GENERALIZED QUATERNIONS

KEITH CONRAD

1. INTRODUCTION

The quaternion group Q_8 is one of the two nonabelian groups of size 8 (up to isomorphism). The other one, D_4, can be constructed as a semi-direct product:

$$D_4 \cong \mathrm{Aff}(\mathbf{Z}/(4)) \cong \mathbf{Z}/(4) \rtimes (\mathbf{Z}/(4))^\times \cong \mathbf{Z}/(4) \rtimes \mathbf{Z}/(2),$$

where the elements of $\mathbf{Z}/(2)$ act on $\mathbf{Z}/(4)$ as the identity and negation. While Q_8 is not a semi-direct product, it can be constructed as the quotient group of a semi-direct product. We will see how this is done in Section 2 and then jazz up the construction in Section 3 to make an infinite family of similar groups with Q_8 as the simplest member. In Section 4 we will compare this family with the dihedral groups and see how it fits into a bigger picture.

2. The quaternion group from a semi-direct product

The group Q_8 is built out of its subgroups $\langle i\rangle$ and $\langle j\rangle$ with the condition $i^2 = j^2 = -1$ and the conjugacy relation $jij^{-1} = -i = i^{-1}$. More generally, for odd a we have $j^a ij^{-a} = -i = i^{-1}$, and for even a we have $j^a ij^{-a} = i$. We can combine these into one formula:

$$j^a ij^{-a} = i^{(-1)^a} \tag{2.1}$$

for all $a \in \mathbf{Z}$. These relations suggest the following way to construct the group Q_8.[1]

Theorem 2.1. *Let $H = \mathbf{Z}/(4) \rtimes \mathbf{Z}/(4)$, where*

$$(a, b)(c, d) = (a + (-1)^b c, b + d),$$

The element $(2, 2)$ in H has order 2, lies in the center, and $H/\langle(2, 2)\rangle \cong Q_8$.

Proof. Since $-2 = 2$ in $\mathbf{Z}/(4)$,

$$(a, b)(2, 2) = (a + (-1)^b 2, b + 2) = (a + 2, b + 2)$$

and

$$(2, 2)(a, b) = (2 + (-1)^2 a, 2 + b) = (2 + a, b + 2) = (a + 2, b + 2),$$

$(2, 2)$ is in the center of H. Also $(2, 2)(2, 2) = (2 + (-1)^2 2, 2 + 2) = (0, 0)$, so $(2, 2)$ has order 2 in H. Therefore the quotient group

$$Q := H/\langle(2, 2)\rangle$$

makes sense and has size $16/2 = 8$.

Since H is generated by $(1, 0)$ and $(0, 1)$:

$$(a, b) = (a, 0)(0, b) = (1, 0)^a (0, 1)^b.$$

In Q, set $\mathbf{i}$ to be the class of $(1, 0)$ and $\mathbf{j}$ to be the class of $(0, 1)$, so $\mathbf{i}$ and $\mathbf{j}$ generate Q: $\overline{(a, b)} = \mathbf{i}^a \mathbf{j}^b$.

[1] A quaternion group built differently is https://advisor.morganstanley.com/the-quaternion-group.

To show $Q \cong Q_8$, we will create a homomorphism from the semi-direct product H onto Q_8 and check $(2,2)$ is in its kernel, so we get an induced homomorphism from Q onto Q_8.

Define $f\colon H \to Q_8$ by $f(a,b) = i^a j^b$. This is well-defined since $i^4 = 1$ and $j^4 = 1$. It is a homomorphism since

$$f((a,b)(c,d)) = f(a + (-1)^b c, b + d) = i^{a+(-1)^b c} j^{b+d}$$

and

$$f(a,b)f(c,d) = i^a j^b i^c j^d = i^a (j^b i^c j^{-b}) j^{b+d} = i^a (j^b i j^{-b})^c j^{b+d} = i^a i^{(-1)^b c} j^{b+d},$$

where the last equation comes from (2.1).

The image of f is a subgroup of Q_8 containing $i = f(1,0)$ and $j = f(0,1)$, so the image is Q_8: f is onto. Since $f(2,2) = i^2 j^2 = (-1)(-1) = 1$, the kernel of f contains $(2,2)$, so f induces a surjective homomorphism $Q \to Q_8$ given by $\mathbf{i}^a \mathbf{j}^b \mapsto i^a j^b$. The groups Q and Q_8 have the same size, so this surjective homomorphism is an isomorphism. □

3. Generalized Quaternions

While Q_8 is generated by two cyclic subgroups of order 4, we can extend its construction by letting one of the two cyclic subgroups be an arbitrary cyclic 2-group.

Definition 3.1. For $n \geq 3$, set

$$Q_{2^n} = (\mathbf{Z}/(2^{n-1}) \rtimes \mathbf{Z}/(4))/\langle (2^{n-2}, 2) \rangle,$$

where the semi-direct product has group law

$$(a,b)(c,d) = (a + (-1)^b c, b + d). \tag{3.1}$$

The groups Q_{2^n} are called *generalized quaternion groups*.

Note Q_{2^n} is not the semi-direct product $\mathbf{Z}/(2^{n-1}) \rtimes \mathbf{Z}/(4)$, but rather the quotient of this semi-direct product modulo the subgroup $\langle (2^{n-2}, 2) \rangle$. Since $2^{n-2} \bmod 2^{n-1}$ and $2 \bmod 4$ have order 2 in the additive groups $\mathbf{Z}/(2^{n-1})$ and $\mathbf{Z}/(4)$, a calculation as in Section 2 shows $(2^{n-2}, 2)$ is in the center of the semi-direct product and has order 2, so $\langle (2^{n-2}, 2) \rangle$ is a normal subgroup of the semi-direct product and the size of Q_{2^n} is $(2^{n-1} \cdot 4)/2 = 2^n$. The next theorem brings the construction of Q_{2^n} down to earth.

Theorem 3.2. *For $n \geq 3$, let $\mathbf{x} = \overline{(1,0)}$ and $\mathbf{y} = \overline{(0,1)}$ in Q_{2^n}. Then $Q_{2^n} = \langle \mathbf{x}, \mathbf{y} \rangle$, where*

1. *$\mathbf{x}$ has order 2^{n-1} and $\mathbf{y}$ has order 4,*
2. *every element of Q_{2^n} can be written in the form $\mathbf{x}^a$ or $\mathbf{x}^a \mathbf{y}$ for some $a \in \mathbf{Z}$,*
3. *$\mathbf{x}^{2^{n-2}} = \mathbf{y}^2$,*
4. *for each $g \in Q_{2^n}$ such that $g \notin \langle \mathbf{x} \rangle$, $g\mathbf{x}g^{-1} = \mathbf{x}^{-1}$.*

This theorem says, roughly, that Q_{2^n} is made by taking a cyclic group of order 2^{n-1} and a cyclic group of order 4 and "gluing" them at their unique elements of order 2 while being noncommutative.

Proof. Since $\mathbf{Z}/(2^{n-1})$ is generated by 1 and $\mathbf{Z}/(4)$ is generated by 1, Q_{2^n} is generated by the cosets of $(1,0)$ and $(0,1)$, so $\mathbf{x}$ and $\mathbf{y}$ generate Q_{2^n}.

(1): The smallest power of $(1,0)$ in $\langle (2^{n-2}, 2) \rangle = \{(2^{n-2}, 2), (0,0)\}$ is its 2^{n-1}-th power, which is $(0,0)$, so $\mathbf{x}$ has order 2^{n-1} in Q_{2^n}. Similarly, the smallest power of $(0,1)$ in $\langle (2^{n-2}, 2) \rangle$ is its fourth power, so $\mathbf{y}$ has order 4 in Q_{2^n}.

(2) and (3): Each element of $\mathbf{Z}/(2^{n-1}) \rtimes \mathbf{Z}/(4)$ has the form $(a,b) = (1,0)^a(0,1)^b$, so each element of Q_{2^n} has the form $\mathbf{x}^a\mathbf{y}^b$. Since $(2^{n-2},2)$ is trivial in Q_{2^n}, the relation $(2^{n-2},2) = (1,0)^{2^{n-2}}(0,1)^2$ in Q_{2^n} says $\mathbf{x}^{2^{n-2}}\mathbf{y}^2 = 1$, so $\mathbf{x}^{2^{n-2}} = \mathbf{y}^{-2} = \mathbf{y}^2$. Therefore in $\mathbf{x}^a\mathbf{y}^b$ we can absorb even powers of $\mathbf{y}$ into the power of $\mathbf{x}$. Thus we can use $b = 0$ or $b = 1$.

(4): Each $g \notin \langle \mathbf{x} \rangle$ has the form $g = \mathbf{x}^a\mathbf{y}$, so $g\mathbf{x}g^{-1} = \mathbf{x}^a\mathbf{y}\mathbf{x}\mathbf{y}^{-1}\mathbf{x}^{-a}$. Therefore it suffices to focus on the case $g = \mathbf{y}$. In $\mathbf{Z}/(2^{n-1}) \rtimes \mathbf{Z}/(4)$, $(0,1)(1,0)(0,1)^{-1} = (-1,1)(0,-1) = (-1,0) = (1,0)^{-1}$, so $\mathbf{y}\mathbf{x}\mathbf{y}^{-1} = \mathbf{x}^{-1}$. □

Since $n \geq 3$, $\mathbf{x}$ has order greater than 2, so the condition $\mathbf{y}\mathbf{x}\mathbf{y}^{-1} = \mathbf{x}^{-1} \neq \mathbf{x}$, shows Q_{2^n} is noncommutative. While we didn't define Q_{2^n} when $n = 2$, the definition makes sense at $n = 2$: Q_4 is a cyclic group of order 4 generated by $\mathbf{y}$ (with $\mathbf{x} = \mathbf{y}^2$).

The following theorem describes a special mapping property of Q_{2^n}: all groups with a few of the basic features of Q_{2^n} are homomorphic images of it.

Theorem 3.3. *For $n \geq 3$, let $G = \langle x, y \rangle$ where $x^{2^{n-1}} = 1$, $y^4 = 1$, $yxy^{-1} = x^{-1}$, and $x^{2^{n-2}} = y^2$. There is a unique homomorphism $Q_{2^n} \to G$ such that $\mathbf{x} \mapsto x$ and $\mathbf{y} \mapsto y$, and it is onto. If $|G| = 2^n$, then this homomorphism is an isomorphism.*

The trivial group fits the conditions of the theorem (taking $x = 1$ and $y = 1$), so not all such groups must be isomorphic to Q_{2^n} (only such groups of the right size are). Remember: saying $x^{2^{n-1}} = 1$ and $y^4 = 1$ does *not* mean x has order 2^{n-1} and y has order 4, but only that their orders divide 2^{n-1} and 4.

Proof. If there is a homomorphism $Q_{2^n} \to G$ such that $\mathbf{x} \mapsto x$ and $\mathbf{y} \mapsto y$, then the homomorphism is completely determined everywhere since $\mathbf{x}$ and $\mathbf{y}$ generate Q_{2^n}. So such a homomorphism is unique. To actually construct such a homomorphism (prove existence, that is), we adapt the idea in the proof of Theorem 2.1: rather than directly write down a homomorphism $Q_{2^n} \to G$, start with a homomorphism from a semi-direct product to G.

Let $f\colon \mathbf{Z}/(2^{n-1}) \rtimes \mathbf{Z}/(4) \to G$ by $f(a,b) = x^a y^b$. This is well-defined since $x^{2^{n-1}} = 1$ and $y^4 = 1$. To check f is a homomorphism, we will use the condition $yxy^{-1} = x^{-1}$, which implies $y^b x y^{-b} = x^{(-1)^b}$. First we have

$$f((a,b)(c,d)) = f(a + (-1)^b c, b + d) = x^{a+(-1)^b c} y^{b+d},$$

and next we have

$$f(a,b)f(c,d) = x^a y^b x^c y^d = x^a (y^b x^c y^{-b}) y^{b+d} = x^a (y^b x y^{-b})^c y^{b+d} = x^a x^{(-1)^b c} y^{b+d}.$$

Thus f is a homomorphism. It is surjective since we are told x and y generate G and x and y are values of f. Since $f(2^{n-2},2) = x^{2^{n-2}}y^2 = y^2y^2 = y^4 = 1$, $(2^{n-2},2)$ is in the kernel of f. Therefore f induces a surjective homomorphism $Q_{2^n} \to G$ given by $\mathbf{x}^a\mathbf{y}^b \mapsto x^a y^b$, so G is a homomorphic image of Q_{2^n}.

When $|G| = 2^n$, f is a surjective homomorphism between finite groups of the same size, so it is an isomorphism. □

Theorem 3.3 is true for $n = 2$ when we define $Q_4 = \langle \mathbf{y} \rangle$ to be a cyclic group of order 4 with $\mathbf{x} = \mathbf{y}^2$. Theorem 3.3 also gives us a recognition criterion for generalized quaternion groups in terms of generators and relations.

Example 3.4. Here is a matrix model of Q_{2^n} in $\mathrm{GL}_2(\mathbf{C})$. Let $\zeta = e^{2\pi i/2^{n-1}}$ be a root of unity of order 2^{n-1}. In $\mathrm{GL}_2(\mathbf{C})$, the matrix $x = \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \bar{\zeta} \end{smallmatrix}\right)$ has order 2^{n-1} and the matrix $y = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ has order 4. Since $x^{2^{n-2}} = y^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $yxy^{-1} = x^{-1}$, the group generated

by x and y is a homomorphic image of Q_{2^n} by Theorem 3.3. Therefore $\langle x, y\rangle$ has size dividing 2^n. This group contains $\langle x\rangle$, of order 2^{n-1}, so $2^{n-1} \mid |\langle x, y\rangle|$. We have $y \notin \langle x\rangle$ since x and y do not commute (because $yxy^{-1} = x^{-1} \neq x$), so $|\langle x, y\rangle| = 2^n$. Therefore $\langle x, y\rangle \cong Q_{2^n}$. The division ring of real quaternions $a + bi + cj + dk$ is isomorphic to the ring of complex matrices of the form $\left(\begin{smallmatrix} z & -w \\ \overline{w} & \overline{z} \end{smallmatrix}\right)$, where $z = a + bi$ and $w = c + di$. The matrices x and y have this form, so all the groups Q_{2^n} can be embedded in the real quaternions.

Remark 3.5. The basic idea behind the construction of Q_{2^n} can be pushed further. Let A be an abelian group of even order, written additively. There is an element of A with order 2, say ε. For a positive integer t that is divisible by 4, consider the semi-direct product $A \rtimes \mathbf{Z}/(t)$ with group law as in (3.1). Since $-\varepsilon = \varepsilon$ and $t/2$ is even, a short calculation shows $(\varepsilon, t/2)$ is in the center of $A \rtimes \mathbf{Z}/(t)$ and has order 2. The quotient group

$$(A \rtimes \mathbf{Z}/(t))/\langle(\varepsilon, t/2)\rangle \tag{3.2}$$

generalizes the construction of Q_{2^n} (the special case $A = \mathbf{Z}/(2^{n-1})$, $t = 4$). This group is noncommutative when some $a \in A$ has order greater than 2. If A is cyclic of even order $2m \geq 4$ (not necessarily a 2-group, *e.g.*, $A = \mathbf{Z}/(6)$ for $m = 3$) and $t = 4$, then (3.2) has order $4m$ with generators $\mathbf{x}$ and $\mathbf{y}$ such that $\mathbf{x}^{2m} = 1$, $\mathbf{y}\mathbf{x}\mathbf{y}^{-1} = \mathbf{x}^{-1}$, and $\mathbf{x}^m = \mathbf{y}^2$ (so $\mathbf{y}^4 = \mathbf{x}^{2m} = 1$). Properties of these groups are in Section 5.

4. Comparing Dihedral and Generalized Quaternion Groups

For all $n \geq 3$, the groups $D_{2^{n-1}}$ and Q_{2^n}, both of order 2^n, are similar. First, their generators and relations are analogous (but of course not the same): $D_{2^{n-1}} = \langle r, s\rangle$ where

$$r^{2^{n-1}} = 1, \quad s^2 = 1, \quad srs^{-1} = r^{-1}$$

and $Q_{2^n} = \langle \mathbf{x}, \mathbf{y}\rangle$ where

$$\mathbf{x}^{2^{n-1}} = 1, \quad \mathbf{y}^4 = 1, \quad \mathbf{y}\mathbf{x}\mathbf{y}^{-1} = \mathbf{x}^{-1}, \quad \mathbf{x}^{2^{n-2}} = \mathbf{y}^2.$$

The condition $\mathbf{y}^4 = 1$ can be dropped, since the first and fourth conditions imply it, but we include it to make the similarity with dihedral groups clearer. In both $D_{2^{n-1}}$ and Q_{2^n}, there are two generators (r and s or $\mathbf{x}$ and $\mathbf{y}$) where the first generator has order 2^{n-1} and the second generator conjugates the first to its inverse ($srs^{-1} = r^{-1}$ and $\mathbf{y}\mathbf{x}\mathbf{y}^{-1} = \mathbf{x}^{-1}$). In $D_{2^{n-1}}$, s has order 2 and the intersection $\langle r\rangle \cap \langle s\rangle$ is trivial, while in Q_{2^n}, $\mathbf{y}$ has order 4 and the intersection $\langle \mathbf{x}\rangle \cap \langle \mathbf{y}\rangle$ has order 2. In the degenerate case $n = 2$, $D_2 \cong \mathbf{Z}/(2) \times \mathbf{Z}/(2)$ and $Q_4 \cong \mathbf{Z}/(4)$ are the two possible groups of order 4.

We now state without proof a catch-all theorem about the dihedral groups $D_{2^{n-1}}$ and then see what an analogue is for Q_{2^n}.

Theorem 4.1. *For $n \geq 3$, $D_{2^{n-1}}$ has the following properties:*

1. *the subgroup $\langle r\rangle$ has index 2 and every element of $D_{2^{n-1}}$ outside of $\langle r\rangle$ has order 2,*
2. *the center of $D_{2^{n-1}}$ is $\{1, r^{2^{n-2}}\}$ and $D_{2^{n-1}}/Z(D_{2^{n-1}}) \cong D_{2^{n-2}}$,*
3. *the commutator subgroup of $D_{2^{n-1}}$ is $\langle r^2\rangle$, and $D_{2^{n-1}}/\langle r^2\rangle \cong \mathbf{Z}/(2) \times \mathbf{Z}/(2)$,*
4. *there are $2^{n-2}+3$ conjugacy classes, with representatives given in the following table.*

Rep.	1	r	r^2	$\cdots$	$r^{2^{n-2}-1}$	$r^{2^{n-2}}$	s	rs
Size	1	2	2	$\cdots$	2	1	2^{n-2}	2^{n-2}

Table 1. Conjugacy class representatives in $D_{2^{n-1}}$.

Theorem 4.2. *For $n \geq 3$, Q_{2^n} has the following properties:*

(1) *the subgroup $\langle \mathbf{x} \rangle$ has index 2 and every element of Q_{2^n} outside of $\langle \mathbf{x} \rangle$ has order 4,*
(2) *the center of Q_{2^n} is $\{1, \mathbf{x}^{2^{n-2}}\} = \{1, \mathbf{y}^2\}$ and $Q_{2^n}/Z(Q_{2^n}) \cong D_{2^{n-2}}$,*
(3) *the commutator subgroup of Q_{2^n} is $\langle \mathbf{x}^2 \rangle$, and $Q_{2^n}/\langle \mathbf{x}^2 \rangle \cong \mathbf{Z}/(2) \times \mathbf{Z}/(2)$,*
(4) *there are $2^{n-2}+3$ conjugacy classes, with representatives given in the following table.*

Rep.	1	$\mathbf{x}$	$\mathbf{x}^2$	$\cdots$	$\mathbf{x}^{2^{n-2}-1}$	$\mathbf{x}^{2^{n-2}}$	$\mathbf{y}$	$\mathbf{xy}$
Size	1	2	2	$\cdots$	2	1	2^{n-2}	2^{n-2}

TABLE 2. Conjugacy class representatives in Q_{2^n}.

Proof. (1): Since $\mathbf{x}$ has order 2^{n-1}, $[Q_{2^n} : \langle \mathbf{x} \rangle] = 2$. The elements of Q_{2^n} that are not powers of $\mathbf{x}$ have the form $\mathbf{x}^a\mathbf{y}$, and

$$(\mathbf{x}^a\mathbf{y})^2 = \mathbf{x}^a(\mathbf{y}\mathbf{x}^a\mathbf{y}^{-1})\mathbf{y}^2 = \mathbf{x}^a(\mathbf{y}\mathbf{x}\mathbf{y}^{-1})^a\mathbf{y}^2 = \mathbf{x}^a\mathbf{x}^{-a}\mathbf{y}^2 = \mathbf{y}^2 = \mathbf{x}^{2^{n-2}},$$

so $\mathbf{x}^a\mathbf{y}$ has order 4.

(2): Since $\mathbf{x}^{2^{n-2}} = \mathbf{y}^2$, $\mathbf{x}^{2^{n-2}}$ commutes with both $\mathbf{x}$ and $\mathbf{y}$, and hence with all of Q_{2^n}, so $\mathbf{x}^{2^{n-2}}$ is in the center. If $\mathbf{x}^a$ is in the center, then $\mathbf{y}\mathbf{x}^a\mathbf{y}^{-1} = \mathbf{x}^a$. The left side is $(\mathbf{y}\mathbf{x}\mathbf{y}^{-1})^a = \mathbf{x}^{-a}$, so $\mathbf{x}^{-a} = \mathbf{x}^a$. Therefore $\mathbf{x}^{2a} = 1$, so $2^{n-1} \mid 2a$, so $2^{n-2} \mid a$, which means $\mathbf{x}^a$ is a power of $\mathbf{x}^{2^{n-2}}$.

Each element of Q_{2^n} that is not a power of $\mathbf{x}$ is not in the center: it is some $\mathbf{x}^a\mathbf{y}$ and $\mathbf{x}(\mathbf{x}^a\mathbf{y})\mathbf{x}^{-1} = \mathbf{x}^{a+1}\mathbf{x}\mathbf{y} = \mathbf{x}^{a+2}\mathbf{y} \neq \mathbf{x}^a\mathbf{y}$. (Here we need $n \geq 3$ to be sure that $\mathbf{x}^2 \neq 1$.)

The quotient group $Q_{2^n}/Z(Q_{2^n})$ has generators $\overline{\mathbf{x}}$ and $\overline{\mathbf{y}}$ such that $\overline{\mathbf{x}}^{2^{n-2}} = \overline{1}$ (since $\mathbf{x}^{2^{n-2}} = \mathbf{y}^2$ is in the center), $\overline{\mathbf{y}}^2 = \overline{1}$, and $\overline{\mathbf{y}}\,\overline{\mathbf{x}}\,\overline{\mathbf{y}}^{-1} = \overline{\mathbf{x}}^{-1}$. Therefore this quotient group is a homomorphic image of $D_{2^{n-2}}$. Since the size of $Q_{2^n}/Z(Q_{2^n})$ is $2^{n-1} = |D_{2^{n-2}}|$, $Q_{2^n}/Z(Q_{2^n})$ is isomorphic to $D_{2^{n-2}}$: the cosets $\overline{\mathbf{x}}$ and $\overline{\mathbf{y}}$ in $Q_{2^n}/Z(Q_{2^n})$ play the roles of r and s in the dihedral group.

(3): Since $\mathbf{x}\mathbf{y}\mathbf{x}^{-1}\mathbf{y}^{-1} = \mathbf{x}^2$, the commutator subgroup of Q_{2^n} contains $\langle \mathbf{x}^2 \rangle$. (In fact, $\mathbf{x}^a\mathbf{y}\mathbf{x}^{-a}\mathbf{y}^{-1} = \mathbf{x}^{2a}$, so all elements of $\langle \mathbf{x}^2 \rangle$ are commutators.) The subgroup $\langle \mathbf{x}^2 \rangle$ has size 2^{n-2} and thus index 4. It is a normal subgroup of Q_{2^n} since $\mathbf{y}\mathbf{x}^2\mathbf{y}^{-1} = \mathbf{x}^{-2} \in \langle \mathbf{x}^2 \rangle$. The group $Q_{2^n}/\langle \mathbf{x}^2 \rangle$ has size 4, hence is abelian, so every commutator in Q_{2^n} is in $\langle \mathbf{x}^2 \rangle$. Therefore $\langle \mathbf{x}^2 \rangle$ is the commutator subgroup of Q_{2^n}. In $Q_{2^n}/\langle \mathbf{x}^2 \rangle$, the images of $\mathbf{x}$ and $\mathbf{y}$ are distinct and have order 2, so $Q_{2^n}/\langle \mathbf{x}^2 \rangle \cong \mathbf{Z}/(2) \times \mathbf{Z}/(2)$.

(4): For each $g \in Q_{2^n}$ we compute $\mathbf{x}^a g \mathbf{x}^{-a}$ and $(\mathbf{x}^a\mathbf{y})g(\mathbf{x}^a\mathbf{y})^{-1} = \mathbf{x}^a\mathbf{y}g\mathbf{y}^{-1}\mathbf{x}^{-a}$ as a varies.

First suppose g is a power of $\mathbf{x}$, say $g = \mathbf{x}^k$ with $0 \leq k \leq 2^{n-1} - 1$. Then

$$\mathbf{x}^a\mathbf{x}^k\mathbf{x}^{-a} = \mathbf{x}^k, \quad (\mathbf{x}^a\mathbf{y})\mathbf{x}^k(\mathbf{x}^a\mathbf{y})^{-1} = \mathbf{x}^{-k},$$

so the conjugacy class of $\mathbf{x}^k$ is $\{\mathbf{x}^k, \mathbf{x}^{-k}\}$. Thus we may take $0 \leq k \leq 2^{n-2}$, and $|\{\mathbf{x}^k, \mathbf{x}^{-k}\}| = 2$ if $\mathbf{x}^{2k} \neq 1$. We have $\mathbf{x}^{2k} = 1$ when $\mathbf{x}^k$ is 1 or $\mathbf{x}^{2^{n-2}}$, which form the center.

If $g = \mathbf{y}$ then check

$$\mathbf{x}^a\mathbf{y}\mathbf{x}^{-a} = \mathbf{x}^{2a}\mathbf{y}, \quad (\mathbf{x}^a\mathbf{y})\mathbf{y}(\mathbf{x}^a\mathbf{y})^{-1} = \mathbf{x}^{2a}\mathbf{y},$$

so the conjugacy class of $\mathbf{y}$ is all $\mathbf{x}^{2a}\mathbf{y}$ as a varies.

Finally, if $g = \mathbf{x}\mathbf{y}$ then

$$\mathbf{x}^a\mathbf{x}\mathbf{y}\mathbf{x}^{-a} = \mathbf{x}^{2a+1}\mathbf{y}, \quad (\mathbf{x}^a\mathbf{y})\mathbf{x}\mathbf{y}(\mathbf{x}^a\mathbf{y})^{-1} = \mathbf{x}^{2a-1}\mathbf{y} = \mathbf{x}^{2(a-1)+1}\mathbf{y},$$

so the conjugacy class of $\mathbf{x}\mathbf{y}$ is all $\mathbf{x}^{2a+1}\mathbf{y}$ as a varies. □

The first parts of Theorems 4.1 and 4.2 are a noticeable contrast between $D_{2^{n-1}}$ and Q_{2^n}: at least half the elements of the dihedral group have order 2 and at least half the elements of Q_{2^n} have order 4. The only elements of $D_{2^{n-1}}$ with order 4 are $r^{2^{n-2}}$ and its inverse. What are the elements of Q_{2^n} with order 2?

Corollary 4.3. *For $n \geq 2$, the only element of Q_{2^n} with order 2 is $\mathbf{x}^{2^{n-2}}$.*

Proof. This is easy for $n = 2$. For $n \geq 3$, since $\mathbf{x}$ has order 2^{n-1} its only power with order 2 is $\mathbf{x}^{2^{n-2}}$. Each element of Q_{2^n} that is not a power of $\mathbf{x}$ has order 4 by Theorem 4.2(1). □

Remark 4.4. While Theorem 4.2 lists some properties common to the groups Q_{2^n} for all $n \geq 3$, Q_8 has a feature not shared by its larger analogues. In Q_8 every subgroup is normal, but for $n \geq 4$ the group Q_{2^n} has the non-normal subgroup $\langle \mathbf{y} \rangle = \{1, \mathbf{y}, \mathbf{y}^2, \mathbf{y}^3\} = \{1, \mathbf{y}, \mathbf{x}^{2^{n-2}}, \mathbf{x}^{2^{n-2}}\mathbf{y}\}$. This is not normal because $\mathbf{x}\mathbf{y}\mathbf{x}^{-1} = \mathbf{x}^2\mathbf{y}$, which is not in $\langle \mathbf{y} \rangle$ because $1 < 2 < 2^{n-2}$.

By Theorem 3.2(4), $g\mathbf{x}^a g^{-1} = \mathbf{x}^{\pm a}$ for all $g \in Q_{2^n}$, so every subgroup of $\langle \mathbf{x} \rangle$ is normal in Q_{2^n}. All proper subgroups of Q_8 are normal: $\langle 1 \rangle$, $\langle -1 \rangle$, $\langle i \rangle$, $\langle j \rangle$, and $\langle k \rangle$. What are the proper normal subgroups of Q_{2^n} for $n \geq 4$?

Corollary 4.5. *For $n \geq 4$, the proper normal subgroups of Q_{2^n} are the subgroups of $\langle \mathbf{x} \rangle$ and the two subgroups $\langle \mathbf{x}^2, \mathbf{y} \rangle$ and $\langle \mathbf{x}^2, \mathbf{x}\mathbf{y} \rangle$, which are both of index 2 and are isomorphic to $Q_{2^{n-1}}$.*

Proof. We indicated above why all subgroups of $\langle \mathbf{x} \rangle$ are normal in Q_{2^n}. Let N be a proper normal subgroup of Q_{2^n} such that $N \not\subset \langle \mathbf{x} \rangle$. Pick $g \in N$ with $g \notin \langle \mathbf{x} \rangle$. Then $g = \mathbf{x}^a\mathbf{y}$ for some a, so $g^2 = \mathbf{y}^2 = \mathbf{x}^{2^{n-2}}$ by the proof of Theorem 4.2(1). By Theorem 3.2(4), $g\mathbf{x}g^{-1} = \mathbf{x}^{-1}$. Since N is a normal subgroup of Q_{2^n}, N contains

$$g(\mathbf{x}g^{-1}\mathbf{x}^{-1}) = (g\mathbf{x}g^{-1})\mathbf{x}^{-1} = \mathbf{x}^{-2},$$

so $N \supset \langle \mathbf{x}^2 \rangle$. Since $[Q_{2^n} : \langle \mathbf{x}^2 \rangle] = 4$ and $|N| > |\langle \mathbf{x}^2 \rangle|$, $[Q_{2^n} : N] = 2$. The coset representatives of $Q_{2^n}/\langle \mathbf{x}^2 \rangle$ are $\{1, \mathbf{x}, \mathbf{y}, \mathbf{x}\mathbf{y}\}$ (see proof of Theorem 4.2(3)), so N is one of

$$\langle \mathbf{x}^2, \mathbf{x} \rangle = \langle \mathbf{x} \rangle, \quad \langle \mathbf{x}^2, \mathbf{y} \rangle, \quad \langle \mathbf{x}^2, \mathbf{x}\mathbf{y} \rangle.$$

Discard the first one since $N \neq \langle \mathbf{x} \rangle$. The second and third subgroups are distinct and have index 2 in Q_{2^n} (why?), so they are both normal. Since $\mathbf{x}^2$ has order 2^{n-2}, the second and third subgroups are isomorphic to $Q_{2^{n-1}}$ by Theorem 3.3 with n replaced by $n - 1$. □

Corollary 4.6. *For $n \geq 2$, every subgroup of Q_{2^n} is cyclic or generalized quaternion.*

Proof. The result is true for $n = 2$ and 3, so take $n \geq 4$. Since Q_{2^n} is a 2-group, every proper subgroup of Q_{2^n} is contained in an index-2 subgroup. Index-2 subgroups are normal, so they are cyclic or isomorphic to $Q_{2^{n-1}}$ by Corollary 4.5, and thus we're done by induction. □

It is natural to ask if the group $\mathrm{Aut}(Q_{2^n})$ has an explicit description. If $n = 3$ then $\mathrm{Aut}(Q_8) \cong S_4$ [5]. For $n \geq 4$, the following answer was pointed out to me by Sean Cotner as an application of the "universal" description of Q_{2^n} in Theorem 3.3. I later found it appears in a more general form as [3, Cor. 1.2, p. 156].

Theorem 4.7. *For $n \geq 4$,*

$$\mathrm{Aut}(Q_{2^n}) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/(2^{n-1}))^\times, b \in \mathbf{Z}/(2^{n-1}) \right\}.$$

In particular, for $n \geq 4$ the order of $\mathrm{Aut}(Q_{2^n})$ is 2^{2n-3}.

Proof. Each automorphism f of Q_{2^n} is determined by where it sends $\mathbf{x}$ and $\mathbf{y}$. Since $f(\mathbf{x})$ has order 2^{n-1} and all elements outside $\langle \mathbf{x}\rangle$ have order 4, which is less than 2^{n-1}, we must have $f(\mathbf{x}) = \mathbf{x}^a$ with a odd, so $f(\langle \mathbf{x}\rangle) = \langle \mathbf{x}\rangle$. Then $f(\mathbf{y}) \notin \langle \mathbf{x}\rangle$, so

$$f(\mathbf{x}) = \mathbf{x}^a, \quad f(\mathbf{y}) = \mathbf{x}^b\mathbf{y}$$

where $a \in (\mathbf{Z}/(2^{n-1}))^\times$ and $b \in \mathbf{Z}/(2^{n-1})$.

Conversely, for $a \in (\mathbf{Z}/(2^{n-1}))^\times$ and $b \in \mathbf{Z}/(2^{n-1})$ we will show there is a unique automorphism of Q_{2^n} sending $\mathbf{x}$ to $\mathbf{x}^a$ and $\mathbf{y}$ to $\mathbf{x}^b\mathbf{y}$. We have $\langle \mathbf{x}^a, \mathbf{x}^b\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{x}^b\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle = Q_{2^n}$ since $\langle \mathbf{x}^a\rangle = \langle \mathbf{x}\rangle$, so by Theorem 3.3 it suffices to show

- $(\mathbf{x}^a)^{2^{n-1}} = 1$,
- $(\mathbf{x}^b\mathbf{y})^4 = 1$,
- $(\mathbf{x}^b\mathbf{y})(\mathbf{x}^a)(\mathbf{x}^b\mathbf{y})^{-1} = \mathbf{x}^{-a}$,
- $(\mathbf{x}^a)^{2^{n-2}} = (\mathbf{x}^b\mathbf{y})^2$.

That $(\mathbf{x}^a)^{2^{n-1}} = 1$ follows from $\mathbf{x}^{2^{n-1}} = 1$. That $(\mathbf{x}^b\mathbf{y})^4 = 1$ follows from Theorem 4.2(1). By Theorem 3.2(4), $(\mathbf{x}^b\mathbf{y})(\mathbf{x})(\mathbf{x}^b\mathbf{y})^{-1} = \mathbf{x}^{-1}$, and raising both sides to the ath power gives us $(\mathbf{x}^b\mathbf{y})(\mathbf{x}^a)(\mathbf{x}^b\mathbf{y})^{-1} = \mathbf{x}^{-a}$. To prove

$$(\mathbf{x}^a)^{2^{n-2}} = (\mathbf{x}^b\mathbf{y})^2,$$

we compute each side separately. On the left, $(\mathbf{x}^a)^{2^{n-2}} = (\mathbf{x}^{2^{n-2}})^a = (\mathbf{y}^2)^a = \mathbf{y}^2$ since $\mathbf{y}^2$ has order 2 and a is odd. On the right, a calculation at the start of the proof of Theorem 4.2 tells us $(\mathbf{x}^b\mathbf{y})^2 = \mathbf{y}^2$.

We have shown $\mathrm{Aut}(Q_{2^n})$ is parametrized by pairs (a, b) in $(\mathbf{Z}/(2^{n-1}))^\times \times \mathbf{Z}/(2^{n-1})$: for each (a, b), there is a unique $f_{a,b} \in \mathrm{Aut}(Q_{2^n})$ determined by the conditions $f_{a,b}(\mathbf{x}) = \mathbf{x}^a$ and $f_{a,b}(\mathbf{y}) = \mathbf{x}^b\mathbf{y}$. For two automorphisms $f_{a,b}$ and $f_{c,d}$,

$$(f_{a,b} \circ f_{c,d})(\mathbf{x}) = f_{a,b}(\mathbf{x}^c) = (f_{a,b}(\mathbf{x}))^c = (\mathbf{x}^a)^c = \mathbf{x}^{ac}$$

and

$$(f_{a,b} \circ f_{c,d})(\mathbf{y}) = f_{a,b}(\mathbf{x}^d\mathbf{y}) = (f_{a,b}(\mathbf{x}))^d f_{a,b}(\mathbf{y}) = \mathbf{x}^{ad}(\mathbf{x}^b\mathbf{y}) = \mathbf{x}^{ad+b}\mathbf{y}.$$

Therefore $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$. Since $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} ac & ad+b \\ 0 & 1 \end{smallmatrix}\right)$, we get an isomorphism

$$\mathrm{Aut}(Q_{2^n}) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/(2^{n-1}))^\times, b \in \mathbf{Z}/(2^{n-1}) \right\}$$

by $f_{a,b} \mapsto \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$. □

Corollary 4.8. *For $n \geq 2$ and each pair of elements g and h in $Q_{2^n} - \langle \mathbf{x}\rangle$, there is a unique automorphism f of Q_{2^n} fixing all of $\langle \mathbf{x}\rangle$ and $f(g) = h$.*

Proof. Each f in $\mathrm{Aut}(Q_{2^n})$ is determined by the values $f(\mathbf{x}) = \mathbf{x}^a$ and $f(\mathbf{y}) = \mathbf{x}^b\mathbf{y}$, where $a \in (\mathbf{Z}/(2^{n-1}))^\times$ and $b \in \mathbf{Z}/(2^{n-1})$. That f fixes all of $\langle \mathbf{x}\rangle$ means $a \equiv 1 \bmod 2^{n-1}$. What does the condition $f(g) = h$ tell us?

Write $g = \mathbf{x}^i\mathbf{y}$ and $h = \mathbf{x}^j\mathbf{y}$ where i and j are unique mod 2^{n-1}. Then $f(g) = f(\mathbf{x})^i f(\mathbf{y}) = \mathbf{x}^i\mathbf{x}^b\mathbf{y} = \mathbf{x}^{i+b}\mathbf{y}$, so the condition $f(g) = h$ says $\mathbf{x}^{i+b}\mathbf{y} = \mathbf{x}^j\mathbf{y}$, meaning $b \equiv j - i \bmod 2^{n-1}$. Thus $f_{1,j-i}$ fixes all of $\langle \mathbf{x}\rangle$, maps g to h, and is the only such automorphism of Q_{2^n}. □

Since $\mathbf{Z}/(2^{n-1})$ is generated by 1 and $(\mathbf{Z}/(2^{n-1}))^\times$ is generated by -1 and 5, $\mathrm{Aut}(Q_{2^n})$ has the 3 generators $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and $C = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbf{Z}/(2^{n-1}))$, which satisfy the 6 relations $A^{2^{n-1}} = 1$, $B^{2^{n-3}} = 1$, $C^2 = 1$, $BAB^{-1} = A^5$, $CAC^{-1} = A^{-1}$, and $BC = CB$. This is shown to be a presentation of $\mathrm{Aut}(Q_{2^n})$ in [9].

Remark 4.9. There is a description of $\mathrm{Aut}(D_m)$, for $m \geq 3$, that is similar to our description of $\mathrm{Aut}(Q_{2^n})$. The group D_m is "universal" as a group described by $\langle r, s\rangle$ where $r^m = 1$, $s^2 = 1$, and $srs^{-1} = r^{-1}$. That means every group of the form $\langle x, y\rangle$ where $x^m = 1$, $y^2 = 1$, and $yxy^{-1} = x^{-1}$ admits a unique homomorphism from D_m where $r \mapsto x$ and $s \mapsto y$. Each automorphism of D_m has to send r to an r^a where $(a, m) = 1$ (the elements of order m) and s to an $r^b s$ (since $\langle r\rangle \mapsto \langle r^a\rangle = \langle r\rangle$), so

$$\mathrm{Aut}(D_m) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/(m))^\times, b \in \mathbf{Z}/(m) \right\},$$

where each $f \in \mathrm{Aut}(D_m)$ corresponds to the matrix $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ where $f(r) = r^a$ and $f(s) = r^b s$. Thus $\mathrm{Aut}(Q_{2^n}) \cong \mathrm{Aut}(D_{2^{n-1}})$ for $n \geq 4$, even though $Q_{2^n} \ncong D_{2^{n-1}}$. (What if $n = 3$? We have $\mathrm{Aut}(Q_8) \cong S_4$ and $\mathrm{Aut}(D_4) \cong D_4$.)

Here is an interesting role for the groups Q_{2^n} alongside cyclic p-groups.

Theorem 4.10. *For a finite p-group, the following conditions are equivalent:*

(1) *there is a unique subgroup of order p,*
(2) *all abelian subgroups are cyclic,*
(3) *the group is cyclic or generalized quaternion.*

Proof. See the appendix. □

Corollary 4.11. *When p is an odd prime, a finite p-group is cyclic if and only if it has one subgroup of order p. A finite 2-group of order at least 4 is cyclic if and only if it has one subgroup of order 2 and one subgroup of order 4.*

Proof. For $n \geq 3$, Q_{2^n} has at least 2 subgroups of order 4, such as $\langle \mathbf{x}^{2^{n-3}}\rangle$ and $\langle \mathbf{y}\rangle$. □

Corollary 4.12. *If D is a division ring, every Sylow subgroup of a finite subgroup of $D^\times$ is cyclic or generalized quaternion.*

Proof. For a finite abelian subgroup A of $D^\times$, each equation $a^n = 1$ has at most n solutions in A, so A is cyclic. Thus we can apply the second part of Theorem 4.10 to Sylow subgroups of a finite subgroup of D. □

Remark 4.13. Amitsur [2] classified all finite groups in division rings.

Theorem 4.10 is also applicable to the Sylow subgroups of finite groups with periodic cohomology. (Groups with periodic cohomology arise in studying group actions on spheres.) The finite groups with periodic cohomology were determined by Zassenhaus [8] for solvable groups and by Suzuki [7] for non-solvable groups.

While Theorem 3.3 provides a criterion to recognize a generalized quaternion group in terms of generators and relations, Theorem 4.10 provides a more abstract criterion: the non-cyclic 2-groups with a unique element of order 2 are the generalized quaternion groups. Here is a nice use of this, relying partly on Galois theory for finite fields.

Corollary 4.14. *Let F be a finite field not of characteristic 2. The 2-Sylow subgroups of $\mathrm{SL}_2(F)$ are generalized quaternion groups.*

Proof. (Taken from [4, p. 43].) The only element of order 2 in $\mathrm{SL}_2(F)$ is $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, so a 2-Sylow subgroup of $\mathrm{SL}_2(F)$ has a unique element of order 2. Therefore the 2-Sylow subgroup is either a cyclic group or a generalized quaternion group. We need to eliminate the cyclic option. It would be *wrong* to do this just by writing down two noncommuting elements

of 2-power order in $\mathrm{SL}_2(F)$, because that by itself doesn't imply the 2-Sylow subgroups are noncommutative (and hence not cyclic): elements of 2-power order need not generate a subgroup of 2-power order. For example, the dihedral group $D_n = \langle r, s\rangle$ ($n \geq 3$) is generated by the two reflections s and rs, which both have order 2.

Let $q = |F|$, so q is an odd prime power and $|\mathrm{SL}_2(F)| = q(q^2-1)$. We are going to show every $A \in \mathrm{SL}_2(F)$ with 2-power order has order dividing either $q+1$ or $q-1$. These numbers are both even, so the highest power of 2 in $|\mathrm{SL}_2(F)|$ is not a factor of $q+1$ or $q-1$ and therefore the order of a 2-Sylow subgroup is not the order of an element of $\mathrm{SL}_2(F)$. Thus a 2-Sylow subgroup can't be cyclic.

Since the characteristic polynomial of A has degree 2, its eigenvalues λ and μ are in F or a quadratic extension of F, and $\lambda\mu = 1$ since $\det A = 1$. If $\lambda = \mu$ either both eigenvalues are 1 or both are -1, which would imply A is conjugate to either $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} -1 & b \\ 0 & -1 \end{smallmatrix}\right)$, and these have 2-power order only when $b = 0$, so $A = \pm I_2$. The order of A is 1 or 2, which both divide $q+1$ and $q-1$.

Now we may assume $\lambda \neq \mu$, so A is diagonalizable over a field containing its (distinct) eigenvalues. We will show $A^{q-1} = I_2$ or $A^{q+1} = I_2$. If the eigenvalues of A are in F then A is conjugate over F to $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$, so $A^{q-1} = I_2$. If A's eigenvalues are not in F then the characteristic polynomial of A is irreducible over F, so λ and μ are F-conjugate. Thus $\mu = \lambda^q$ by Galois theory for finite fields, so $1 = \lambda\mu = \lambda^{q+1}$ and $\mu^{q+1} = 1/\lambda^{q+1} = 1$. Since A is conjugate (over a quadratic extension of F) to $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$, $A^{q+1} = I_2$. □

A 2-Sylow subgroup of $\mathrm{SL}_2(F)$ can be written down explicitly when $q \equiv 1 \bmod 4$. Let 2^k be the highest power of 2 in $q-1$, so the highest power of 2 in $q(q^2-1) = q(q-1)(q+1)$ is 2^{k+1}. The group $F^\times$ is cyclic of order $q-1$, so it contains an element a with order 2^k. Let $x = \left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Both are in $\mathrm{SL}_2(F)$, x has order 2^k, y has order 4, $x^{2^{k-1}} = -I_2 = y^2$, and $y \notin \langle x\rangle$, so $\langle x, y\rangle \cong Q_{2^{k+1}}$ by the same argument as in Example 3.4. In particular, $\langle x, y\rangle$ has order 2^{k+1}, so it is a 2-Sylow subgroup of $\mathrm{SL}_2(F)$.

As an example of this, when $q = 5$ we can use $a = 2$: the 2-Sylow subgroup of $\mathrm{SL}_2(\mathbf{F}_5)$ is $\langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\rangle$ and is isomorphic to Q_8. For $k \geq 1$, the highest power of 2 dividing $3^{2^k} - 1$ is $k+2$, so the 2-Sylow subgroup of $\mathrm{SL}_2(\mathbf{F}_{3^{2^k}})$ is isomorphic to $Q_{2^{k+2}}$.

Alas, when $q \equiv 3 \bmod 4$ the group $F^\times$ has no elements of 2-power order besides ± 1, since the highest power of 2 in $q-1$ is 2. So the explicit construction above of a 2-Sylow subgroup of $\mathrm{SL}_2(F)$ no longer works. For a generator and relations method of showing the 2-Sylow subgroup of $\mathrm{SL}_2(F)$ is generalized quaternion when $q \equiv 3 \bmod 4$, see [1, p. 147].

What if F has characteristic 2? Letting $q = |F|$, which is a power of 2, the 2-Sylow subgroups of $\mathrm{SL}_2(F)$ have order q and $\{\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) : x \in F\}$ is a subgroup of order q that is isomorphic to the additive group of F. So a 2-Sylow in $\mathrm{SL}_2(F)$ is a direct sum of cyclic groups of order 2, since that is the group structure of F (additively).

What can be said about the structure of the p-Sylow subgroups of $\mathrm{SL}_2(F)$ at odd primes p? If p is the characteristic of F, then the p-Sylow subgroup is isomorphic to F by the same argument used in the previous paragraph. If p is an odd prime dividing q^2-1 then the p-Sylow subgroups of $\mathrm{SL}_2(F)$ are cyclic, but we omit the proof.

5. More generalized quaternion groups

In Remark 3.5 we met a family of groups of order $4m$ for $m \geq 2$: the quotient groups

$$(\mathbf{Z}/(2m) \rtimes \mathbf{Z}/(4))/\langle (m, 2)\rangle \tag{5.1}$$

where the group law on $\mathbf{Z}/(2m) \rtimes \mathbf{Z}/(4)$ is given by $(a,b)(c,d) = (a + (-1)^b c, b + d)$ and $(m, 2)$ is in the center of $\mathbf{Z}/(2m) \rtimes \mathbf{Z}/(4)$ with order 2. Write (5.1) as Q_{4m}. It is called both the generalized quaternion group of order $4m$ and the *dicyclic* group of order $4m$. When $m = 2^{n-2}$ for $n \geq 3$, Q_{4m} is the group Q_{2^n} we met already. As before, set $Q_4 = \mathbf{Z}/(4)$.

Earlier results we proved for the groups Q_{2^n} for $n \geq 3$ all generalize to Q_{4m} for $m \geq 2$. We will state the generalizations below and leave proofs to the reader except at the end.

Here are generalizations of Theorems 3.2 and 3.3.

Theorem 5.1. *In Q_{4m}, let $\mathbf{x} = \overline{(1,0)}$ and $\mathbf{y} = \overline{(0,1)}$. Then $Q_{4m} = \langle \mathbf{x}, \mathbf{y} \rangle$, where*

1. *$\mathbf{x}$ has order $2m$ and $\mathbf{y}$ has order 4,*
2. *every element of Q_{2m} can be written in the form $\mathbf{x}^a$ or $\mathbf{x}^a\mathbf{y}$ for some $a \in \mathbf{Z}$,*
3. *$\mathbf{x}^m = \mathbf{y}^2$,*
4. *for each $g \in Q_{4m}$ such that $g \notin \langle \mathbf{x} \rangle$, $g\mathbf{x}g^{-1} = \mathbf{x}^{-1}$.*

Theorem 5.2. *For $m \geq 2$, let $G = \langle x, y \rangle$ where $x^{2m} = 1$, $y^4 = 1$, $yxy^{-1} = x^{-1}$, and $x^m = y^2$. There is a unique homomorphism $Q_{4m} \to G$ such that $\mathbf{x} \mapsto x$ and $\mathbf{y} \mapsto y$, and it is onto. If $|G| = 4m$, then this homomorphism is an isomorphism.*

There is a matrix model for Q_{4m} in $\mathrm{GL}_2(\mathbf{C})$ that generalizes Example 3.4: set $x = \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \overline{\zeta} \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ where $\zeta = e^{2\pi i/(2m)} = e^{\pi i/m}$. Check x has order $2m$, y has order 4, $x^m = y^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $yxy^{-1} = x^{-1}$. Use Theorem 5.2 to show $\langle x, y \rangle \cong Q_{4m}$.

Here are generalizations of Theorem 4.2 and its first two corollaries.

Theorem 5.3. *For $m \geq 2$, Q_{4m} has the following properties:*

1. *the subgroup $\langle \mathbf{x} \rangle$ has index 2 and every element of Q_{4m} outside of $\langle \mathbf{x} \rangle$ has order 4,*
2. *the center of Q_{2m} is $\{1, \mathbf{x}^m\} = \{1, \mathbf{y}^2\}$ and $Q_{4m}/Z(Q_{4m}) \cong D_m$,*
3. *the commutator subgroup of Q_{4m} is $\langle \mathbf{x}^2 \rangle$, with $Q_{4m}/\langle \mathbf{x}^2 \rangle \cong \mathbf{Z}/(2) \times \mathbf{Z}/(2)$ for even m and $Q_{4m}/\langle \mathbf{x}^2 \rangle \cong \mathbf{Z}/(4)$ for odd m.*
4. *there are $m + 3$ conjugacy classes, with representatives given in the following table.*

Rep.	1	$\mathbf{x}$	$\mathbf{x}^2$	$\cdots$	$\mathbf{x}^{m-1}$	$\mathbf{x}^m$	$\mathbf{y}$	$\mathbf{xy}$
Size	1	2	2	$\cdots$	2	1	m	m

TABLE 3. Conjugacy class representatives in Q_{4m}.

The description of $Q_{2m}/\langle \mathbf{x}^2 \rangle$ in (3) is different when m is even and odd since the relation $\mathbf{x}^m = \mathbf{y}^2$ in Q_{4m} implies that in $Q_{2m}/\langle \mathbf{x}^2 \rangle$, $\overline{\mathbf{y}}^2 = \overline{1}$ for even m and $\overline{\mathbf{y}}^2 = \overline{\mathbf{x}} \neq \overline{1}$ for odd m.

Corollary 5.4. *For $m \geq 1$, the only element of Q_{4m} with order 2 is $\mathbf{x}^m$.*

Corollary 5.5. *For even $m \geq 4$, the proper normal subgroups of Q_{4m} are the subgroups of $\langle \mathbf{x} \rangle$ and the two subgroups $\langle \mathbf{x}^2, \mathbf{y} \rangle$ and $\langle \mathbf{x}^2, \mathbf{xy} \rangle$, which are both of index 2 and are isomorphic to Q_{2m}. For odd $m \geq 3$, the proper normal subgroups of Q_{4m} are the subgroups of $\langle \mathbf{x} \rangle$.*

For odd m, the reason $\langle \mathbf{x}^2, \mathbf{y} \rangle$ and $\langle \mathbf{x}^2, \mathbf{xy} \rangle$ are not index-2 subgroups of Q_{4m} is that these subgroups contain $\mathbf{x}$ and thus are all of Q_{4m}: $\mathbf{y}^2 = \mathbf{x}^m = \mathbf{x}^{m-1}\mathbf{x} = (\mathbf{x}^2)^{(m-1)/2}\mathbf{x}$, so $\mathbf{x} \in \langle \mathbf{x}^2, \mathbf{y} \rangle$, and similarly, $(\mathbf{xy})^2 = \mathbf{y}^2 = (\mathbf{x}^2)^{(m-1)/2}\mathbf{x}$, so $\mathbf{x} \in \langle \mathbf{x}^2, \mathbf{xy} \rangle$. The description of the proper normal subgroups of Q_{4m} in Corollary 5.5 for even m (but not for odd m)

resembles that of the proper normal subgroups of the dihedral group $D_{2m} = \langle r, s\rangle$ of the same size: the subgroups of $\langle r\rangle$ and also the two index-2 subgroups $\langle r^2, s\rangle$ and $\langle r^2, rs\rangle$.[2]

Here is a generalization of Theorem 4.7 and its corollary.

Theorem 5.6. *For $m \geq 3$,*

$$\mathrm{Aut}(Q_{4m}) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}/(2m))^\times, b \in \mathbf{Z}/(2m) \right\}.$$

Corollary 5.7. *For every pair of elements g and h in $Q_{4m} - \langle \mathbf{x}\rangle$, there is a unique automorphism f of Q_{4m} such that f fixes all of $\langle \mathbf{x}\rangle$ and $f(g) = h$.*

Here is a generalization of Corollary 4.6. We include a proof.

Theorem 5.8. *For $m \geq 1$, every subgroup of Q_{4m} is cyclic or dicyclic. A complete listing of the subgroups of Q_{4m} is as follows:*

(1) *$\langle \mathbf{x}^d\rangle$, where $d \mid 2m$, with index $2d$,*
(2) *$\langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y}\rangle$, where $d \mid m$ and $0 \leq i \leq d-1$, with index d.*

Every subgroup of Q_{4m} occurs exactly once in this listing.

In this theorem, subgroups of the first type are cyclic and subgroups of the second type are dicyclic: $\langle \mathbf{x}^d\rangle \cong \mathbf{Z}/(2m/d)$ and $\langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y}\rangle \cong Q_{4m/d}$.

Proof. It is left to the reader to check $m = 1$. We now assume $m \geq 2$ and adapt the proof of Theorem 3.1 in https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral2.pdf.

Let H be a subgroup of Q_{4m}. Since $\langle \mathbf{x}\rangle$ is cyclic of order $2m$, if $H \subset \langle \mathbf{x}\rangle$ then $H = \langle \mathbf{x}^d\rangle$ where $d \mid 2m$ (and $d > 0$). The order of $\langle \mathbf{x}^d\rangle$ is $2m/d$, so its index in Q_{4m} is $4m/(2m/d) = 2d$.

Now assume $H \not\subset \langle \mathbf{x}\rangle$, so H contains some $\mathbf{x}^i\mathbf{y}$. First we'll treat the case $\mathbf{y} \in H$ and then we'll reduce the more general case (some $\mathbf{x}^i\mathbf{y}$ is in H) to the case $\mathbf{y} \in H$.

The intersection $H \cap \langle \mathbf{x}\rangle$ is a subgroup of $\langle \mathbf{x}\rangle$, so it is $\langle \mathbf{x}^d\rangle$ for some $d > 0$ that divides $2m$. If $\mathbf{y} \in H$ then let's show $d \mid m$ and $H = \langle \mathbf{x}^d, \mathbf{y}\rangle$. Since H contains $\mathbf{y}^2 = \mathbf{x}^m \subset \langle \mathbf{x}^d\rangle$, $d \mid m$. We have $\langle \mathbf{x}^d, \mathbf{y}\rangle \subset H$ since $\mathbf{x}^d$ and $\mathbf{y}$ are in H. To prove the reverse containment, pick $h \in H$. If $h \in \langle \mathbf{x}\rangle$ then $h \in H \cap \langle \mathbf{x}\rangle = \langle \mathbf{x}^d\rangle \subset \langle \mathbf{x}^d, \mathbf{y}\rangle$. If $h \notin \langle \mathbf{x}\rangle$ then $h = \mathbf{x}^i\mathbf{y}$ for some i. Since $\mathbf{y} \in H$, we get $\mathbf{x}^i = h\mathbf{y}^{-1} \in H \cap \langle \mathbf{x}\rangle$, so $\mathbf{x}^i = \mathbf{x}^{dk}$ for some k. Thus $h = \mathbf{x}^i\mathbf{y} = \mathbf{x}^{dk}\mathbf{y} = (\mathbf{x}^d)^k\mathbf{y} \in \langle \mathbf{x}^d, \mathbf{y}\rangle$, so $H \subset \langle \mathbf{x}^d, \mathbf{y}\rangle$.

Consider now the case where $H \not\subset \langle \mathbf{x}\rangle$ and we don't assume $\mathbf{y} \in H$. In H is an element of the form $\mathbf{x}^i\mathbf{y}$. Since $\mathbf{y}$ and $\mathbf{x}^i\mathbf{y}$ are not in $\langle \mathbf{x}\rangle$, by Corollary 4.8 there's an automorphism f of Q_{4m} such that $f(\mathbf{x}) = \mathbf{x}$ and $f(\mathbf{x}^i\mathbf{y}) = \mathbf{y}$. Then $f(H)$ is a subgroup of Q_{4m} containing $\mathbf{y}$, so by the previous paragraph $f(H) = \langle \mathbf{x}^d, \mathbf{y}\rangle$ where $d \mid m$ (and $d > 0$). Then $H = f^{-1}(\langle \mathbf{x}^d, \mathbf{y}\rangle) = \langle f^{-1}(\mathbf{x})^d, f^{-1}(\mathbf{y})\rangle = \langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y}\rangle$. From $\langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y}\rangle = \langle \mathbf{x}^d, \mathbf{x}^j\mathbf{y}\rangle$ for $j \equiv i \bmod d$, we can adjust $i \bmod d$ without affecting $\langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y}\rangle$ and thus write $H = \langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y}\rangle$ where $0 \leq i \leq d-1$.

What is the index of $\langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y}\rangle$ in Q_{4m} when $d \mid m$ and $d > 0$? Because $(\mathbf{x}^i\mathbf{y})\mathbf{x}^k = \mathbf{x}^{-k}(\mathbf{x}^i\mathbf{y})$ and $(\mathbf{x}^i\mathbf{y})^2 = \mathbf{y}^2 = \mathbf{x}^m \in \langle \mathbf{x}^d\rangle$, all elements of $\langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y}\rangle$ that are not powers of $\mathbf{x}$ have the form $(\mathbf{x}^d)^\ell(\mathbf{x}^i\mathbf{y}) = \mathbf{x}^{d\ell}(\mathbf{x}^i\mathbf{y})$. Thus $H = \langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y}\rangle = \langle \mathbf{x}^d\rangle \cup \langle \mathbf{x}^d\rangle\mathbf{x}^i\mathbf{y}$ (a disjoint union), so $|H| = 2|\langle \mathbf{x}^d\rangle| = 2(2m/d)$, which makes $[Q_{4m} : H] = 4m/(2(2m/d)) = d$.

It remains to show the subgroups in the theorem have no duplications. First let's show the two lists are disjoint. Everything in $\langle \mathbf{x}^d\rangle$ commutes with $\mathbf{x}$ while $\langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y}\rangle$ contain $\mathbf{x}^i\mathbf{y}$ that does not commute with $\mathbf{x}$, so these types of subgroups are not equal.

[2]See Theorem 3.8 in https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral2.pdf.

Among subgroups on the first list, there are no duplications since $\langle \mathbf{x}^d \rangle$ determines d when d is a positive divisor of n: it has index $2d$. If two subgroups of the second type are equal, then they have equal index in D_n, say d, so they must be $\langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y} \rangle$ and $\langle \mathbf{x}^d, \mathbf{x}^j\mathbf{y} \rangle$ where i and j are in $\{0, \ldots, d-1\}$. Then $\mathbf{x}^j\mathbf{y} \in \langle \mathbf{x}^d, \mathbf{x}^i\mathbf{y} \rangle = \langle \mathbf{x}^d \rangle \cup \langle \mathbf{x}^d \rangle \mathbf{x}^i\mathbf{y}$, so $\mathbf{x}^j\mathbf{y} = \mathbf{x}^{dk+i}\mathbf{y}$ for some $k \in \mathbf{Z}$. Therefore $j \equiv dk + i \bmod 2m$. We can reduce both sides mod d, since $d \mid m$, to get $j \equiv i \bmod d$. That forces $j = i$ since $0 \leq i, j \leq d-1$. □

Appendix A. Proof of Theorem 4.10

We will prove Theorem 4.10 following the argument in [6, Theorem 9.7.3].

We want to show a nontrivial finite p-group is cyclic or generalized quaternion if it has a unique subgroup of order p or if all of its abelian subgroups are cyclic. (A nontrivial cyclic p-group and a generalized quaternion group have both of these properties.)

We will consider separately abelian and nonabelian p-groups.

If G is a nontrivial abelian p-group, then by the structure theorem for finite abelian groups we can write G as a direct product of cyclic p-groups: $G \cong \mathbf{Z}/(p^{r_1}) \times \cdots \times \mathbf{Z}/(p^{r_d})$. If $d > 1$ then G has more than one subgroup of order p and it has a non-cyclic subgroup (such as G itself). Hence a finite abelian p-group is cyclic if it has a unique subgroup of order p or if all of its (abelian) subgroups are cyclic.

From now on let G be nonabelian. If G has a unique subgroup of order p or if all of its abelian subgroups are cyclic, we want to show G is a generalized quaternion group. If G has a unique subgroup of order p then all of its nontrivial subgroups share this property, so all of its abelian subgroups are cyclic by the previous paragraph. Therefore it suffices to focus on the hypothesis of all abelian subgroups being cyclic, and show (when G is nonabelian) this forces G to be generalized quaternion.

Since G is nonabelian, its center Z is a nontrivial proper subgroup of G, and Z has to be cyclic since it's abelian. For all $g \in G$, the subgroup $\langle g, Z \rangle$ is abelian, hence cyclic. The subgroups of a cyclic p-group are totally ordered, so either $\langle g \rangle \subset Z$ or $Z \subset \langle g \rangle$. Therefore

$$g \notin Z \Longrightarrow Z \subsetneqq \langle g \rangle. \tag{A.1}$$

In particular, $|Z|$ is less than the order of g. So all elements of $G - Z$ must have order at least p^2. If p is odd we will construct an element of $G - Z$ with order p, which is a contradiction, so $p = 2$. If $p = 2$ we will construct an element of $G - Z$ with order 4, so $|Z| = 2$.

Since G/Z is nontrivial, it contains an $\overline{a}$ with order p: $a \notin Z$ and $a^p \in Z$. Thus $\langle a^p \rangle \subset Z \subsetneqq \langle a \rangle$ by (A.1). Since $\langle a^p \rangle$ has index p in $\langle a \rangle$, and $Z \neq \langle a \rangle$, we must have

$$Z = \langle a^p \rangle.$$

Subgroups of a cyclic p-group are totally ordered, so all proper subgroups of $\langle a \rangle$ are in Z.

Since $a \notin Z$, some $b \in G$ does not commute with a. Therefore $\langle a \rangle \cap \langle b \rangle$ is a proper subgroup of $\langle a \rangle$, so $\langle a \rangle \cap \langle b \rangle \subset Z$. At the same time, Z is a subgroup of $\langle a \rangle$ and $\langle b \rangle$ by (A.1), so

$$Z = \langle a \rangle \cap \langle b \rangle.$$

Since $b \notin \langle a \rangle$, $\langle a \rangle \cap \langle b \rangle$ is a proper subgroup of $\langle b \rangle$, so $\langle a \rangle \cap \langle b \rangle = \langle b^{p^r} \rangle$ for some $r \geq 1$. Since $\langle a \rangle \cap \langle b \rangle = Z = \langle a^p \rangle$, b^{p^r} and a^p generate the same group, so $b^{p^r} = a^{pk}$ for some k not divisible by p. Since $\langle a^k \rangle = \langle a \rangle$ and $\langle a^{pk} \rangle = \langle a^p \rangle$, we can rename a^k as a to have $b^{p^r} = a^p$ while still having

$$\langle a \rangle \cap \langle b \rangle = Z = \langle a^p \rangle = \langle b^{p^r} \rangle.$$

Since $Z = \langle a^p \rangle \subset \langle a \rangle \cap \langle b^{p^{r-1}} \rangle \subset \langle a \rangle$ and $a \notin \langle b^{p^{r-1}} \rangle$ (a and b do not commute), the second inclusion is strict, so $\langle a \rangle \cap \langle b^{p^{r-1}} \rangle = Z$. Now we rename $b^{p^{r-1}}$ as b, so $b^p = a^p$ and

$$\langle a \rangle \cap \langle b \rangle = Z = \langle a^p \rangle.$$

Let $c = b^{-1}$, so a and c do not commute (recall a and b do not commute). Up to this point, all we have used about a is that $\overline{a}$ has order p in G/Z. (In the course of the proof we replaced a with a power a^k such that $(p, k) = 1$, but this doesn't change the condition that $\overline{a}$ has order p.) Since G/Z is a nontrivial p-group, its center is nontrivial, so we could have chosen a from the beginning such that $\overline{a}$ is an element of order p in the center of G/Z. Make that choice. Then in G/Z, $\overline{a}$ and $\overline{c}$ commute, so

$$ca = acz \tag{A.2}$$

for some $z \in Z$ with $z \neq 1$. Rewriting (A.2) as $a^{-1}ca = cz$ and raising to the p-th power, $a^{-1}c^p a = c^p z^p$. Since $c^p = b^{-p} = a^{-p}$, we obtain $1 = z^p$. From (A.2) and induction,

$$(ac)^n = a^n c^n z^{\binom{n}{2}} \tag{A.3}$$

for all positive integers n. Setting $n = p$ in (A.3),

$$(ac)^p = a^p c^p z^{p(p-1)/2} = a^p a^{-p} z^{p(p-1)/2} = z^{p(p-1)/2}.$$

If $p \neq 2$ then p is a factor of $p(p-1)/2$, so $z^{p(p-1)/2} = 1$ because $z^p = 1$. Thus $(ac)^p = 1$. Since $c \notin \langle a \rangle$, $ac \neq 1$, so ac has order p. But $ac \notin \langle a \rangle \supset Z$, so ac is an element of order p in $G - Z$, which we noted earlier is impossible. Hence $p = 2$, so G is a 2-group and $z^2 = 1$.

Returning to (A.3) and setting $n = 4$,

$$(ac)^4 = a^4 c^4 z^6 = a^4 b^{-4} (z^2)^3 = 1,$$

so ac has order dividing 4. Since $(ac)^2 = a^2 c^2 z = a^2 b^{-2} z = z \neq 1$, ac has order 4. Since $ac \notin \langle a \rangle \supset Z$, $|Z| < 4$ by (A.1), so $|Z| = 2$.

There is a normal subgroup $N \lhd G$ with order 4. It must be abelian, so it is cyclic. Consider the conjugation action of G on N, which is a group homomorphism $G \to \mathrm{Aut}(N) \cong \{\pm 1\}$. The center of G has order 2, while N has order 4, so not every element of G commutes with every element of N, which means the conjugation action $G \to \mathrm{Aut}(N)$ is onto. Let K be the kernel, so K has index 2 in G and thus is a normal subgroup of G. All abelian subgroups of K are cyclic because it is so in G. Since $|K| < |G|$, by induction K is either cyclic or generalized quaternion. Since N is abelian, $N \subset K$ (look at the definition of K), so $N \subset Z(K)$. Then the center of K has size at least 4, which means K is not generalized quaternion, so K is cyclic.

In the cyclic 2-group K there are two elements of order 4, which are inverses of each other. If these are the only elements of G with order 4 then each element not of order 1 or 2 has these as powers of it, so commutes with them. The elements of order 1 or 2 commute with everything since they are in the center of G, so the elements of order 4 in K commute with everything. That means $|Z(G)| \geq 4$, a contradiction. Thus there has to be some $y \in G - K$ with order 4. Since $y \notin K$, y acts by conjugation nontrivially on N.

Set $|G| = 2^n$ and $K = \langle x \rangle$, so x has order 2^{n-1}, $N = \langle x^{2^{n-3}} \rangle$, and $Z = \langle x^{2^{n-2}} \rangle$. Since the conjugation action of y on N is nontrivial,

$$yx^{2^{n-3}}y^{-1} = x^{-2^{n-3}}.$$

Since $K \lhd G$, $yxy^{-1} = x^i$ for some i. We have $G = \langle x, y \rangle$ since K has index 2 and $y \notin K$, so x and y don't commute (G is nonabelian). Therefore $yxy^{-1} \neq x$, so $i \not\equiv 1 \bmod 2^{n-1}$.

We have $y^2 \in K$, since $[G : K] = 2$, and $x^{2^{n-2}}$ is the only element of order 2 in K, so

$$y^2 = x^{2^{n-2}}.$$

Therefore $y^2xy^{-2} = y(yxy^{-1})y^{-1} = yx^iy^{-1} = (yxy^{-1})^i = x^{i^2}$, so $i^2 \equiv 1 \bmod 2^{n-1}$. When $n = 3$ we have $i^2 \equiv 1 \bmod 4$ and $i \not\equiv 1 \bmod 4$, so $i \equiv -1 \bmod 4$. Now let $n \geq 4$. From $i^2 \equiv 1 \bmod 2^{n-1}$, we get $i \equiv \pm 1$ or $2^{n-2} \pm 1 \bmod 2^{n-1}$. We want to show $i \equiv -1 \bmod 2^{n-1}$, since then $G \cong Q_{2^n}$ by Theorem 3.3. We know already that $i \not\equiv 1 \bmod 2^{n-1}$, so it remains to eliminate the choices $i \equiv 2^{n-2} \pm 1 \bmod 2^{n-1}$.

Assume $i \equiv 2^{n-2} \pm 1 \bmod 2^{n-1}$. Then $x^i = x^{2^{n-2}\pm 1} = y^2x^{\pm 1}$, so $yxy^{-1} = y^2x^{\pm 1}$. Therefore

$$xy^{-1} = yx^{\pm 1}.$$

If $xy^{-1} = yx^{-1}$ then $xy^{-1} = (xy^{-1})^{-1}$, so $(xy^{-1})^2 = 1$. Elements of order 1 and 2 in G are in $Z \subset \langle x \rangle$, so xy^{-1} is a power of x. Thus y is a power of x, but x and y don't commute. We have a contradiction. If instead $xy^{-1} = yx$ then $xy^{-1}x^{-1} = y$. Conjugating this by x, $x^2y^{-1}x^{-2} = xyx^{-1} = y^{-1}$, so x^2 and y commute. Then x^2 is in the center of G. The center has order 2 and x^2 has order $2^{n-2} > 2$, so we have a contradiction. Alternatively, we get a contradiction since the subgroup $\langle x^2, y \rangle$ is abelian and not cyclic since $\langle y \rangle$ and $\langle x^{2^{n-3}} \rangle$ are two subgroups of it with order 4.

References

[1] A. Adem and R. J. Milgram, "Cohomology of Groups," 2nd ed., Springer-Verlag, Berlin, 2004.

[2] S. A. Amitsur, Finite subgroups of division rings, *Trans. Amer. Math. Soc.* **80** (1955), 361–386.

[3] M. Golasiński and D. L. Gonçalves, Spherical space forms – homotopy types and self-equivalences, pp. 153–165 in "Categorial Decomposition Techniques in Algebraic Topology" (ed. G. Arone, J. Hubbuck, R. Levi, M. Weiss), Birkhäuser, Basel, 2004.

[4] D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968.

[5] M. Kato, Automorphism group of the quaternion group, https://math.stackexchange.com/questions/195932.

[6] W. R. Scott, "Group Theory," Dover, New York, 1987.

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

[8] H. Zassenhaus, Über endliche Fastkörper, *Abh. Math. Sem. Hamburg Univ.* **11** (1935), 187–220.

[9] D. G. Zhu and G. X. Zuo, The automorphism group and holomorph of quaternion group (in generalized sense), *Acta Math. Sci. Ser. A (Chin. ed.)* **25** (2005), 79–83.