

Example: We cannot realize C_5.

Suppose R realizes C_5 and say $R^\times = \langle u \rangle \cong C_5$. Since $|R^\times| = 5$ is odd, the characteristic of R must be 2 so that $x = -x$ for all $x \in R$. Notice that

$(1 + u^2 + u^3)^3 = u^9 + 3u^8 + 3u^7 + 4u^6 + 6u^5 + 3u^4 + 3u^3 + 3u^2 + 1$

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.
Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ ($R = \{0\}$) and $n = 2$.
Proof #2: If $u \neq -u$, then units come in pairs.

Example: We cannot realize C_5.

Suppose R realizes C_5 and say $R^\times = \langle u \rangle \cong C_5$. Since $|R^\times| = 5$ is odd, the characteristic of R must be 2 so that $x = -x$ for all $x \in R$. Notice that
$(1 + u^2 + u^3)^3 = u^9 + 3u^8 + 3u^7 + 4u^6 + 6u^5 + 3u^4 + 3u^3 + 3u^2 + 1$
$= u^9 + u^8 + u^7 + u^4 + u^3 + u^2 + 1$

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.
Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ ($R = \{0\}$) and $n = 2$.
Proof #2: If $u \neq -u$, then units come in pairs.

Example: We cannot realize C_5.

Suppose R realizes C_5 and say $R^\times = \langle u \rangle \cong C_5$. Since $|R^\times| = 5$ is odd, the characteristic of R must be 2 so that $x = -x$ for all $x \in R$. Notice that
$(1 + u^2 + u^3)^3 = u^9 + 3u^8 + 3u^7 + 4u^6 + 6u^5 + 3u^4 + 3u^3 + 3u^2 + 1$
$= u^9 + u^8 + u^7 + u^4 + u^3 + u^2 + 1 = 2u^4 + 2u^3 + 2u^2 + 1 = 1.$

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.
Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ ($R = \{0\}$) and $n = 2$.
Proof #2: If $u \neq -u$, then units come in pairs.

Example: We cannot realize C_5.

Suppose R realizes C_5 and say $R^\times = \langle u \rangle \cong C_5$. Since $|R^\times| = 5$ is odd, the characteristic of R must be 2 so that $x = -x$ for all $x \in R$. Notice that
$(1 + u^2 + u^3)^3 = u^9 + 3u^8 + 3u^7 + 4u^6 + 6u^5 + 3u^4 + 3u^3 + 3u^2 + 1$
$= u^9 + u^8 + u^7 + u^4 + u^3 + u^2 + 1 = 2u^4 + 2u^3 + 2u^2 + 1 = 1.$
Therefore, if $a = 1 + u^2 + u^3$, then $a^3 = 1$ so that $a^{-1} = a^2$.

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.
Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ ($R = \{0\}$) and $n = 2$.
Proof #2: If $u \neq -u$, then units come in pairs.

Example: We cannot realize C_5.

Suppose R realizes C_5 and say $R^\times = \langle u \rangle \cong C_5$. Since $|R^\times| = 5$ is odd, the characteristic of R must be 2 so that $x = -x$ for all $x \in R$. Notice that
$(1 + u^2 + u^3)^3 = u^9 + 3u^8 + 3u^7 + 4u^6 + 6u^5 + 3u^4 + 3u^3 + 3u^2 + 1$
$= u^9 + u^8 + u^7 + u^4 + u^3 + u^2 + 1 = 2u^4 + 2u^3 + 2u^2 + 1 = 1.$
Therefore, if $a = 1 + u^2 + u^3$, then $a^3 = 1$ so that $a^{-1} = a^2$. This means a is a unit of order 1 or 3.

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.
Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ ($R = \{0\}$) and $n = 2$.
Proof #2: If $u \neq -u$, then units come in pairs.

Example: We cannot realize C_5.

Suppose R realizes C_5 and say $R^\times = \langle u \rangle \cong C_5$. Since $|R^\times| = 5$ is odd, the characteristic of R must be 2 so that $x = -x$ for all $x \in R$. Notice that
$(1 + u^2 + u^3)^3 = u^9 + 3u^8 + 3u^7 + 4u^6 + 6u^5 + 3u^4 + 3u^3 + 3u^2 + 1$
$= u^9 + u^8 + u^7 + u^4 + u^3 + u^2 + 1 = 2u^4 + 2u^3 + 2u^2 + 1 = 1.$
Therefore, if $a = 1 + u^2 + u^3$, then $a^3 = 1$ so that $a^{-1} = a^2$. This means a is a unit of order 1 or 3. But $R^\times$ has order 5. Therefore, a's order is 1.

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.
Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ ($R = \{0\}$) and $n = 2$.
Proof #2: If $u \neq -u$, then units come in pairs.

Example: We cannot realize C_5.

Suppose R realizes C_5 and say $R^\times = \langle u \rangle \cong C_5$. Since $|R^\times| = 5$ is odd, the characteristic of R must be 2 so that $x = -x$ for all $x \in R$. Notice that
$(1 + u^2 + u^3)^3 = u^9 + 3u^8 + 3u^7 + 4u^6 + 6u^5 + 3u^4 + 3u^3 + 3u^2 + 1$
$= u^9 + u^8 + u^7 + u^4 + u^3 + u^2 + 1 = 2u^4 + 2u^3 + 2u^2 + 1 = 1$.
Therefore, if $a = 1 + u^2 + u^3$, then $a^3 = 1$ so that $a^{-1} = a^2$. This means a is a unit of order 1 or 3. But $R^\times$ has order 5. Therefore, a's order is 1. Thus $a = 1$ so $u^2 + u^3 = 0$

We Cannot Realize Cyclic Order 5:

Theorem: Non-trivial groups of odd order can only be realized in characteristic 2.
Proof #1: $\mathbb{Z}_n^\times$ only has odd order for $n = 1$ $(R = \{0\})$ and $n = 2$.
Proof #2: If $u \neq -u$, then units come in pairs.

Example: We cannot realize C_5.

Suppose R realizes C_5 and say $R^\times = \langle u \rangle \cong C_5$. Since $|R^\times| = 5$ is odd, the characteristic of R must be 2 so that $x = -x$ for all $x \in R$. Notice that
$(1 + u^2 + u^3)^3 = u^9 + 3u^8 + 3u^7 + 4u^6 + 6u^5 + 3u^4 + 3u^3 + 3u^2 + 1$
$= u^9 + u^8 + u^7 + u^4 + u^3 + u^2 + 1 = 2u^4 + 2u^3 + 2u^2 + 1 = 1.$
Therefore, if $a = 1 + u^2 + u^3$, then $a^3 = 1$ so that $a^{-1} = a^2$. This means a is a unit of order 1 or 3. But $R^\times$ has order 5. Therefore, a's order is 1. Thus $a = 1$ so $u^2 + u^3 = 0$ so $u^2 = u^3$ so $1 = u$ (contradiction).

Group Rings:

Let R be a commutative ring (with $1 \neq 0$).

$$R[G] = \{r_1 g_1 + \cdots + r_\ell g_\ell \mid r_1, \ldots, r_\ell \in R \text{ and } g_1, \ldots, g_\ell \in G\}$$

Add coordinatewise and extend G's multiplication "linearly". Then $R[G]$ is the group ring of G with coefficients in R.

Example: Let $D_3 = \langle a, x \mid a^3 = 1, x^2 = 1, xa = a^{-1}x\rangle$ $= \{1, a, a^2, x, ax, a^2x\}$ be the Dihedral group of order 6. The group ring of D_3 with coefficients in $\mathbb{Z}_4$ is a ring with $4^6 = 4096$ elements.

$$\mathbb{Z}_4[D_3] = \{r_1 + r_2 a + r_3 a^2 + r_4 x + r_5 ax + r_6 a^2 x \mid r_1, \ldots, r_6 \in \mathbb{Z}_4\}$$

$(2 + a + 3x) + (3 + 2a^2 + x)$

Group Rings:

Let R be a commutative ring (with $1 \neq 0$).

$$R[G] = \{r_1 g_1 + \cdots + r_\ell g_\ell \mid r_1, \ldots, r_\ell \in R \text{ and } g_1, \ldots, g_\ell \in G\}$$

Add coordinatewise and extend G's multiplication "linearly". Then $R[G]$ is the group ring of G with coefficients in R.

Example: Let $D_3 = \langle a, x \mid a^3 = 1, x^2 = 1, xa = a^{-1}x \rangle$ $= \{1, a, a^2, x, ax, a^2x\}$ be the Dihedral group of order 6. The group ring of D_3 with coefficients in $\mathbb{Z}_4$ is a ring with $4^6 = 4096$ elements.

$$\mathbb{Z}_4[D_3] = \{r_1 + r_2 a + r_3 a^2 + r_4 x + r_5 ax + r_6 a^2 x \mid r_1, \ldots, r_6 \in \mathbb{Z}_4\}$$

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

Group Rings:

Let R be a commutative ring (with $1 \neq 0$).

$$R[G] = \{r_1 g_1 + \cdots + r_\ell g_\ell \mid r_1, \ldots, r_\ell \in R \text{ and } g_1, \ldots, g_\ell \in G\}$$

Add coordinatewise and extend G's multiplication "linearly". Then $R[G]$ is the group ring of G with coefficients in R.

Example: Let $D_3 = \langle a, x \mid a^3 = 1, x^2 = 1, xa = a^{-1}x \rangle$ $= \{1, a, a^2, x, ax, a^2x\}$ be the Dihedral group of order 6. The group ring of D_3 with coefficients in $\mathbb{Z}_4$ is a ring with $4^6 = 4096$ elements.

$$\mathbb{Z}_4[D_3] = \{r_1 + r_2 a + r_3 a^2 + r_4 x + r_5 ax + r_6 a^2 x \mid r_1, \ldots, r_6 \in \mathbb{Z}_4\}$$

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

Group Rings:

Let R be a commutative ring (with $1 \neq 0$).

$$R[G] = \{r_1 g_1 + \cdots + r_\ell g_\ell \mid r_1, \ldots, r_\ell \in R \text{ and } g_1, \ldots, g_\ell \in G\}$$

Add coordinatewise and extend G's multiplication "linearly". Then $R[G]$ is the group ring of G with coefficients in R.

Example: Let $D_3 = \langle a, x \mid a^3 = 1, x^2 = 1, xa = a^{-1}x \rangle$ $= \{1, a, a^2, x, ax, a^2x\}$ be the Dihedral group of order 6. The group ring of D_3 with coefficients in $\mathbb{Z}_4$ is a ring with $4^6 = 4096$ elements.

$$\mathbb{Z}_4[D_3] = \{r_1 + r_2 a + r_3 a^2 + r_4 x + r_5 ax + r_6 a^2 x \mid r_1, \ldots, r_6 \in \mathbb{Z}_4\}$$

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

$$(1 + 2a^2 + x)(3a + 2ax)$$

Group Rings:

Let R be a commutative ring (with $1 \neq 0$).

$$R[G] = \{r_1 g_1 + \cdots + r_\ell g_\ell \mid r_1, \ldots, r_\ell \in R \text{ and } g_1, \ldots, g_\ell \in G\}$$

Add coordinatewise and extend G's multiplication "linearly". Then $R[G]$ is the group ring of G with coefficients in R.

Example: Let $D_3 = \langle a, x \mid a^3 = 1, x^2 = 1, xa = a^{-1}x \rangle$ $= \{1, a, a^2, x, ax, a^2x\}$ be the Dihedral group of order 6. The group ring of D_3 with coefficients in $\mathbb{Z}_4$ is a ring with $4^6 = 4096$ elements.

$$\mathbb{Z}_4[D_3] = \{r_1 + r_2 a + r_3 a^2 + r_4 x + r_5 ax + r_6 a^2 x \mid r_1, \ldots, r_6 \in \mathbb{Z}_4\}$$

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

$$(1 + 2a^2 + x)(3a + 2ax) = (1 + 2a^2 + x)3a + (1 + 2a^2 + x)2ax$$

Group Rings:

Let R be a commutative ring (with $1 \neq 0$).

$$R[G] = \{r_1g_1 + \cdots + r_\ell g_\ell \mid r_1, \ldots, r_\ell \in R \text{ and } g_1, \ldots, g_\ell \in G\}$$

Add coordinatewise and extend G's multiplication "linearly". Then $R[G]$ is the group ring of G with coefficients in R.

Example: Let $D_3 = \langle a, x \mid a^3 = 1, x^2 = 1, xa = a^{-1}x\rangle$ $= \{1, a, a^2, x, ax, a^2x\}$ be the Dihedral group of order 6. The group ring of D_3 with coefficients in $\mathbb{Z}_4$ is a ring with $4^6 = 4096$ elements.

$$\mathbb{Z}_4[D_3] = \{r_1 + r_2a + r_3a^2 + r_4x + r_5ax + r_6a^2x \mid r_1, \ldots, r_6 \in \mathbb{Z}_4\}$$

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

$$(1 + 2a^2 + x)(3a + 2ax) = (1 + 2a^2 + x)3a + (1 + 2a^2 + x)2ax =$$
$$3a + 6a^3 + 3xa + 2ax + 4a^3x + 2xax$$

Group Rings:

Let R be a commutative ring (with $1 \neq 0$).

$$R[G] = \{r_1 g_1 + \cdots + r_\ell g_\ell \mid r_1, \ldots, r_\ell \in R \text{ and } g_1, \ldots, g_\ell \in G\}$$

Add coordinatewise and extend G's multiplication "linearly". Then $R[G]$ is the group ring of G with coefficients in R.

Example: Let $D_3 = \langle a, x \mid a^3 = 1, x^2 = 1, xa = a^{-1}x\rangle = \{1, a, a^2, x, ax, a^2x\}$ be the Dihedral group of order 6. The group ring of D_3 with coefficients in $\mathbb{Z}_4$ is a ring with $4^6 = 4096$ elements.

$$\mathbb{Z}_4[D_3] = \{r_1 + r_2 a + r_3 a^2 + r_4 x + r_5 ax + r_6 a^2 x \mid r_1, \ldots, r_6 \in \mathbb{Z}_4\}$$

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

$$(1 + 2a^2 + x)(3a + 2ax) = (1 + 2a^2 + x)3a + (1 + 2a^2 + x)2ax =$$
$$3a + 6a^3 + 3xa + 2ax + 4a^3x + 2xax = 3a + 2 + 3a^2x + 2ax + 0 + 2a^2$$

Group Rings:

Let R be a commutative ring (with $1 \neq 0$).

$$R[G] = \{r_1 g_1 + \cdots + r_\ell g_\ell \mid r_1, \ldots, r_\ell \in R \text{ and } g_1, \ldots, g_\ell \in G\}$$

Add coordinatewise and extend G's multiplication "linearly". Then $R[G]$ is the group ring of G with coefficients in R.

Example: Let $D_3 = \langle a, x \mid a^3 = 1, x^2 = 1, xa = a^{-1}x \rangle$ $= \{1, a, a^2, x, ax, a^2x\}$ be the Dihedral group of order 6. The group ring of D_3 with coefficients in $\mathbb{Z}_4$ is a ring with $4^6 = 4096$ elements.

$$\mathbb{Z}_4[D_3] = \{r_1 + r_2 a + r_3 a^2 + r_4 x + r_5 ax + r_6 a^2 x \mid r_1, \ldots, r_6 \in \mathbb{Z}_4\}$$

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

$$(1 + 2a^2 + x)(3a + 2ax) = (1 + 2a^2 + x)3a + (1 + 2a^2 + x)2ax = 3a + 6a^3 + 3xa + 2ax + 4a^3x + 2xax = 3a + 2 + 3a^2x + 2ax + 0 + 2a^2 = 2 + 3a + 2a^2 + 2ax + 3a^2x$$

Summary Basic Results:

Theorem: Let G be a group and n a non-negative integer. Suppose G can be realized by a ring R of characteristic n.

- There is an ideal I of $\mathbb{Z}_n[G]$ such that $(\mathbb{Z}_n[G]/I)^\times \cong G$. Moreover, G can be realized by a finite ring if and only if G is finite and realizable in a positive characteristic.
- Let S be the subring of R generated by the units G. Then $S^\times = G$.
- If a ring realizes an Abelian group, one of its commutative subrings realizes that group.
- If G is cyclic, then there is some ideal I of $\mathbb{Z}_n[x]$ such that $(\mathbb{Z}_n[x]/I)^\times \cong G$.
- Units of the prime subring are central units: $\mathbb{Z}_n^\times \subseteq Z(R^\times) = Z(G)$.
- We have -1 is a unit of order 1 or 2. Moreover, -1 is a unit of order 2 if and only if the characteristic of R is not 1 or 2.
- Non-trivial realizable groups of odd order must be realized in characteristic 2.

Using our Tools:

Example: Cyclic groups C_n where $n = 5, 11$, or 13 cannot be realized.

Using our Tools:

Example: Cyclic groups C_n where $n = 5, 11,$ or 13 cannot be realized.

Suppose R realizes C_n. These groups have odd order so we must work in characteristic 2.

Using our Tools:

Example: Cyclic groups C_n where $n = 5, 11$, or 13 cannot be realized.

Suppose R realizes C_n. These groups have odd order so we must work in characteristic 2.
Note that in $\mathbb{Z}_2[x]$ for $n = 5, 11$, and 13, the factorization of $x^n - 1 = x^n + 1$ into irreducibles is $(x+1)(x^{n-1} + \cdots + x + 1)$.

Using our Tools:

Example: Cyclic groups C_n where $n = 5, 11$, or 13 cannot be realized.

Suppose R realizes C_n. These groups have odd order so we must work in characteristic 2.
Note that in $\mathbb{Z}_2[x]$ for $n = 5, 11$, and 13, the factorization of $x^n - 1 = x^n + 1$ into irreducibles is $(x+1)(x^{n-1} + \cdots + x + 1)$.
Thus can assume R is a quotient of

$$\mathbb{Z}_2[x]/(x^n - 1) \cong \mathbb{Z}_2[x]/(x+1) \times \mathbb{Z}_2[x]/(x^{n-1} + \cdots + x + 1)$$

Using our Tools:

Example: Cyclic groups C_n where $n = 5, 11$, or 13 cannot be realized.

Suppose R realizes C_n. These groups have odd order so we must work in characteristic 2.
Note that in $\mathbb{Z}_2[x]$ for $n = 5, 11$, and 13, the factorization of $x^n - 1 = x^n + 1$ into irreducibles is $(x+1)(x^{n-1} + \cdots + x + 1)$.
Thus can assume R is a quotient of

$$\mathbb{Z}_2[x]/(x^n - 1) \cong \mathbb{Z}_2[x]/(x+1) \times \mathbb{Z}_2[x]/(x^{n-1} + \cdots + x + 1) \cong \mathbb{F}_2 \times \mathbb{F}_{2^{n-1}}$$

Using our Tools:

Example: Cyclic groups C_n where $n = 5, 11$, or 13 cannot be realized.

Suppose R realizes C_n. These groups have odd order so we must work in characteristic 2.
Note that in $\mathbb{Z}_2[x]$ for $n = 5, 11$, and 13, the factorization of $x^n - 1 = x^n + 1$ into irreducibles is $(x+1)(x^{n-1} + \cdots + x + 1)$.
Thus can assume R is a quotient of

$$\mathbb{Z}_2[x]/(x^n - 1) \cong \mathbb{Z}_2[x]/(x+1) \times \mathbb{Z}_2[x]/(x^{n-1} + \cdots + x + 1) \cong \mathbb{F}_2 \times \mathbb{F}_{2^{n-1}}$$

Thus R must be isomorphic to $\{0\}$, $\mathbb{F}_2$, $\mathbb{F}_{2^{n-1}}$, or $\mathbb{F}_2 \times \mathbb{F}_{2^{n-1}}$.

Using our Tools:

Example: Cyclic groups C_n where $n = 5, 11$, or 13 cannot be realized.

Suppose R realizes C_n. These groups have odd order so we must work in characteristic 2.
Note that in $\mathbb{Z}_2[x]$ for $n = 5, 11$, and 13, the factorization of $x^n - 1 = x^n + 1$ into irreducibles is $(x+1)(x^{n-1} + \cdots + x + 1)$.
Thus can assume R is a quotient of

$$\mathbb{Z}_2[x]/(x^n - 1) \cong \mathbb{Z}_2[x]/(x+1) \times \mathbb{Z}_2[x]/(x^{n-1} + \cdots + x + 1) \cong \mathbb{F}_2 \times \mathbb{F}_{2^{n-1}}$$

Thus R must be isomorphic to $\{0\}$, $\mathbb{F}_2$, $\mathbb{F}_{2^{n-1}}$, or $\mathbb{F}_2 \times \mathbb{F}_{2^{n-1}}$.
But none of these realize C_n.

What is known?

Cyclic Groups: The work of Gilmer (1963) and then Pearson & Schneider (1970) settled which cyclic groups can and cannot be realized.

Theorem: A finite cyclic group is realizable if its order is the product of a set of pairwise relatively prime integers drawn from the following list:

(a) $p^k - 1$ where p is prime and $k \geq 1$;

(b) $(p-1)p^k$ where $p > 2$ and $k \geq 1$;

(c) $2k$ where k is odd;

(d) $4k$ where any prime dividing k is congruent to 1 modulo 4.

What is known?

Symmetric and Alternating Groups: Davis & Occhipinti (2014) gave a complete solution for which symmetric (S_n) and alternating (A_n) groups are realizable. The only realizable symmetric and alternating groups are... $S_1, S_2, S_3, S_4, A_1, A_2, A_3, A_4,$ and A_8

What is known?

Symmetric and Alternating Groups: Davis & Occhipinti (2014) gave a complete solution for which symmetric (S_n) and alternating (A_n) groups are realizable.
The only realizable symmetric and alternating groups are... $S_1, S_2, S_3, S_4, A_1, A_2, A_3, A_4,$ and A_8

Finite Simple Groups: In a different paper, Davis & Occhipinti (2014) settled which finite simple groups can be realized.
The only realizable finite simple groups are...
C_2, C_p where p is a Mersenne prime, $\mathrm{PSL}_n(\mathbb{F}_2)$ where $n \geq 3$

What is known?

Dihedral Groups: Chebolu & Lockridge (2016) gave a complete solution for which dihedral groups can be realized.

Recall $D_n = \langle a, x \mid a^n = 1, x^2 = 1, ax = xa^{-1} \rangle = \{1, a, \ldots, a^{n-1}, x, ax, \ldots, a^{n-1}x\}$ is the dihedral group of order $2n$.
The only realizable dihedral groups are...

$$D_2, D_4, D_6, \text{ and } D_k \text{ where } k \text{ is odd.}$$

Generalized Quaternion = Dicyclic Groups:

Let $\mathrm{Dic}_n = \langle a, x \mid a^{2n} = 1, a^n = x^2, ax = xa^{-1} \rangle$
$= \{1, a, \ldots, a^{2n-1}, x, ax, \ldots, a^{2n-1}x\}$
be the dicyclic group of order $4n$.

- These groups can be constructed inside the quaternion algebra letting a be a primitive $2n$-th root of unity and $x = j$.

Generalized Quaternion = Dicyclic Groups:

Let $$\begin{aligned}\mathrm{Dic}_n &= \langle a, x \mid a^{2n} = 1, a^n = x^2, ax = xa^{-1} \rangle \\ &= \{1, a, \ldots, a^{2n-1}, x, ax, \ldots, a^{2n-1}x\}\end{aligned}$$
be the dicyclic group of order $4n$.

- These groups can be constructed inside the quaternion algebra letting a be a primitive $2n$-th root of unity and $x = j$.
- $\mathrm{Dic}_1 \cong C_4$ is the only Abelian dicyclic group.

Generalized Quaternion = Dicyclic Groups:

Let $\mathrm{Dic}_n = \langle a, x \mid a^{2n} = 1, a^n = x^2, ax = xa^{-1} \rangle$
$= \{1, a, \ldots, a^{2n-1}, x, ax, \ldots, a^{2n-1}x\}$
be the dicyclic group of order $4n$.

- These groups can be constructed inside the quaternion algebra letting a be a primitive $2n$-th root of unity and $x = j$.
- $\mathrm{Dic}_1 \cong C_4$ is the only Abelian dicyclic group.
- $\mathrm{Dic}_2 \cong Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group of order 8.

Generalized Quaternion = Dicyclic Groups:

Let $\mathrm{Dic}_n = \langle a, x \mid a^{2n} = 1, a^n = x^2, ax = xa^{-1} \rangle$
$= \{1, a, \ldots, a^{2n-1}, x, ax, \ldots, a^{2n-1}x\}$
be the dicyclic group of order $4n$.

- These groups can be constructed inside the quaternion algebra letting a be a primitive $2n$-th root of unity and $x = j$.
- $\mathrm{Dic}_1 \cong C_4$ is the only Abelian dicyclic group.
- $\mathrm{Dic}_2 \cong Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group of order 8.
- $\langle a \rangle = \{1, a, \ldots, a^{2n-1}\}$ has order $2n$.
- The elements $x, ax, \ldots, a^{2n-1}x$ all have order 4.

Generalized Quaternion = Dicyclic Groups:

Let $\mathrm{Dic}_n = \langle a, x \mid a^{2n} = 1, a^n = x^2, ax = xa^{-1} \rangle$
$= \{1, a, \ldots, a^{2n-1}, x, ax, \ldots, a^{2n-1}x\}$
be the dicyclic group of order $4n$.

- These groups can be constructed inside the quaternion algebra letting a be a primitive $2n$-th root of unity and $x = j$.
- $\mathrm{Dic}_1 \cong C_4$ is the only Abelian dicyclic group.
- $\mathrm{Dic}_2 \cong Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group of order 8.
- $\langle a \rangle = \{1, a, \ldots, a^{2n-1}\}$ has order $2n$.
- The elements $x, ax, \ldots, a^{2n-1}x$ all have order 4.
- $a^n = x^2$ is the only element of order 2.

Generalized Quaternion = Dicyclic Groups:

Let $\mathrm{Dic}_n = \langle a, x \mid a^{2n} = 1, a^n = x^2, ax = xa^{-1} \rangle$
$= \{1, a, \ldots, a^{2n-1}, x, ax, \ldots, a^{2n-1}x\}$
be the dicyclic group of order $4n$.

- These groups can be constructed inside the quaternion algebra letting a be a primitive $2n$-th root of unity and $x = j$.
- $\mathrm{Dic}_1 \cong C_4$ is the only Abelian dicyclic group.
- $\mathrm{Dic}_2 \cong Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group of order 8.
- $\langle a \rangle = \{1, a, \ldots, a^{2n-1}\}$ has order $2n$.
- The elements $x, ax, \ldots, a^{2n-1}x$ all have order 4.
- $a^n = x^2$ is the only element of order 2.
- $Z(\mathrm{Dic}_n) = \{1, a^n\}$ when $n > 1$.

Generalized Quaternion = Dicyclic Groups:

Let $n > 1$. Then since $|Z(\mathrm{Dic}_n)| = 2$, if R realizes Dic_n, we have

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

Generalized Quaternion = Dicyclic Groups:

Let $n > 1$. Then since $|Z(\mathrm{Dic}_n)| = 2$, if R realizes Dic_n, we have

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

Note that $\mathrm{Dic}_1 = Z(\mathrm{Dic}_1) \cong C_4$ allows for more possibilities:

$$\mathrm{char}(R) = 0, 2, 3, 4, 5, 6, \text{ or } 10.$$

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4$

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4 = 1+4x+6x^2+4x^3+x^4$

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4 = 1+4x+6x^2+4x^3+x^4 = 1+x+0+(-1)x+1 = 2 = -1$.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4 = 1+4x+6x^2+4x^3+x^4 = 1+x+0+(-1)x+1 = 2 = -1$.
So $(1+x)^8 = 1$ and thus $1+x$ is a unit of order 8.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4 = 1+4x+6x^2+4x^3+x^4 = 1+x+0+(-1)x+1 = 2 = -1$.
So $(1+x)^8 = 1$ and thus $1+x$ is a unit of order 8.Therefore,
$1+x = a^k$ for some k since $x, ax, \ldots, a^{2n-1}x$ have order 4.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4 = 1+4x+6x^2+4x^3+x^4 = 1+x+0+(-1)x+1 = 2 = -1$.
So $(1+x)^8 = 1$ and thus $1+x$ is a unit of order 8.Therefore, $1+x = a^k$ for some k since $x, ax, \ldots, a^{2n-1}x$ have order 4. Then
$a(1+x) = a^{k+1} = (1+x)a$

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4 = 1+4x+6x^2+4x^3+x^4 = 1+x+0+(-1)x+1 = 2 = -1$.
So $(1+x)^8 = 1$ and thus $1+x$ is a unit of order 8.Therefore, $1+x = a^k$ for some k since $x, ax, \ldots, a^{2n-1}x$ have order 4. Then $a(1+x) = a^{k+1} = (1+x)a$ so $a + ax = a + xa$ and so $ax = xa$.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4 = 1+4x+6x^2+4x^3+x^4 = 1+x+0+(-1)x+1 = 2 = -1$.
So $(1+x)^8 = 1$ and thus $1+x$ is a unit of order 8.Therefore, $1+x = a^k$ for some k since $x, ax, \ldots, a^{2n-1}x$ have order 4. Then $a(1+x) = a^{k+1} = (1+x)a$ so $a + ax = a + xa$ and so $ax = xa$.
But $xa^{-1} = ax = xa$ so that $a^{-1} = a$.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4 = 1+4x+6x^2+4x^3+x^4 = 1+x+0+(-1)x+1 = 2 = -1$.
So $(1+x)^8 = 1$ and thus $1+x$ is a unit of order 8.Therefore, $1+x = a^k$ for some k since $x, ax, \ldots, a^{2n-1}x$ have order 4. Then $a(1+x) = a^{k+1} = (1+x)a$ so $a + ax = a + xa$ and so $ax = xa$.
But $xa^{-1} = ax = xa$ so that $a^{-1} = a$.Thus $a^2 = 1$ and so $n = 1$.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4 = 1+4x+6x^2+4x^3+x^4 = 1+x+0+(-1)x+1 = 2 = -1$.
So $(1+x)^8 = 1$ and thus $1+x$ is a unit of order 8. Therefore, $1+x = a^k$ for some k since $x, ax, \ldots, a^{2n-1}x$ have order 4. Then $a(1+x) = a^{k+1} = (1+x)a$ so $a + ax = a + xa$ and so $ax = xa$.
But $xa^{-1} = ax = xa$ so that $a^{-1} = a$. Thus $a^2 = 1$ and so $n = 1$. But $\mathrm{Dic}_1 \cong C_4$ does not have an element of order 8!
(contradiction)

Generalized Quaternion = Dicyclic Groups:

Proposition: Dicyclic groups cannot be realized in char. 3 or 6.

Proof: Suppose R realizes Dic_n. If R's characteristic is not 2, then $1 \neq -1$ so -1 has order 2. Thus $a^n = x^2 = -1$.
Suppose $\mathrm{char}(R) = 3$. Then
$(1+x)^4 = 1+4x+6x^2+4x^3+x^4 = 1+x+0+(-1)x+1 = 2 = -1$.
So $(1+x)^8 = 1$ and thus $1+x$ is a unit of order 8.Therefore, $1+x = a^k$ for some k since $x, ax, \ldots, a^{2n-1}x$ have order 4. Then $a(1+x) = a^{k+1} = (1+x)a$ so $a+ax = a+xa$ and so $ax = xa$. But $xa^{-1} = ax = xa$ so that $a^{-1} = a$.Thus $a^2 = 1$ and so $n = 1$.But $\mathrm{Dic}_1 \cong C_4$ does not have an element of order 8! (contradiction)
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 $(2+x)^8 = 1$ and thus $2+x$ is a unit of order 8. Again, we must have $2+x = a^k$ for some k and again $a(2+x) = a^{k+1} = (2+x)a$ implies $ax = xa$. This leads to the same contradiction. □

Generalized Quaternion = Dicyclic Groups:

Proposition: Dic_n can be realized in char. 2 or 4 if and only if $n = 1$ or $n = 2$.

Proof: This is similar in flavor to the characteristic 3 and 6 proof, but it is a bit more involved. $\square$

Generalized Quaternion = Dicyclic Groups:

Proposition: Dic_n can be realized in char. 2 or 4 if and only if $n = 1$ or $n = 2$.

Proof: This is similar in flavor to the characteristic 3 and 6 proof, but it is a bit more involved. $\square$

Example: $\mathbb{Z}[-1, j]^\times \cong C_4 \cong \mathrm{Dic}_1$, $\mathbb{Z}[i, j]^\times \cong Q \cong \mathrm{Dic}_2$, and...

$$\mathbb{Z}[e^{\pi i/3}, j]^\times \cong \mathrm{Dic}_3.$$

Generalized Quaternion = Dicyclic Groups:

Proposition: Dic_n can be realized in char. 2 or 4 if and only if $n = 1$ or $n = 2$.

Proof: This is similar in flavor to the characteristic 3 and 6 proof, but it is a bit more involved. $\square$

Example: $\mathbb{Z}[-1, j]^\times \cong C_4 \cong \mathrm{Dic}_1$, $\mathbb{Z}[i, j]^\times \cong Q \cong \mathrm{Dic}_2$, and...
$\mathbb{Z}[e^{\pi i/3}, j]^\times \cong \mathrm{Dic}_3$.

Proposition: We have a complete picture for small Dicyclic groups...

- Dic_1 can only be realized in char. 0, 2, 4, 5, and 10.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dic_n can be realized in char. 2 or 4 if and only if $n = 1$ or $n = 2$.

Proof: This is similar in flavor to the characteristic 3 and 6 proof, but it is a bit more involved. □

Example: $\mathbb{Z}[-1, j]^\times \cong C_4 \cong \mathrm{Dic}_1$, $\mathbb{Z}[i, j]^\times \cong Q \cong \mathrm{Dic}_2$, and...
$\mathbb{Z}[e^{\pi i/3}, j]^\times \cong \mathrm{Dic}_3$.

Proposition: We have a complete picture for small Dicyclic groups...

- Dic_1 can only be realized in char. 0, 2, 4, 5, and 10.
- Dic_2 can only be realized in char. 0, 2, and 4.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dic_n can be realized in char. 2 or 4 if and only if $n = 1$ or $n = 2$.

Proof: This is similar in flavor to the characteristic 3 and 6 proof, but it is a bit more involved. □

Example: $\mathbb{Z}[-1, j]^\times \cong C_4 \cong \mathrm{Dic}_1$, $\mathbb{Z}[i, j]^\times \cong Q \cong \mathrm{Dic}_2$, and...

$$\mathbb{Z}[e^{\pi i/3}, j]^\times \cong \mathrm{Dic}_3.$$

Proposition: We have a complete picture for small Dicyclic groups...

- Dic_1 can only be realized in char. 0, 2, 4, 5, and 10.
- Dic_2 can only be realized in char. 0, 2, and 4.
- Dic_3 can only be realized in char. 0.

Generalized Quaternion = Dicyclic Groups:

Proposition: Dic_n can be realized in char. 2 or 4 if and only if $n = 1$ or $n = 2$.

Proof: This is similar in flavor to the characteristic 3 and 6 proof, but it is a bit more involved. □

Example: $\mathbb{Z}[-1, j]^\times \cong C_4 \cong \mathrm{Dic}_1$, $\mathbb{Z}[i, j]^\times \cong Q \cong \mathrm{Dic}_2$, and...

$\mathbb{Z}[e^{\pi i/3}, j]^\times \cong \mathrm{Dic}_3$.

Proposition: We have a complete picture for small Dicyclic groups...

- Dic_1 can only be realized in char. 0, 2, 4, 5, and 10.
- Dic_2 can only be realized in char. 0, 2, and 4.
- Dic_3 can only be realized in char. 0.

Dic_3 cannot be realized by a finite ring!

Some Partial Results:

Sadly, $\mathbb{Z}[e^{\pi i/(2n)}]^\times$ is infinite for $n > 3$, so we cannot use $\mathbb{Z}[e^{\pi i/(2n)}, j]$ to realize Dic_n for $n > 3$.

Some Partial Results:

Sadly, $\mathbb{Z}[e^{\pi i/(2n)}]^\times$ is infinite for $n > 3$, so we cannot use $\mathbb{Z}[e^{\pi i/(2n)}, j]$ to realize Dic_n for $n > 3$.

Proposition: If every prime factor of n is congruent to 1 modulo 4 (i.e., $\mathbb{Z}_n^\times$ has an element of order 4 that squares to be -1), then we can realize Dic_n in characteristic 0.

Let $R = \mathbb{Z}_n \rtimes \mathbb{Z}[i]$ $(= \mathbb{Z}_n \times \mathbb{Z}[i]$ as a group under addition). Define $f(x + yi) = x + y\tau$ and $g(x + yi) = x - y\tau$ where $\tau^2 = -1$ in $\mathbb{Z}_n$. We multiply as follows: $(a, b)(x, y) = (af(y) + xg(b), by)$. Then $R = \mathbb{Z}_n \rtimes \mathbb{Z}[i]$ realizes Dic_n (in characteristic 0).

Some Partial Results:

Sadly, $\mathbb{Z}[e^{\pi i/(2n)}]^\times$ is infinite for $n > 3$, so we cannot use $\mathbb{Z}[e^{\pi i/(2n)}, j]$ to realize Dic_n for $n > 3$.

Proposition: If every prime factor of n is congruent to 1 modulo 4 (i.e., $\mathbb{Z}_n^\times$ has an element of order 4 that squares to be -1), then we can realize Dic_n in characteristic 0.

Let $R = \mathbb{Z}_n \rtimes \mathbb{Z}[i]$ ($= \mathbb{Z}_n \times \mathbb{Z}[i]$ as a group under addition). Define $f(x + yi) = x + y\tau$ and $g(x + yi) = x - y\tau$ where $\tau^2 = -1$ in $\mathbb{Z}_n$. We multiply as follows: $(a, b)(x, y) = (af(y) + xg(b), by)$. Then $R = \mathbb{Z}_n \rtimes \mathbb{Z}[i]$ realizes Dic_n (in characteristic 0).

Proposition: If G is realizable in characteristic n, then so is every maximal Abelian subgroup of G.

Some Partial Results:

Sadly, $\mathbb{Z}[e^{\pi i/(2n)}]^\times$ is infinite for $n > 3$, so we cannot use $\mathbb{Z}[e^{\pi i/(2n)}, j]$ to realize Dic_n for $n > 3$.

Proposition: If every prime factor of n is congruent to 1 modulo 4 (i.e., $\mathbb{Z}_n^\times$ has an element of order 4 that squares to be -1), then we can realize Dic_n in characteristic 0.

Let $R = \mathbb{Z}_n \rtimes \mathbb{Z}[i]$ ($= \mathbb{Z}_n \times \mathbb{Z}[i]$ as a group under addition). Define $f(x + yi) = x + y\tau$ and $g(x + yi) = x - y\tau$ where $\tau^2 = -1$ in $\mathbb{Z}_n$. We multiply as follows: $(a, b)(x, y) = (af(y) + xg(b), by)$. Then $R = \mathbb{Z}_n \rtimes \mathbb{Z}[i]$ realizes Dic_n (in characteristic 0).

Proposition: If G is realizable in characteristic n, then so is every maximal Abelian subgroup of G.

Corollary: If we can realize Dic_n in characteristic 0, then we must be able to realize C_{2n} as well. As a consequence, for example, Dic_{4n} cannot be realized for any $n \geq 1$.

Groups of Small Order:

Order	Isomorphism Classes
1,2,3	$C_1 \cong \mathbb{Z}_2^\times$, $C_2 \cong \mathbb{Z}_3^\times$, $C_3 \cong \mathbb{F}_4^\times$
4	$C_4 \cong \mathbb{Z}_5^\times$ and $C_2 \times C_2 \cong (\mathbb{Z}_3 \times \mathbb{Z}_3)^\times$
5	C_5 is not realizable
6	$C_6 \cong \mathbb{Z}_7^\times$ and $S_3 \cong (\mathbb{Z}_2^{2\times 2})^\times$
7	$C_7 \cong \mathbb{F}_8^\times$
8	$C_8 \cong \mathbb{F}_9^\times$, $C_2 \times C_4 \cong (\mathbb{Z}_3 \times \mathbb{Z}_5)^\times$, $C_2 \times C_2 \times C_2 \cong (\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3)^\times$, $D_4 \cong U_3(\mathbb{Z}_2)^\times$, and $Q \cong (\mathbb{Z}_2[\mathrm{Dic}_2]/(1+x+a+ax))^\times$
9	C_9 is not realizable and $C_3 \times C_3 \cong (\mathbb{F}_4 \times \mathbb{F}_4)^\times$
10	$C_{10} \cong \mathbb{Z}_{11}^\times$ and D_5 is not realizable
11	C_{11} is not realizable
12	$C_{12} \cong \mathbb{Z}_{13}^\times$, $C_2 \times C_6 \cong (\mathbb{Z}_3 \times \mathbb{Z}_7)^\times$, $D_6 \cong U_2(\mathbb{Z}_3)^\times$, $A_4 \cong (\mathcal{O}/2\mathcal{O})^\times$, and $\mathrm{Dic}_3 \cong (\mathbb{Z}[e^{\pi i/3}, j])^\times$
13	C_{13} is not realizable
14	$C_{14} \cong (\mathbb{Z}_3 \times \mathbb{F}_8)^\times$ and D_7 is not realizable
15	$C_{15} \cong \mathbb{F}_{16}^\times$

References:

- S. Chebolu, K. Lockridge, "Fuchs problem for dihedral groups," *Journal of Pure and Applied Algebra*, 2016.
- C. Davis and T. Occhipinti, "Which alternating and symmetric groups are unit groups?" *Journal of Algebra and Its Applications*. Vol. 13, No. 3 (2014).
- C. Davis and T. Occhipinti, "Which finite simple groups are unit groups?" *Journal of Pure and Applied Algebra*. Vol. 13, No. 3 (2014).
- R. Gilmer, "Finite rings having a cyclic multiplicative group of units," *American Journal of Mathematics*, 1963, 447–452.
- K. R. Pearson and J. E. Schneider, "Rings with a cyclic group of units," *Journal of Algebra*. Vol. 16 (1970).

Theses:

- Joshua Carr, "Realizable Unit Groups" (May 2017)
- Lindsey Wise, "Realizable Dicyclic Groups" (December 2020)

Thank you for listening!
Questions?