GROUPS OF ORDER 4 AND 6

KEITH CONRAD

1. Introduction

Here are several groups of order 4:

$$\mathbf{Z}/(4),\ \mathbf{Z}/(2)\times\mathbf{Z}/(2),\ (\mathbf{Z}/(5))^\times, (\mathbf{Z}/(8))^\times,\ (\mathbf{Z}/(12))^\times.$$

Here are several groups of order 6:

$$\mathbf{Z}/(6),\ \mathbf{Z}/(2)\times\mathbf{Z}/(3),\ (\mathbf{Z}/(7))^\times,\ S_3,\ D_3,\ \mathrm{GL}_2(\mathbf{Z}/(2)).$$

The groups of order 4 exhibit two types of structure: cyclic ($\mathbf{Z}/(4)$ and $(\mathbf{Z}/(5))^\times$) or built out of two commuting[1] elements of order 2 ($(1,0)$ and $(0,1)$ in $\mathbf{Z}/(2)\times\mathbf{Z}/(2)$, 3 and 5 in $(\mathbf{Z}/(8))^\times$, 5 and 7 in $(\mathbf{Z}/(12))^\times$). Among the groups of order 6, the abelian ones are cyclic and the nonabelian ones can each be interpreted as the group of all permutations of a set of size 3 (the set is $\{1,2,3\}$ for S_3, the 3 vertices of an equilateral triangle for D_3, and the mod 2 vectors $\binom{1}{0}$, $\binom{0}{1}$, and $\binom{1}{1}$ for $\mathrm{GL}_2(\mathbf{Z}/(2))$).

We will show that the examples above exhibit the general situation insofar as groups of order 4 and 6 are concerned: isomorphic to $\mathbf{Z}/(4)$ or $\mathbf{Z}/(2)\times\mathbf{Z}/(2)$ for order 4, and isomorphic to $\mathbf{Z}/(6)$ or S_3 for order 6. That means there are essentially only two types of 4-fold symmetries and essentially only two types of 6-fold symmetries.

2. Groups of Order 4

Theorem 2.1. *Any group of order 4 is isomorphic to $\mathbf{Z}/(4)$ or $\mathbf{Z}/(2)\times\mathbf{Z}/(2)$.*

Proof. Let G have order 4. Any element of G has order 1, 2, or 4. If G has an element of order 4 then G is cyclic, so $G\cong\mathbf{Z}/(4)$ since cyclic groups of the same order are isomorphic. (Explicitly, if $G=\langle g\rangle$ then an isomorphism $\mathbf{Z}/(4)\to G$ is $a \bmod 4\mapsto g^a$.)

Assume G is not cyclic. Then every nonidentity element of G has order 2, so $g^2=e$ for every $g\in G$. Pick two nonidentity elements x and y in G, so $x^2=e$, $y^2=e$, and $(xy)^2=e$. That implies $xy=(xy)^{-1}=y^{-1}x^{-1}=yx$, so *$x$ and y commute.* This argument shows that any group in which all nonidentity elements have order 2 is abelian.

The roles of x and y in G resemble $(1,0)$ and $(0,1)$ in $\mathbf{Z}/(2)\times\mathbf{Z}/(2)$, suggesting the function $f\colon\mathbf{Z}/(2)\times\mathbf{Z}/(2)\to G$ where $f(a \bmod 2, b \bmod 2)=x^ay^b$. Explicitly, this function is

$$(0,0)\mapsto 1,\quad (1,0)\mapsto x,\quad (0,1)\mapsto y,\quad (1,1)\mapsto xy. \tag{2.1}$$

To see that f is a homomorphism, we compute

$$f(\overline{a},\overline{b})f(\overline{c},\overline{d})=(x^ay^b)(x^cy^d)=x^a(y^bx^c)y^d=x^ax^cy^by^d=x^{a+c}y^{b+d}=f(\overline{a+c},\overline{b+d}).$$

The function f is a bijection by (2.1), so f is an isomorphism. $\square$

[1]There is an infinite group generated by two elements of order 2 that do not commute.

3. Groups of Order 6

To describe groups of order 6, we begin with a lemma about elements of order 2.

Lemma 3.1. *If a group has even order then it contains an element of order* 2*.*

Proof. Call the group G. Let us pair together each $g \in G$ with its inverse g^{-1}. The set $\{g, g^{-1}\}$ has two elements unless $g = g^{-1}$, meaning $g^2 = e$. Therefore

$$|G| = 2|\{\text{pairs } \{g, g^{-1}\} : g \neq g^{-1}\}| + |\{g \in G : g = g^{-1}\}|.$$

The left side is even by hypothesis, and the first term on the right side is even from the factor of 2. Therefore $|\{g \in G : g^2 = e\}|$ is even. This count is positive, since $g = e$ is one possibility where $g^2 = e$. Since this count is even, there must be at least one more g, so some $g \neq e$ in G satisfies $g^2 = e$, which implies g has order 2. □

Theorem 3.2. *A group of order* 6 *is isomorphic to* $\mathbf{Z}/(6)$ *or to* S_3*.*

Proof. Let $|G| = 6$ have order 6. By Lemma 3.1, G contains an element x of order 2.

Case 1: G is abelian.

Suppose all nonidentity elements have order 2. Choose y other than x and e, so $y^2 = e$. Since G is abelian, $\{e, x, y, xy\}$ is a subgroup of G, but this violates Lagrange's theorem since 4 doesn't divide 6. Therefore some element of G has order 3 or 6.

If G has an element of order 6 then G is cyclic and $G \cong \mathbf{Z}/(6)$. If some $z \in G$ has order 3 then xz has order 6 since $(xz)^6 = e$, $(xz)^2 = x^2z^2 = z^2 \neq e$, and $(xz)^3 = x^3z^3 = x \neq e$. Thus again G is cyclic, so $G \cong \mathbf{Z}/(6)$.

Case 2: G is nonabelian.

Step 1: G has an element of order 2 and an element of order 3.

No element has order 6, so orders of elements are 1, 2, or 3. If every nonidentity element had order 2, G would be abelian (see pf. of Theorem 2.1), so G has an element of order 3.

Step 2: Make G look like S_3.

By Step 1, in G there are elements x of order 2 and y of order 3. Let $H = \langle x \rangle = \{e, x\}$, so H has 3 left cosets. Since $y \notin H$ and $y^2 \notin H$, the left cosets of H are H, yH, and y^2H.

For each $g \in G$, let $\ell_g \colon \{H, yH, y^2H\} \to \{H, yH, y^2H\}$ by $\ell_g(cH) = gcH$ for left cosets cH. Each ℓ_g is a permutation since it has inverse $\ell_{g^{-1}}$. Labeling H, yH, and y^2H as 1,2,3, the permutations of $\{H, yH, y^2H\}$ are placed inside S_3, and thus we can view ℓ_g in S_3.[2]

The function $G \to S_3$ where $g \mapsto \ell_g$ is a homomorphism, because multiplication in G goes over to composition of permutations: $\ell_g \circ \ell_{g'} = \ell_{gg'}$ since for any left coset cH

$$(\ell_g \circ \ell_{g'})(cH) = g(g'cH) = gg'cH = (gg')cH = \ell_{gg'}(cH).$$

The homomorphism $G \to S_3$ by $g \mapsto \ell_g$ is between finite groups of equal size, so to prove it's an isomorphism it suffices to show it's injective or surjective. We'll prove it's surjective.

The permutation ℓ_y cyclically permutes H, yH, and y^2H: H to yH, yH to y^2H, and y^2H to $y^3H = H$, so the image of $G \to S_3$ contains a 3-cycle. Let's check ℓ_x transposes yH and y^2H. Since $x \in H$, $\ell_x(H) = xH = H$. Since ℓ_x is a permutation, if $\ell_x(yH) \neq y^2H$ then $\ell_x(yH) = yH$, so $xyH = yH$: $\{xy, xyx\} = \{y, yx\}$. Thus xy is y or yx. If $xy = y$ then $x = e$ (false) and if $xy = yx$ then x and y commute, so xy has order 6 (false: G is nonabelian). Thus $\ell_x(yH) = y^2H$ and $\ell_x(y^2H) = yH$: ℓ_x is a transposition in S_3. The image of $G \to S_3$ is a subgroup of S_3 containing a transposition and element of order 3, so it has order 6 by Lagrange. Thus $G \cong S_3$. □

[2] The specific way we view ℓ_g in S_3 depends on the way we label the left cosets of H as 1, 2, and 3.

The fact that, up to isomorphism, there are two groups of order 4 and two groups of order 6, goes back to Cayley's 1854 paper on groups [1], which was the first work on abstract groups; previously groups had been considered only as groups of permutations. Almost 25 years later, Cayley wrote in [2] "The general problem is to find all the groups of a given order n," and then proceeded to claim there are *three* groups of order 6: see Figure 1. From Cayley's examples it appears he thought $\mathbf{Z}/(6)$ and $\mathbf{Z}/(2)\times\mathbf{Z}/(3)$ are not isomorphic, which confused form with structure.

The general problem is to find all the groups of a given order n; thus if $n = 2$, the only group is $1, \alpha$ $(\alpha^2 = 1)$; $n = 3$, the only group is $1, \alpha, \alpha^2$ $(\alpha^3 = 1)$; $n = 4$, the groups are $1, \alpha, \alpha^2, \alpha^3$ $(\alpha^4 = 1)$, and $1, \alpha, \beta, \alpha\beta$ $(\alpha^2 = 1, \beta^2 = 1, \alpha\beta = \beta\alpha)$;* $n = 6$, there are three groups, a group $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$ $(\alpha^6 = 1)$; and two groups $1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2$ $(\alpha^2 = 1. \beta^3 = 1)$, viz: in the first of these $\alpha\beta = \beta\alpha$; while in the other of them (that mentioned above) we have $\alpha\beta = \beta^2\alpha$, $\alpha\beta^2 = \beta\alpha$.

* If $n = 5$, the only group is $1, a, a^2, a^3, a^4$ $(a^5 = 1)$. W. E. S.

FIGURE 1. Cayley's error in [2]: three groups of order 6.

References

[1] A. Cayley, "On the Theory of Groups, as Depending on the Symbolic Equation $\theta^n = 1$," pp. 123–130 of *The Collected Papers of Arthur Cayley*, Vol. II, Cambridge Univ. Press, 1889.

[2] A. Cayley "Desiderata and Suggestions," *Amer. J. Mathematics* **1** (1878), pp. 50-52.