## Groups of Order Six

In this handout, we'll use Lagrange's Theorem to prove:

**Theorem**. Let $G$ be a group of order 6. Then $G$ is isomorphic either to $C_6$ or to $S_3$.

(That is, up to isomorphism, there are only two groups of order 6. We haven't formally defined "isomorphic" yet, so that portion of the proof will be a little handwavy for now.)

To this end, we will follow the outline suggested by Exercise 10.14 in Saracino's textbook.

Throughout this handout, let $G$ be an arbitrary group of order 6

---

**Lemma 1**. If $G$ has an element of order 6, then $G$ is cyclic.

**Proof of Lemma 1**. If there is some $x \in G$ with $o(x) = 6$, then the cyclic subgroup $\langle x \rangle \subseteq G$ has $o(x) = 6$ elements, and hence $\langle x \rangle = G$. Thus, $G$ is cyclic, generated by $x$. QED Lemma 1

---

**Lemma 2**. If $G$ is not cyclic, then all elements of $G$ have order 1, 2, or 3.

**Proof of Lemma 2**. By Theorem 10.4, every $x \in G$ has order dividing 6, and thus $o(x)$ is 1, 2, 3, or 6. By part (a), since $G$ is not cyclic, we cannot have $o(x) = 6$, and thus $o(x)$ is 1, 2, or 3. QED Lemma 2

---

**Lemma 3**. If $G$ is not cyclic, then there is some $a \in G$ of order 3.

**Proof of Lemma 3**. Suppose, toward contradiction, that $G$ has no elements of order 3. Then by Lemma 2, all elements of $G$ have order 1 or 2. That is, $g^2 = e$ for all $g \in G$. By Problem 3.11, $G$ is abelian.

Pick $x \in G \smallsetminus \{e\}$ and $y \in G \smallsetminus \{e, x\}$, so that $e, x, y \in G$ are three distinct elements. Define $H = \{e, x, y, xy\}$. We claim that $H$ is a subgroup of $G$ of order 4.

To see that $|H| = 4$, we need to show that all four elements we listed are distinct; we already saw that $e, x, y$ are distinct. If $xy = x$, then $y = e$ by cancellation, a contradiction. If $xy = y$, then $x = e$, another contradiction. If $xy = e$, then multiplying by $x$, we have $y = x$ since $x^2 = e$, again giving a contradiction. Thus, $H$ does indeed have four elements.

To see that $H$ is a group, note that it is nonempty and (since $g^2 = e$ for all $g \in G$) every element is its own inverse, and hence $H$ is closed under inverses. It suffices to show that $H$ is closed under the operation.

Given $g, h \in H$, if $g = e$, then $gh = h \in H$; similarly if $h = e$. If $g = h$, then $gh = g^2 = e \in H$. The only remaining cases are that $g, h$ are two distinct elements of $\{x, y, xy\}$. Recalling that $G$ is abelian, we have $yx = xy \in H$, and $(xy)x = x(xy) = ey = y \in H$, and $y(xy) = (xy)y = xe = x \in H$. Thus, $H$ is indeed closed under the operation, proving our claim that $H \subseteq G$ is a subgroup of order 4.

By Lagrange's Theorem, we must have $|H| \big| |G|$, and hence $4|6$, a contradiction. Thus, our assumption that $G$ has no elements of order 3 is false. That is, there is some $a \in G$ with $o(a) = 3$. QED Lemma 3

---

For Lemmas 4–6, let us make the following assumptions:

$$G \text{ is not cyclic, } a \in G \text{ has order 3, and fix } b \in G \smallsetminus \langle a \rangle \qquad (\star)$$

**Lemma 4**. Assume $(\star)$. Then $e, a, a^2, b, ab, a^2b$ are all distinct.

**Proof of Lemma 4**. Since $\langle a \rangle$ has $o(a) = 3$ elements, we know that $e, a, a^2$ are all distinct. By our choice of $b$, we know that $b$ is also distinct from all three of $e, a, a^2$.
In addition, the three elements $b, ab, a^2b$ must be different from one another; otherwise, multiplying all three on the right by $b^{-1}$, we would have $e, a, a^2$ not all distinct, and contradiction.
It remains to show that each of $ab$ and $a^2b$ is distinct from each of $e, a, a^2$.
If $ab = e$, then multiplying by $a^2$ on the left gives $b = a^2$, a contradiction.
If $ab = a$, then multiplying by $a^2$ on the left gives $b = e$, a contradiction.
If $ab = a^2$, then multiplying by $a^2$ on the left gives $b = a$, a contradiction.
Similarly, if $a^2b$ equals one of $e$, $a$, or $a^2$, then multiplying on the right by $a$ gives $b$ is one of $a$, $a^2$, or $e$, a contradiction.
Thus, all six of $e, a, a^2, b, ab, a^2b$ are distinct. QED Lemma 4

---

**Lemma 5**. Assume $(\star)$. Then $o(a^jb) = 2$ for all $j = 0, 1, 2$.

**Proof of Lemma 5**. We claim that $b^2 = e$, proceeding by contradiction. If $b^2 = a^jb$ for some $j = 0, 1, 2$, then multiplying on the right by $b^{-1}$ gives $b = a^j$, a contradiction. If $b^2 = a$, then $b^3 = ab \neq e$, and hence $o(b) \neq 1, 2, 3$, contradicting Lemma 2. Similarly, if $b^2 = a^2$, then $b^3 = a^2b \neq e$, again contradicting Lemma 2. By process of elimination, then, $b^2 = e$, as claimed. Since $b \neq e$ and $b^2 = e$, we have $o(b) = 2$.
Going back to assumption $(\star)$, recall that $b$ was chosen arbitrarily from the set $G \setminus \langle a \rangle$, and through Lemmas 4 and 5 we deduced that $o(b) = 2$. Thus, we really proved a "for all" statement, that *every* element of $G \setminus \langle a \rangle$ has order 2. QED Lemma 5

---

**Lemma 6**. Assume $(\star)$. Then $ba = a^2b$ and $ba^2 = ab$.

**Proof of Lemma 6**. Since $o(ab) = 2$, we have $abab = e$, and hence $ba = a^{-1}b^{-1} = a^2b$, where the last equality is because $o(a) = 3$ and $o(b) = 2$.
Finally, $ba^2 = baa = a^2ba = a^2a^2b = ab$. QED Lemma 6

---

---

**Proof of Theorem**. **Case 1**: $G$ has an element $x$ of order 6. Then by Lemma 1, $G$ is cyclic. (And by renaming $x^j$ as $j$ for each $j = 0, 1, \ldots, 5$, we see that $G$ is isomorphic to $C_6$.)

**Case 2**: $G$ has no element of order 6. Then by Lemma 3, there is some $a \in G$ of order 3. Choose $b \in G \setminus \langle a \rangle$. By Lemma 4, the six elements of $G$ are $\{a^ib^j \mid i \in \{0, 1, 2\} \text{ and } j \in \{0, 1\}\}$, and Lemmas 5 and 6 show us that the multiplication table for $G$ must be

| * | $e$ | $a$ | $a^2$ | $b$ | $ab$ | $a^2b$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $b$ | $ab$ | $a^2b$ |
| $a$ | $a$ | $a^2$ | $e$ | $ab$ | $a^2b$ | $b$ |
| $a^2$ | $a^2$ | $e$ | $a$ | $a^2b$ | $b$ | $ab$ |
| $b$ | $b$ | $a^2b$ | $ab$ | $e$ | $\boxed{a^2}$ | $\boxed{a}$ |
| $ab$ | $ab$ | $\boxed{b}$ | $\boxed{a^2b}$ | $a$ | $e$ | $\boxed{a^2}$ |
| $a^2b$ | $a^2b$ | $\boxed{ab}$ | $\boxed{b}$ | $a^2$ | $\boxed{a}$ | $e$ |

where the boxed values are from computations like $(ab)(a^2b) = a(ba^2)b = a(ab)b = a^2b^2 = a^2$.

Replacing $a$ with the 3-cycle $(1, 2, 3) \in S_3$, and $b$ with the 2-cycle $(1, 2)$, the above multiplication table coincides with that of $S_3$, with $a^2 = (1, 3, 2)$, with $ab = (1, 3)$, and with $a^2b = (2, 3)$. QED