

CONTENTS

1. Review: the counting formula	1
2. Classifying groups of order six	1

1. REVIEW: THE COUNTING FORMULA

Let $H \leq G$. Last time we saw that G is partitioned into the left cosets of H , and that G/H denotes the set of *distinct* left cosets. If $R \subseteq G$ contains exactly one representative of each left coset, then

$$G = \bigsqcup_{r \in R} rH.$$

Since each coset rH is in bijection with H , counting both sides gives the following.

Theorem 1.1 (Counting formula). *If G is finite and $H \leq G$, then*

$$|G| = |G/H| \cdot |H| = [G : H] |H|. \quad (1.1)$$

In particular (Lagrange's theorem), if $x \in G$ then $\text{ord}(x) = |\langle x \rangle|$ divides $|G|$.

2. CLASSIFYING GROUPS OF ORDER SIX

Let $|G| = 6$. Lagrange's theorem (Theorem 1.1) shows that an element can have order 1, 2, 3, or 6. We first establish that elements of orders 2 and 3 must occur.

Lemma 2.1. *Every finite group of even order contains an element of order 2.*

Proof. Pair each element a with its inverse a^{-1} . The distinct sets $\{a, a^{-1}\}$ partition G into parts of size one or two. A part has size one exactly when $a = a^{-1}$. If the identity were the only such element, then $|G|$ would be one plus an even number, hence odd. Thus there is some $a \neq e_G$ with $a = a^{-1}$. It satisfies $a^2 = e_G$ and has order 2. $\square$

Here is a similar exercise from the homework:

Question 2.1. Show that every group of order 35 has an element of order 5 or 7.

Hints: If there are no elements of order 5, show that every element has order 7 or 1 (the identity). Now if x and y are elements of order 7, show that the subgroups $\langle x \rangle$ and $\langle y \rangle$ are either equal or contain just the identity element in common. Now count!

Lemma 2.2. *If $a^2 = e_G$ for every $a \in G$, then G is abelian.*

Proof. Every element is its own inverse, so for $a, b \in G$,

$$ba = b^{-1}a^{-1} = (ab)^{-1} = ab.$$

$\square$

Proposition 2.1. *A group of order 6 contains an element of order 3.*

Proof. Suppose first that every nonidentity element has order 2. The preceding lemma makes G abelian. Choose distinct nonidentity elements a, b . Then

$$K = \{e_G, a, b, ab\} = \langle a, b \rangle$$

is a subgroup: since a, b commute and $a^2 = b^2 = e_G$, every product of powers of a, b reduces to one of these four elements. They are distinct: $ab = e_G$ would imply $a = b$, while $ab = a$ or $ab = b$ would force $b = e_G$ or $a = e_G$, respectively. Thus $|K| = 4$, contradicting Lagrange's theorem because 4 does not divide 6.

There is therefore an element a whose order is neither 1 nor 2. Its order is 3 or 6. In the first case, take $x = a$. In the second case, take $x = a^2$; then $x^3 = e_G$ and $x \neq e_G$, so x has order 3. $\square$

Choose x of order 3 and y of order 2, and put $H = \langle x \rangle = \{e_G, x, x^2\}$. Since the elements of H have orders 1 or 3, we have $y \notin H$. The coset criterion gives $yH \neq H$. Both cosets have three elements, so

$$G = H \sqcup yH = \{e_G, x, x^2, y, yx, yx^2\}. \quad (2.1)$$

In particular, x and y generate G .

How do x and y multiply? The product xy is an element of G , so it must be one of the six elements listed above. Which one?

First, $xy \notin H$. Indeed, if $xy \in H$, then $y = x^{-1}(xy) \in x^{-1}H = H$, since $x^{-1} \in H$. This contradicts $y \notin H$. Hence $xy \in yH = \{y, yx, yx^2\}$. Moreover $xy \neq y$, since cancelling y would give $x = e_G$. We are left with two possibilities:

$$xy = yx \quad \text{or} \quad xy = yx^2. \quad (2.2)$$

A priori, both could happen.

Proposition 2.2. *Once we know which case of (2.2) holds, the multiplication in G is completely determined.*

Sketch. Let's just explain the idea by way of example: suppose $xy = yx^2$ and $x^3 = y^2 = 1$. Now given two elements of $G = \{1, x, x^2, y, yx, yx^2\}$, we claim that we can always move all the y 's to the left using the above rules. For example,

$$x^2 \cdot (yx) = x \cdot (x \cdot y) \cdot x = x \cdot (yx^2) \cdot x = x \cdot y = yx^2 \quad (2.3)$$

and the latter is one of the elements we listed in G . $\square$

Are there actually groups in which each case occurs? Yes:

- *Case $xy = yx$, $x^3 = e_G$, $y^2 = e_G$.* Now x and y commute, so G is abelian and $(xy)^n = x^n y^n$. Hence

$$(xy)^2 = x^2, \quad (xy)^3 = y, \quad (xy)^4 = x, \quad (xy)^5 = x^2 y, \quad (xy)^6 = e_G.$$

These six powers are distinct, so xy has order 6 and $G = \langle xy \rangle$ is the cyclic group C_6 of order 6. For example, $\mathbb{Z}/6\mathbb{Z}$ with $x = \bar{2}$, $y = \bar{3}$.

- *Case $xy = yx^2$, $x^3 = e_G$, $y^2 = e_G$.* Note that $xy = yx^2$ is equivalent to (taking inverses of both sides and remembering that $y^{-1} = y$ and $x^{-1} = x^2$)

$$yx^2 = y^{-1}x^{-1} = x^{-2}y^{-1} = xy. \quad (2.4)$$

But we have seen these relations before: this is just S_3 : take $x = (1\ 2\ 3)$ and $y = (1\ 3)$.

Theorem 2.1. *Every group of order 6 is isomorphic to exactly one of C_6 and S_3 .*

Proof. By the discussion above, a group of order 6 has elements x, y of orders 3, 2 with $G = \{e_G, x, x^2, y, yx, yx^2\}$, and satisfies one of the relations (2.2). By Proposition 2.2, its multiplication table is then the same as that of C_6 or of S_3 , respectively; matching $y^b x^a$ with the corresponding element gives an isomorphism. The two groups are not isomorphic, since C_6 is abelian and S_3 is not. $\square$