GENERALIZED QUATERNIONS

KEITH CONRAD

1. Introduction

The quaternion group Q_8 is one of the two non-abelian 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 overlapping condition $i^2 = j^2 = -1$ and the conjugacy relation $jij^{-1} = -i = i^{-1}$. More generally, for odd a we have $j^aij^{-a} = -i = i^{-1}$, while for even a we have $j^aij^{-a} = i$ for even a. We can combine these into the single formula

$$j^aij^{-a} = i^{(-1)^a}$$

for all integers a. These relations suggest the following way of building the quaternion group from scratch.

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: $\overline{(a, b)} = \mathbf{i}^a\mathbf{j}^b$.

To create an isomorphsm $Q \to Q_8$, we will back up and 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

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

which are the same. 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 surjection is an isomorphism. $\square$

3. Generalized Quaternions

While Q_8 is made out of two cyclic groups of order 4, we can extend the construction by letting one of the two cyclic groups be any 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 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. *In Q_{2^n}, let $\mathbf{x} = \overline{(1,0)}$ and $\mathbf{y} = \overline{(0,1)}$. Then $Q_{2^n} = \langle \mathbf{x}, \mathbf{y}\rangle$, where*

1. *$\mathbf{x}$ has order 2^{n-1}, $\mathbf{y}$ 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 any $g \in Q_{2^n}$ 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 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): A typical element of $\mathbf{Z}/(2^{n-1}) \rtimes \mathbf{Z}/(4)$ has the form $(a,b) = (1,0)^a(0,1)^b$, so every 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} and $(2^{n-2},2) = (1,0)^{2^{n-2}}(0,1)^2$, $\mathbf{x}^{2^{n-2}} = \mathbf{y}^{-2} = \mathbf{y}^2$ in Q_{2^n}. Therefore in a product $\mathbf{x}^a\mathbf{y}^b$ we can absorb any even power of $\mathbf{y}$ into the power of $\mathbf{x}$, which means we can take $b = 0$ or $b = 1$.

(4): Any $g \notin \langle \mathbf{x} \rangle$ 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 of Q_4 makes sense and 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 $\#G = 2^n$ 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 $Q_{2^n} \to G$, we back up and start with a map out of a semi-direct product to G.

Let $f\colon \mathbf{Z}/(2^{n-1}) \rtimes \mathbf{Z}/(4) \to G$ by $f(a,b) = x^ay^b$. 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 $y^bxy^{-b} = x^{(-1)^b}$. First we have

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

and next we have

$$f(a,b)f(c,d) = x^ay^bx^cy^d = x^a(y^bx^cy^{-b})y^{b+d} = x^a(y^bxy^{-b})^cy^{b+d} = x^ax^{(-1)^bc}y^{b+d}.$$

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 $\mathbf{x}^a\mathbf{y}^b \mapsto x^ay^b$, so G is a homomorphic image of Q_{2^n}.

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

Theorem 3.3 is true when $n = 2$ if 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. Let $\zeta = e^{2\pi i/2^{n-1}}$, a root of unity of order 2^{n-1}. In $\mathrm{GL}_2(\mathbf{C})$, the matrix $x = \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \overline{\zeta} \end{smallmatrix}\right)$ 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 $2^{n-1}|\#\langle x, y\rangle$. 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, and m be a positive integer divisible by 4. There is an element of A with order 2. Pick one, say ε. Consider the semi-direct product $G = A \rtimes (\mathbf{Z}/(m))$, with group law as in (3.1). Since $-\varepsilon = \varepsilon$ and $m/2$ is even, a short calculation shows $(\varepsilon, m/2)$ is in the center of G and has order 2. The quotient group

$$G/\langle(\varepsilon, m/2)\rangle$$

generalizes the construction of Q_{2^n} (which is the special case $A = \mathbf{Z}/(2^{n-1})$, $m = 4$). This group is noncommutative as long as A has an element of order greater than 2. When A is cyclic of even order $2r$ (but not necessarily a 2-group, *e.g.*, $A = \mathbf{Z}/(6)$ for $r = 3$) and $m = 4$, this group is called a *dicyclic group*. It has order $4r$ with generators x and y such that $x^{2r} = 1$, $yxy^{-1} = x^{-1}$, and $x^r = y^2$.

4. Dihedral and Generalized Quaternion Groups

For all $n \geq 3$, the dihedral group $D_{2^{n-1}}$ and quaternion group Q_{2^n}, both of order 2^n, are similar in a number of ways. 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 last conditions imply it, but we included it to make the similarity with dihedral groups clearer. 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 groups of size 4.

We will state without proof a catch-all theorem about the groups $D_{2^{n-1}}$ and then see what the 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

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

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 $\mathbf{x}^{2^{n-2}} = \mathbf{y}^2$ 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 $2^{n-1}|2a$, so $2^{n-2}|a$, which means $\mathbf{x}^a$ is a power of $\mathbf{x}^{2^{n-2}}$.

No element of Q_{2^n} that is not a power of $\mathbf{x}$ is in the center, since $\mathbf{x}(\mathbf{x}^a\mathbf{y})\mathbf{x}^{-1} = \mathbf{x}^{a+1}\mathbf{x}\mathbf{y} = \mathbf{x}^{a+2}\mathbf{y} \neq \mathbf{x}^a\mathbf{y}$. (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 $\overline{\mathbf{x}\mathbf{y}}^{-1} = \overline{\mathbf{x}}^{-1}$. 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}. That $Q_{2^n}/\langle \mathbf{x}^2 \rangle \cong \mathbf{Z}/(2) \times \mathbf{Z}/(2)$ is left to the reader.

(4): For each $g \in Q_{2^n}$ we will 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 $g = \mathbf{x}^k$. 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 $\{\mathbf{x}^k, \mathbf{x}^{-k}\}$, which has size 2 as long as $\mathbf{x}^{2k} \neq 1$. The two exceptions here are $g = 1$ and $g = \mathbf{x}^{2^{n-2}}$, which are in the center.

If $g = \mathbf{y}$ then

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

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

Finally, if $g = \mathbf{xy}$ then

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

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

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. *The only element of Q_{2^n} with order 2 is $\mathbf{x}^{2^{n-2}}$:*

Proof. Since $\mathbf{x}$ has order 2^{n-1}, its only power with order 2 is $\mathbf{x}^{2^{n-2}}$. Any element of Q_{2^n} that is not a power of $\mathbf{x}$ has order 4 by Theorem 4.2(1). $\square$

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 higher 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 does not belong to $\langle \mathbf{y} \rangle$ because $2 < 2^{n-2}$.

Corollary 4.5. *Any normal subgroup $N \lhd Q_{2^n}$ which is nonabelian has index 1 or 2.*

Proof. Since N is nonabelian, $N \not\subset \langle \mathbf{x} \rangle$. Pick $g \in N$ with $g \notin \langle \mathbf{x} \rangle$. Then g has order 4 (Theorem 4.2(1)), so g^2 has order 2. That means $g^2 = \mathbf{x}^{2^{n-2}}$ (Corollary 4.3). Every element of Q_{2^n} outside of $\langle \mathbf{x} \rangle$ conjugates $\mathbf{x}$ into $\mathbf{x}^{-1}$ (Theorem 3.2(4)), so $g\mathbf{x}g^{-1} = \mathbf{x}^{-1}$. 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 $N \supset \langle \mathbf{x}^2, g \rangle$. The subgroup $\langle \mathbf{x}^2 \rangle$ has index 4 in Q_{2^n} and N is strictly larger, so its index is 1 or 2. $\square$

Corollary 4.6. *For $n \geq 4$, $\mathrm{Aut}(Q_{2^n})$ is a 2-group.*

This is not true for $n = 3$: $\mathrm{Aut}(Q_8) \cong S_4$.

Proof. If $\mathrm{Aut}(Q_{2^n})$ is not a 2-group, it has an element f of odd order > 1. Set $G = \langle \mathbf{x} \rangle$. All elements Q_{2^n} outside of G have order 4 (Theorem 4.2(1)), while G is cyclic of order $2^{n-1} > 4$ (since $n \geq 4$), so f must send any generator of G to another generator of G. Therefore $f(G) = G$, so f restricts to an automorphism of G. Since $G \cong \mathbf{Z}/(2^{n-1})$, $\mathrm{Aut}(G) \cong (\mathbf{Z}/(2^{n-1}))^\times$, which is a 2-group ($\varphi(2^{n-1}) = 2^{n-2}$), so f must be the identity on G because f has odd order.

Since $f(G) = G$, also $f(Q_{2^n} - G) = Q_{2^n} - G$. Although $Q_{2^n} - G$ is not a group, it is a set and f is a permutation of this set. The size of $Q_{2^n} - G$ is $2^n - 2^{n-1} = 2^{n-1}$, a power of 2, and f has odd order as a permutation on this set, so it must have a fixed point: $f(q) = q$ for some $q \in Q_{2^n} - G$. Then f is the identity on the subgroup $\langle G, q \rangle = \langle \mathbf{x}, q \rangle$, which is Q_{2^n} since G has index 2 in Q_{2^n}. $\square$

Here is an interesting role for the generalized quaternion groups, alongside cyclic p-groups.

Theorem 4.7. *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. $\square$

Corollary 4.8. *Every subgroup of Q_{2^n} is cyclic or generalized quaternion.*

Proof. There is a unique subgroup of order 2 in Q_{2^n}, so every nontrivial subgroup has a unique subgroup of order 2. Now use Theorem 4.7. $\square$

Corollary 4.9. *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 is cyclic if and only if it has one subgroup of order 2 and one subgroup of order 4.*

Proof. A generalized quaternion group Q_{2^n} has at least 2 subgroups of order 4, such as the subgroup of order 4 in $\langle \mathbf{x} \rangle$ and the subgroup $\langle \mathbf{y} \rangle$. $\square$

Corollary 4.10. *If D is a division ring, any Sylow subgroup of a finite subgroup of $D^\times$ is cyclic or generalized quaternion.*

Proof. Any finite abelian subgroup of $D^\times$ is cyclic, so we can apply the second part of Theorem 4.7 to its Sylow subgroups. $\square$

Remark 4.11. The classification of all finite groups in division rings was worked out by Amitsur [2].

Theorem 4.7 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 [6] for solvable groups and by Suzuki [5] for non-solvable groups.

While Theorem 3.3 provides a criterion to recognize a generalized quaternion group in terms of generators and relations, Theorem 4.7 provides a more abstract criterion: a non-cyclic 2-group with a unique element of order 2 is generalized quaternion. Here is a nice use of this, relying partly on Galois theory for finite fields.

Corollary 4.12. *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 [3, 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.

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 $A \in \mathrm{SL}_2(F)$ has order dividing either $q+1$ or $q-1$. Both are even, so the highest power of 2 in $\#\,\mathrm{SL}_2(F)$ is not a factor of $q+1$ or $q-1$ and therefore is not the order of A. Thus a 2-Sylow subgroup can't be cyclic.

We want to show $A^{q-1} = I_2$ or $A^{q+1} = I_2$. 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 $\det A = 1$. Since 2 divides $q+1$ and $q-1$, we may assume $A^2 \neq I_2$, so $\lambda \neq \mu$. Therefore A has distinct eigenvalues, so A is diagonalizable over a field containing its eigenvalues. If the eigenvalues are in F then A is diagonalizable over F and is conjugate to $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$, hence $A^{q-1} = I_2$. If the eigenvalues are not in F then the characteristic polynomial of A is irreducible over F, so λ and μ are Galois conjugate over F. Therefore $\mu = \lambda^q$ 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 to $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$, $A^{q+1} = I_2$. $\square$

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 which 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.

Appendix A. Proof of Theorem 4.7

We will prove Theorem 4.7 following the argument in [4, 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 non-abelian 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 non-abelian. 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 non-abelian, its center Z is a nontrivial proper subgroup of G, and Z has to be cyclic since it's abelian. For any $g \in G$, 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

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

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 $\langle a^p \rangle \subset Z \subsetneq \langle a \rangle$ 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 any 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 $xy^{-1} = yx$ then $xy^{-1}x^{-1} = y$. Conjugating by x again, $x^2y^{-1}x^{-2} = xyx^{-1} = y^{-1}$, so x^2 and y commute. Then x^2 is in the center of G. But 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] D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968.
[4] W. R. Scott, "Group Theory," Dover, New York, 1987.
[5] M. Suzuki, On finite groups with cyclic Sylow subgroups for all odd primes, *Amer. J. Math* **77** (1955), 657–691.
[6] H. Zassenhaus, Über endliche Fastkörper, *Abh. Math. Sem. Hamburg Univ.* **11** (1935), 187–220.