Math 71: Algebra

Groups of Small Order

Amittai Siavava

Keywords: *Sage*, *groups*, *permutations*, *symmetric groups*, *Cayley's theorem*.

1. Introduction

Groups are fundamental to life. Indeed, many people have manipulated groups without realizing, or, tragically, without knowing what groups are. Take, for instance, a machine learning engineer using neural networks to coerce sentiments out of text. It is more obvious that linear algebra is involved – since vectors are used to represent the text data and matrices are used to represent the neural network – but, fundamentally, we can still interpret the process as a map between two abstract sets, that of all the text and that of all possible sentiments. We may also observe some likenesses of homomorphisms. For instance, on the domain $-1 \leq s \leq 1$, suppose good sentiments are positive and bad sentiments are negative, le's say $\phi(\text{“bad”}) = -1$ and $\phi(\text{“good”}) = 1$. Let's say I love food, so I give it an extremely positive sentiment of 0.8. In that case, I may have savored a lot of different dishes, so I necessarily have a high bar for food. *I do not appreciate bad food; in fact, I hate it.* Then my sentiment to bad food will be negative. In the neural network, this may be represented as:

$$\phi(\text{“bad food”}) = \phi(\text{“bad”}) \cdot \phi(\text{“food”}) = -1 \cdot 0.8 = -0.8$$

The more I value something, the more I want it as perfect as possible. If I do not care about something, then I assign it as neutral a sentiment as possible. A group theorist would note that I may not include 0 in my range of sentiments since 0 is a multiplicative annihilator ($0a = a0 = 0$ for all a), so I may assign a neutral sentiment infinitesimal value. Take, for instance, that I do not drink, therefore I do not care how good or bad an alcoholic drink is and I assign $\phi(\text{“alcoholic drink”}) = \varepsilon \approx 0.000001$. By extension, my sentiment to a British alcoholic drink is $\phi(\text{“British alcoholic drink”}) = \phi(\text{“British”}) \cdot \varepsilon \approx \varepsilon$, and the same holds for all other types of alcoholic drinks. Similarly, if “not” is assigned a negative sentiment $-x$, then $\phi(\text{“not bad”}) = \phi(\text{“not”}) \cdot \phi(\text{“bad”}) = (-x) \cdot (-1) = x$, a positive sentiment reflecting the double negation. Arguably, the two domains may be represented as groups, with the sentiment map as some homomorphism of groups. So why is this useful?

In some instances, groups and other structures from abstract algebra shed new light on problems. Take, for instance, the use of Rijndael fields in cryptography. Viewed alone, the Advanced Encryption Standard (AES) algorithm operating on binary numbers makes little sense: an **xor** here, a substitution there, a **shift**, an addition... And good luck proving that it is unbreakable. However, we can interpret AES as operations in the Rijndael field $F = \mathbb{F}_2[x]/f(x)$, where $\mathbb{F}_2[x]$ is the set of polynomials over $\mathbb{F}_2$ and $f(x)$, the encryption key, is also a fixed polynomial in $\mathbb{F}_2[x]$. We can then prove that AES is practically unbreakable using the group-theoretic properties of the field F (*cite).

Similarly, algebraic structures such as groups are reflected in many scenarios. However, to recognize such instances, we first need to understand and identify the unique groups that exist of specific sizes (or, in algebraic terms, we say the groups *up to isomorphism*). This paper attempts to identify all groups orders (sizes) less than or equal to 15.

Contents. In section 2, we start by looking at the trivial group, arguably the simplest group. In section 2, we look at groups of prime order. We then advance to groups of order p^2 with p prime in section 3. In section 4, we return to groups of order 6 and classify those that behave differently. In section 5, we look groups of order 8 and classify those behave differently. We will now have classified all groups of order $n \leq 9$. In section 6, we classify all groups of order 10, 14, and 14. In section 7, we finally classify groups of order 12. Finally, in section 8, we review the results and look at how some occurrences of the groups can be identified.

2. The Trivial Group

The trivial group $G = \{\epsilon\}$ has order $n = 1$ and is arguably the least interesting to study. It contains only a single element, which must be the identity for the defined group operation (since groups must contain the identity element). Furthermore, any (general) group operation $*$ has the property $\epsilon * x = x * \epsilon = x$. In this case, the only option for x in G is ϵ itself, so $\epsilon * \epsilon = \epsilon$. Similarly, $\epsilon^{-1} = \epsilon$, therefore the group has the identity and is closed is closed under the group operation and inversion, but it doesn't have any other interesting structures.

3. Groups of Prime Order

Next, let's look at groups of prime order through some motivating theorems.

Theorem 3.1 (Lagrange). If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$ and the number of left cosets of H in G is equal to $\frac{|H|}{|G|}$. (*1*, p.89, Theorem 8)

Proposition 3.2. If G is a finite group of prime order p then every non-identity element of G has order p.

Proof. Let g be a non-identity element of G, without loss of generality, such that the order of g is $x \in \mathbb{Z}_{\geq 0}$. Then $g^x = \epsilon$. This immediately tells us that x cannot be 1, since g is clearly not the group is identity. Let $\langle g \rangle$ be the set of all elements $g^i, i \in \mathbb{Z}$. Notice that $\langle g \rangle$ contains *at least* two elements: $g^x = \epsilon$, and $g^1 = g$. Now, for arbitrary powers $n \in \mathbb{Z}$, let $ax + b = n$. Then:

$$g^n = g^{ax+b} = (g^x)^a \cdot g^b \epsilon^a \cdot g^b = \epsilon \cdot g^b = g^b$$

This tells us that $\langle g \rangle$ has at most x elements. In fact, $\langle g \rangle$ has exactly x elements since we took distinct powers of g and $g^x = \epsilon$ is the smallest power that cycles back to 0. So;

(a) The set $\langle g \rangle$ is finite (it has x elements).

(b) The set $\langle g \rangle$ is closed under the group operation (since the equivalence of every power of g is in the set).

(c) The set $\langle g \rangle$ contains the identity element.

Therefore, $\langle g \rangle$ is a group. Remember that we picked g from G, and G is itself a group that is closed under the group operation, so $\langle g \rangle \leq G$. The first part of Lagrange's theorem tells us that the order of any subgroup $S \leq G$ *must* divide the order of G. So x must divide p, but p is prime so $x = p$. Therefore, the order of the element g is p. □

Proposition 3.3. If a group of order n contains an element of order n then the group is cyclic.

Proof. Let $g \in G$ such that the order of g is n. Then $g^n = \epsilon$. Consider the set $\langle g \rangle$. As we saw in Proposition 3.2, $\langle g \rangle$ is a group of order n, and it is contained in G. Therefore, $\langle g \rangle = G$ since G has order n. Therefore, G is cyclic. □

Proposition 3.4. All cyclic groups of a fixed order n are isomorphic.

Proof. Let G and H be cyclic groups of order n. Let $g \in G$ and $h \in H$ be generators. Then the map $\psi : G \to H$ defined by $\psi(g) = h$ is an isomorphism.

$$\psi(g) = h$$

$$\psi(g^i) = \psi\left(\prod_{j=0}^{i-1} g\right) = \prod_{j=0}^{i-1} \psi(g) = \prod_{j=0}^{i-1} h = h^i$$

$$\psi(g^i \cdot g^k) = \psi(g^{i+k}) = h^{i+k} = h^i \cdot h^k = \psi(g^i) \cdot \psi(g^k)$$

Therefore, the two groups are isomorphic. □

Proposition 3.5. If G is a cyclic group then G is abelian.

Proof. Let G be a cyclic group of order p, with $g \in G$ as a generator. Then every element can be expressed as g^i for some $i \in \{0, 1, \ldots, p-1\}$, with powers interpreted as repeated application of the group operation. Let $x \in G$ and $y \in G$ such that $x = g^a$ and $y = g^b$. Then:

$$xy = g^a \cdot g^b = g^{a+b} = g^b \cdot g^a = yx \tag{3.6}$$

Therefore, for any $x, y \in G$, $xy = yx$, and G is abelian. □

Corollary 3.7. If G is a finite group of prime order, then G abelian.

Proof. In combining propositions 3.2, 3.3, 3.4, and 3.5, we see that any group of prime order has a generating element, and by expressing every element in the group as a power of the generating element, we see that the group operation commutes for all elements. We also see that all groups of a given prime order p are isomorphic. Therefore, every group of prime order is abelian. □

Definition 3.8. The cyclic group of order p is denoted as C_p (or Z_p, in parallel to the integers $\mathbb{Z} \pmod p$).

In summary, we have shown that every group of prime order is cyclic and abelian. This tells us that there is only a single structure for any groups of a given prime order p: the group C_p. For instance, the only groups of order $2, 3, 5, 7, 11$, and 13 are the groups $C_2, C_3, C_5, C_7, C_{11}$, and C_{13} respectively.

Order	Group	Isomorphisms
2	C_2	$\mathbb{Z}/2\mathbb{Z}$
3	C_3	$\mathbb{Z}/3\mathbb{Z}$
5	C_5	$\mathbb{Z}/5\mathbb{Z}$
7	C_7	$\mathbb{Z}/7\mathbb{Z}$
11	C_{11}	$\mathbb{Z}/11\mathbb{Z}$
13	C_{13}	$\mathbb{Z}/13\mathbb{Z}$

TABLE 1. Groups of prime order $n \leq 15$

4. Cyclic Groups of Non-Prime Order

In proposition 3.3, we saw that any group of order n (without loss of generality) that contains an element of order n is cyclic. For an arbitrary element $g \in G$, let x be the order of g. As we saw in proposition 3.2, the set $\langle g \rangle$ generated by g contains x elements and is a subgroup of G. This restricts x to be a divisor of n. But n divides n, so x might be n (not an occurrence in *every* group, but an occurrence in at least one group of order n – for instance, take 1 in $\mathbb{Z}/n\mathbb{Z}$). Since the order of G is n, Proposition 3.3 tells us that G is cyclic, Proposition 3.4 tells us that all such groups are isomorphic for fixed n, and Proposition 3.5 tells us that G is abelian equivalent to the group C_n.

5. Groups of Order Square Prime

Theorem 5.1 (Cauchy's Theorem). If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p. (*1*, p. 93, Theorem 3.1)

Proposition 5.2. A group G generated by two elements x and y having $\langle x\rangle \cap \langle y\rangle = 1$ is isomorphic to the direct product $\langle x\rangle \times \langle y\rangle$.

Proof. Let G be a group generated by x and y where $\langle x\rangle \cap \langle y\rangle = 1$. Define the map $\psi : \langle x\rangle \times \langle y\rangle \to G$ by:

$$\psi(x^m, y^n) = x^m y^n$$

for all $m, n \in \mathbb{Z}$. Then ψ is an isomorphism,. Therefore, G is isomorphic to $\langle x\rangle \times \langle y\rangle$. □

Proposition 5.3. The direct product of two abelian groups is abelian.

Proof. Let G and H be abelian groups. $a, b \in G$ and $c, d \in H$. Let (a, c) and (b, d) be elements of $G \times H$. Then:

$$\begin{aligned}(a, c) \cdot (b, d) &= (a \cdot b, c \cdot d) \\ &= (b \cdot a, d \cdot c) \quad \text{(Since } G \text{ and } H \text{ are abelian)} \\ &= (b, d) \cdot (a, c)\end{aligned}$$

Therefore, $G \times H$ is abelian. □

Corollary 5.4. If G is a finite group of order p^2 with p prime, then G is abelian. and isomorphic to either C_{p^2} or $C_p \times C_p$.

Proof. Let G be a finite group of order p^2 with p prime. Consider the center $Z(G) \leq G$. By Lagrange's theorem 3.1, we know that $\#Z(G) \mid \#G$, therefore $\#Z(G) \in \{1, p, p^2\}$. Considering these cases;

(a) By the class equation (*1*, p. 125, Theorem 8), we know the center of a group of prime power *must be nontrivial*. Therefore, $\#Z(G) \neq 1$.

(b) If G has an element of order p^2, then G is cyclic, therefore abelian and isomorphic to C_{p^2} as demonstrated in Section 4.

(c) Assuming G does not have an element of order p^2, then every non-identity element must have order p since the order must divide p^2 (see 3.1) and the order is greater than 1 (since the element is not identity). Cauchy's theorem (see 5.1) also tells us that G must have an element of order p. Let x be one such element, generating the subgroup $\langle x\rangle$ of order p. Let $y \in G \setminus \langle x\rangle$, then $\langle y\rangle$ is also a subgroup of order p, and the groups $\langle x\rangle$ and $\langle y\rangle$ intersect trivially. Both $\langle x\rangle$ and $\langle y\rangle$ are cyclic, so $\langle x\rangle \cong \langle y\rangle \cong C_p$ by Corollary 3.7 and Definition 3.8. Now, consider the group $\langle x, y\rangle \simeq \langle x\rangle \times \langle y\rangle$ (by 5.2). Since $x \in G$ and $y \in G$, $\langle x, y\rangle \subseteq G$. Additionally,

$\langle x, y\rangle$ has order p^2 since x has order p and y has order p, so $\langle x, y\rangle = G$. However, $\langle x\rangle$ and $\langle y\rangle$ are abelian, so Proposition 5.3, tells us that G, through its isomorphism to a direct product of two abelian groups, must also be abelian.

□

Using Corollary 5.4, we can classify all groups of order 4 and order 9:

Order	Group	Isomorphisms
4	C_4	$\mathbb{Z}/4\mathbb{Z}$
	$C_2 \times C_2 \simeq V_4$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
9	C_9	$\mathbb{Z}/9\mathbb{Z}$
	$C_3 \times C_3$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

TABLE 2. Groups of order $p^2 \leq 15$ for p prime.

6. Abelian Groups

Theorem 6.1 (The Fundamental Theorem of Finitely Generated Abelian Groups). If a group G is a finitely generated abelian group, then:

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s} \tag{6.2}$$

where

(a) $r \geq 0$ and $n_j \geq 1$ for all j; and
(b) $n_{i+1} \mid n_i$ for all i.
(c) Expression 6.2 is unique.

Using the fundamental theorem of finitely generated abelian groups, we may now classify all abelian groups of order $n \leq 15$ (some of which we have already seen):

Order	Invariant Factors	Group	Isomorphic To
1	1×1	C_1	$\{\epsilon\}, S_1$
2	2×1	C_2	$\mathbb{Z}/2\mathbb{Z}, S_2$
3	3×1	C_3	$\mathbb{Z}/3\mathbb{Z}$
4	4×1	C_4	$\mathbb{Z}/4\mathbb{Z}$
	2×2	$C_2 \times C_2 \simeq V_4$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	5×1	C_5	$\mathbb{Z}/5\mathbb{Z}$
6	6×1	C_6	$\mathbb{Z}/6\mathbb{Z}$
7	7×1	C_7	$\mathbb{Z}/7\mathbb{Z}$
8	8×1	C_8	$\mathbb{Z}/8\mathbb{Z}$
	4×2	$C_4 \times C_2$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
	$2 \times 2 \times 2$	$C_2 \times C_2 \times C_2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
9	9×1	C_9	$\mathbb{Z}/9\mathbb{Z}$
	3×3	$C_3 \times C_3$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
10	10×1	C_{10}	$\mathbb{Z}/10\mathbb{Z}$
11	11×1	C_{11}	$\mathbb{Z}/11\mathbb{Z}$
12	12×1	C_{12}	$\mathbb{Z}/12\mathbb{Z}$
	6×2	$C_6 \times C_2$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
13	13×1	C_{13}	$\mathbb{Z}/13\mathbb{Z}$
14	14×1	C_{14}	$\mathbb{Z}/14\mathbb{Z}$
15	15×1	C_{15}	$\mathbb{Z}/15\mathbb{Z}$

TABLE 3. Abelian groups of order $n \leq 15$

So far, we have classified the trivial group, all groups of prime order $p \leq 15$, all groups of order $p^2 \leq 15$ with p prime, and all abelian groups of order $n \leq 15$. This includes every group of order $1, 2, 3, 4\ (= 2^2), 5, 7, 9\ (= 3^2), 11$, and 13. In the next two sections, let us consider the groups of orders 6 and 8.

7. Groups of Order 6

(a) State Cauchy's theorem and the fundamental theorem of finite abelian groups (giving references, but without proofs; if these are of interest, consider one of the other projects!).

(b) Recall the proof why every group of order p^2 with p prime is abelian.

(c) Classify the *abelian* groups of order $n \leq 15$ up to isomorphism using the fundamental theorem.

(d) Classify groups of order 6 by hand: using Cauchy's theorem, there exists $a \in G$ of order 2 and $b \in G$ of order 3; show that $G = \{1, b, b^2, a, ab, ab^2\}$, in a direct manner that $ba = ab$ or $ba = ab^2$, and show that these two possibilities uniquely determine the Cayley table of G.

Let G be a group of order 6. Cauchy's theorem (see 5.1) tells us that G must have an element of order 2 and an element of order 3. Let $a \in$ be an element of order 2 and $b \in G$ be an element of order 3, so $a^2 = b^3 = \epsilon$. It is trivial that the subgroups $\langle a \rangle$ and $\langle b \rangle$ must intersect trivially:

(a) If $a = b$ then $a^2 = b^2$, but $a^2 = \epsilon$, which contradicts that b has order 3.

(b) If $a = b^2$ then $a^2 = b^4 = b$, which contradicts that $a^2 = \epsilon$.

Consider the group $G = \langle x, y \rangle \{\epsilon, b, b^2, a, ab, ab^2\}$.

(a) Since a has order 2, $a^2 = \epsilon$ so $a^{-1} = a$.

(b) Since b has order 3, $b^3 = \epsilon$, so $b^{-1} = b^2$.

(c) Therefore, either $ab^{-1} = ab$ or $ab^{-1} = ab^2$

Suppose $ab^{-1} = ab$. Since $(xy)^{-1} = y^{-1}x^{-1}$ (generally), this implies that $ab = b^2a$ and $ab^2 = ba$. Therefore, the Cayley table of G is determined as:

	1	b	b^2	a	ab	ab^2
1	1	b	b^2	a	ab	ab^2
b	b	b^2	1	ab	ab^2	a
b^2	b^2	1	b	ab^2	a	ab
a	a	ab	ab^2	1	b	b^2
ab	ab	ab^2	a	b^2	1	b
ab^2	ab^2	a	ab	b	b^2	1

Table 4. Cayley table of G when $ba = ab^2$

The group is not symmetric across the diagonal, therefore not abelian. We may recognize this group as either D_6 or S_3, under the isomorphism:

Isomorphism to D_6

$$\psi\colon D_6 \to G$$
$$\psi(1) \mapsto 1$$
$$\psi(r) \mapsto b$$
$$\psi(s62) \mapsto b^2$$
$$\psi(s) \mapsto a$$
$$\psi(sr) \mapsto ab$$
$$\psi(sr^2) \mapsto ab^2$$

Isomorphism to S_3

$$\phi\colon S_3 \to G$$
$$\phi(1) \mapsto 1$$
$$\phi((1\,2\,3)) \mapsto b$$
$$\phi((1\,3\,2)) \mapsto b^2$$
$$\phi((1\,2)) \mapsto a$$
$$\phi((2\,3)) \mapsto ab$$
$$\phi((1\,3)) \mapsto ab^2$$

In the second case, suppose $ab^{-1} = ab^2$. Since $(xy)^{-1} = y^{-1}x^{-1}$ (generally), this implies that $ab = ba$ and $ab^2 = b^2a$. Therefore, the Cayley table of G is determined as:

	1	b	b^2	a	ab	ab^2
1	1	b	b^2	a	ab	ab^2
b	b	b^2	1	ab	ab^2	a
b^2	b^2	1	b	ab^2	a	ab
a	a	ab	ab^2	1	b	b^2
ab	ab	ab^2	a	b	b^2	1
ab^2	ab^2	a	ab	b^2	1	b

Notice the symmetry across the diagonal, implying that G is abelian. Indeed, in this case G is isomorphic to C_6, with generator $1 \sim ab$ as the image of $1 \in C_6$:

$$\begin{aligned}
\psi &: C_6 \to G \\
\psi(0) &\mapsto (1,1) \sim 1 \\
\psi(1) &\mapsto (a,b) \sim ab \\
\psi(2) &\mapsto (1,b^2) \sim b^2 \\
\psi(3) &\mapsto (a,1) \sim a \\
\psi(4) &\mapsto (1,b) \sim b \\
\psi(5) &\mapsto (a,b^2) \sim ab^2
\end{aligned}$$

Therefore, the groups of order 6 are, up to isomorphism, the groups C_6 and S_3.

8. Groups of Order 8

By Lagrange's theorem (3.1), non-identity elements of G may have orders 2, 4, or 8.

Corollary 8.1. If a group G of order 8 has an element of order G, then G is abelian.

Proof. If G has an element of order 8, then G is cyclic (by 3.3), therefore abelian (by 3.5). □

Corollary 8.2. If G has order 8 and every nonidentity element in G has order 2, then G is abelian.

Proof. Take $a \in G$ of order 2, then $\langle a \rangle$ is an abelian, cyclic subgroup of order 2 (by 3.3). Take $b \in G - a$ of order 2, then $\langle b \rangle$ is also an abelian, cyclic subgroup of order 2. Similarly, take $c \in (G - a) - b$ of order 2, then $\langle c \rangle$ is an abelian, cyclic subgroup of order 2. Now, consider the group $\langle a, b, c \rangle$. Since $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$ intersect trivially, then $\langle a, b, c \rangle$ has order has order 8 and is equal to G. This means G is isomorphic to the direct product $C_2 \times C_2 \times C_2$, therefore abelian (since, by 5.3, the direct product of abelian groups is abelian). □

Proposition 8.3. If an element $b \in G$ has order n, then the conjugates of b have order n.

Proof. Consider the conjugate $b' = bab^{-1}$. Then

$$(b')^n = (bab^{-1})^n = bab^{-1} \cdot bab^{-1} \cdots bab^{-1} = ba^n b^{-1} = b\epsilon b^{-1} = bb^{-1} = \epsilon$$

□

Proposition 8.4. If G is a nonabelian group of order 8 having an element a of order 4 and an element b of order 2, $b \notin \langle a \rangle$, then $G \simeq D_4$.

Proof. Let $a \in G$ be of order 4, with $H = \langle a \rangle$. Take $b \in G - H$ such that b has order 2. Then $\langle b \rangle$ is a cyclic subgroup of order 2. Consider $\langle a \rangle \times \langle b \rangle$, which must have order 8. Therefore, the only elements of order 4 in G are in H. By 8.3, H must be closed under conjugation. Therefore, either $bab^{-1} = a^3$ and $ba^2b^{-1} = a^2$. Then G is isomorphic to D_4, under the isomorphism

$$\phi \colon D_4 \to G$$

$$r \mapsto a$$

$$s \mapsto b$$

$$rs^n \mapsto ba^n$$

□

Proposition 8.5. If G is a nonabelian with elements a and b of order 4, $b \notin \langle a \rangle$, then $G \simeq Q_8$.

Proof. As above, the order must be preserved by conjugation, so $\langle a \rangle$ is normal in G. Similarly, $\langle b \rangle$ is normal in G, so G must contain other elements of order 4. In this case, G has 3 elements of order 4, a, b, c, such that $a^2 = b^2 = c^2 = -\epsilon$, and G is isomorphic to Q_8 under the map

$$\phi \colon G \to Q_8$$

$$1 \mapsto 1$$

$$a \mapsto i$$

$$b \mapsto j$$

$$c \mapsto k$$

□

We have now classified all nonabelian groups of order 8, and all groups of order $n \leq 9$ (since 9 is a square of a prime). Next, let's look at groups of order 10 and higher.

9. Groups of Product-of-Prime Orders

(a) Now let G be a group of order pq where p, q are primes with $p < q$ (without loss of generality).

8′. For +3 bonus going a more conceptual route, replace step (8) as follows.

- Read DF, section 4.4.
- Prove that the automorphism group of Z_p is $\mathrm{Aut}(Z_p) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ (DF, section 4.4, Proposition 16, p. 135 proves something more general). State (but you do not need to prove) that $(\mathbb{Z}/p\mathbb{Z})^\times \simeq Z_{p-1}$ is cyclic.
- Suppose that $p \nmid (q-1)$. Show that G is abelian (DF, Example, section 4.4, p. 135–136) and therefore cyclic (DF, section 4.4, Exercise 2, p. 137).
- Now suppose that $p \mid (q-1)$. Let $P \leq G$ be a p-Sylow subgroup and $Q \leq G$ be a q-Sylow subgroup. Show that $Q \trianglelefteq G$ is normal in G (DF, Example, section 4.5, p. 143).
- Read section 5.5. Show that if $p \mid (q-1)$ then either $G \simeq Z_p \times Z_q \simeq Z_{pq}$ or $G \simeq Z_p \rtimes Z_q$, the semi-direct product with respect to the homomorphism $Z_p \to \mathrm{Aut}(Z_q) \simeq (\mathbb{Z}/q\mathbb{Z})^\times = \langle g \rangle$ mapping $x \mapsto g^{(q-1)/p}$ (DF, Example, section 5.5, pp. 181–182; section 5.5, Exercise 6, pp. 184–185).

Consider the automorphism group of C_n, $\mathrm{Aut}(C_n)$, defined to be the group of all homomorphisms from C_n onto itself. Let $\psi : C_n \to C_n \in \mathrm{Aut}(C_n)$ be an automorphism of C_n. C_n is cyclic, so $\psi(x) = x^a$ for some $a \in \mathbb{Z}/n\mathbb{Z}$. The value of a uniquely determines the automorphism ψ, which we denote as ψ_a. (*1*, see DF Section 4.4, Proposition 16).

Proposition 9.1. $\psi_a \in \mathrm{Aut}(C_n)$ if and only if $\mathbf{gcd}\ (a,\ n) = 1$

Proof. Take an arbitrary element $x^\alpha \in C_n$ such that $g = \mathbf{gcd}\ (\alpha,\ p) > 1$, then α is not coprime to n. Taking the least common multiple of Then $\mathbf{lcm}\ (p,\ \alpha) = \frac{\alpha n}{g}$. Since $g \mid \alpha$, then $\mathbf{lcm}\ (p,\ \alpha) = nm$ for some $m \in \mathbb{Z}$. Therefore, $x^{\mathbf{lcm}\ (n,\ \alpha)} = x^{nm} = 0$ (since $x^n = 0$ in C_n) so the map ψ_a cannot be automorphism of C_n (since its kernel is nontrivial, its image cannot equal C_n). Therefore, whenever $(a, n) > 1$ $\psi_a \notin \mathrm{Aut}(C_n)$. Consequently;

$$\psi_a \in \mathrm{Aut}(C_n) \implies (a, n) = 1$$

□

Proposition 9.2. $Aut(C_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. For the cyclic group $\mathbb{Z}/n\mathbb{Z} \simeq C_n$, we define the group $(\mathbb{Z}/n\mathbb{Z})^\times$ as the multiplicative group of all the units of $\mathbb{Z}/n\mathbb{Z}$, which are all coprime to n. Since $\mathrm{Aut}(C_n)$ is the group of all automorphisms ψ_a of C_n all having a

coprime to n, then $\mathrm{Aut}(C_n)$ has the same number of elements and $(\mathbb{Z}/,\mathbb{Z})^\times$. Define the map

$$f\colon\ \mathrm{Aut}(C_n) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

$$f(1) \mapsto 1$$

$$f(\psi_a) \mapsto a$$

□

Proposition 9.3. If $n = p$ is prime, then $\#Aut(C_p) = p - 1$.

Proof. By Proposition 9.2, $\mathrm{Aut}(C_p)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Recall that $(\mathbb{Z}/p\mathbb{Z})^\times = \{x\colon 1 \le x < p, x \nmid p\}$. Since p is prime, then $\#(\mathbb{Z}/p\mathbb{Z})^\times = p - 1$, so $\#\,\mathrm{Aut}(C_p) = p - 1$. □

Proposition 9.4. If G is a group of order pq with p, q prime and $p \nmid (q - 1)$, then G is abelian.

Proof. Let $\#G = pq$ having $p \nmid (q - 1)$. Consider the center $Z(G) \le G$. Suppose $Z(G) \neq 1$. Lagrange's theorem (see 3.1) forces $Z(G)$ to be cyclic. Let g be a generator of $Z(G)$, then Lagrange's theorem further limits the order of g to be a divisor of pq. Therefore, the order of g may be $1, p, q$, or pq. However;

(a) Nonidentity elements may not have order 1.

(b) If every nonidentity element of G has order p, then the centralizer of every nonidentity element has index q, so the class equation reads

$$pq = 1 + kq$$

This is contradictory, since $q \mid pq$ but $q \nmid (1 + kq)$ (because q does not divide 1). Therefore, all nonidentity elements of G cannot have order p, implying that G must have an element of order q.

(c) If G contains an element x of order q, then let $H = \langle x \rangle$ be the subgroup generated by x. Since H has index p in G and p is the smallest prime dividing $\#G = pq$, H is a normal subgroup in G by Corollary 5 (*1*, p. 120). Since $Z(G) = 1$, then $C_G(H) = 1 \cdot H \cdot 1 = H$. Therefore, the quotient group $G/H = N_G(H)/C_G(H)$ has order p and is isomorphic to a group of $\mathrm{Aut}(H)$ by Corollary 15 (*1*, p. 134). By Proposition 16 (*1*, p. 135), $\mathrm{Aut}(H) \simeq C_{q-1}$. and has order $q - 1$, which implies that $p \mid (q - 1)$ by Lagrange's theorem (3.1), a contradiction of the assumption that $p \nmid (q - 1)$. Therefore, G must be abelian.

□

Now, suppose $p \mid (q - 1)$.

Theorem 9.5 (Sylow's Theorem). Let G be a finite group of order $p^\alpha m$ where p is a prime not dividing m.

1. Sylow p-subgroups of G exist, i.e. $n_p \neq \varnothing$.

2. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q = gPg^{-1}$, i.e. Q is conjugate to P.
3. The number of Sylow p-subgroups of G is of the form $n_p = 1 + kp$, i.e.

$$n_p \equiv 1 \pmod{p}.$$

Further, $n - p$ is the index of $N_G(P)$ in G for any Sylow p-subgroup P, hence

$$n_p \mid m.$$

see (*1*, Theorem 18, p. 139). □

Let $P \leq G$ be a Sylow p-subgroup of G and $Q \leq G$ be a Sylow q-subgroup of G. Sylow's theorem (see 9.5) tells us that $n_q = 1 + kq$ for some $k \geq 0$ and $n_q \mid p$. Since we have $p < q$, it must be that $k = 0$ and $n_q = 1$. By Corollary 20 (*1*, p. 142), Q is normal in G.

Since P and Q are of prime order, they are cyclic and are each generated by a single element (by 3.7). Let $P = \langle p \rangle$ and $Q = \langle q \rangle$. Note that $\mathrm{Aut}(Q) \simeq C_{q-1}$ is cyclic and $p \mid (q-1)$, so Q contains a unique *cyclic* subgroup of order p, say $\langle \gamma \rangle$, and any homomorphism $\psi : P \to \mathrm{Aut}(Q)$ must map $y \in P$ to a power of γ. Since $|\gamma| = p$, there are, therefore, p distinct homomorphisms $\psi_i : P \to \mathrm{Aut}(Q)$ given by $\psi(y) = \gamma^i, 0 \leq i \leq p-1$. There are two general cases:

(a) If $i = 0$, then ψ_i is the trivial homomorphism
(b) having $\psi_i(g) = 1$ for all $g \in G$. In this case, $Q \rtimes_{\psi_0} P \simeq Q \times P \simeq C_q \times C_p$.
(c) If $i \neq 0$, then ψ_i is nontrivial and $Q \rtimes_{\psi_i} P$ is a nonabelian group of order p^q. We may also note that all these groups are isomorphic because for each $\psi_i, i \neq 0$, there is some generator element $y_i \in P$ such that $\psi_i(y_i) = \gamma$. (*1*, p. 181)

We may now classify all groups of order $n \leq 15$, except those of order 12.

For $n = 10$, note that $10 = 2 \cdot 5$, which is a product of primes. Also, $2 \mid (5-1)$. Let G be a group of order 10. There are two possibilities:

(a) If G contains an element of order 10, then G is cyclic and isomorphic to C_{10} (see 3.3).
(b) If G does not contain an element of order 10, then G must have an element of order 2 and an element of order 5 (see case b). If $p \in G, |p| = 2$ and $q \in G, |q| = 5$, let $P = \langle p \rangle \simeq C_2$ and $Q = \langle q \rangle \simeq C_5$. Then

$$\mathrm{Aut}(Q) \simeq (Z/5Z)^{\times}$$

Consider the homomorphism $\psi\colon C_2 \to (\mathbb{Z}/5\mathbb{Z})^\times$. Since $(\mathbb{Z}/5\mathbb{Z})^\times$ has the single element 4:

$$\psi_4 : P \simeq C_2 \to (\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathrm{Aut}(Q)$$
$$1 \sim 0 \mapsto 0 \sim 1$$
$$p \sim 1 \mapsto 4 \sim q^4$$

Therefore, the map is the instance ψ_2 of the general case psi_i, and the homomorphism is nontrivial. This means $G \simeq C_5 \rtimes_{\psi_2} C_2$, making G nonabelian (see case c). This group is more commonly seen as the dihedral group D_{10}, generated by r as an element of order 5 with and s as an element of order 2.

For $n = 11$ and $n = 13$, notice that n is prime, therefore the only group of order 11 up to isomorphism is C_{11} and C_13 respectively.

For $n = 14$, note that $14 = 2 \cdot 7$, a product of primes having $2 \mid (7 - 1)$. Suppose G is a group of order 14, then;

(a) If G contains an element of order 14, then G is isomorphic to C_{14}.

(b) Otherwise, G must contain an element of order 7 and an element of order 2. If $p \in G, |p| = 2$ and $q \in G, |q| = 7$, then let's define $P = \langle p \rangle \simeq C_2$ and $Q = \langle q \rangle \simeq C_7$. Then $\mathrm{Aut}(Q) \simeq (\mathbb{Z}/6\mathbb{Z})^\times$. Since $\mathbb{Z}/6\mathbb{Z}$ contains only a single element of order 2, that is 6 with $6^2 = 36 \equiv 1 \pmod 7$, the homomorphism between the two groups is defined as:

$$\psi_6 : C_2 \to (\mathbb{Z}/7\mathbb{Z})^\times$$
$$0 \mapsto 1$$
$$1 \mapsto 6$$

More generally, $\psi_6(y) = \gamma^6$ and the homomorphism is nontrivial. This means $G \simeq C_7 \rtimes_{\psi_3} C_2$, making G nonabelian (see case c). This group is more commonly seen as the dihedral group D_{14} with r as an element of order 7 with and s as an element of order 2.

For $n = 15$, we once again have a product of primes, $15 = 3 \cdot 5$. However, $3 \nmid (5 - 1)$, so every group of order 15 is abelian and isomorphic to C_{15}.

Order	No. Of Isomorphism Types	Abelian Groups	Non-abelian Groups
1	1	C_1	none
2	1	C_2	none
3	1	C_3	none
4	2	C_4	none
		$C_2 \times C_2 \simeq V_4$	
5	1	C_5	none
6	2	C_6	S_3
7	1	C_7	none
8	5	C_8	D_8
		$C_4 \times C_2$	Q_8
		$C_2 \times C_2 \times C_2$	
9	2	C_9	none
		$C_3 \times C_3$	
10	2	C_{10}	D_{10}
11	1	C_{11}	none
12	5	C_{12}	A_4
		$C_6 \times C_2$	D_{12}
			$C_3 \rtimes C_4$
13	1	C_{13}	none
14	2	C_{14}	D_{14}
15	1	C_{15}	none

Table 5. All groups of order $n \leq 15$ up to isomorphism

11. Applications

By application, let's identify the following groups:

(a) $G_1 = C_2 \times D_6$.

$\#C_2 = 2$ and $\#D_6 = 6$, so $\#G_1$. Additionally, C_2 has an element of order 2 and D_6 has elements of orders 2 and 3. Therefore, G_1 must have elements of orders $\mathbf{lcm}\ (2,\ 3) = 6$ and $\mathbf{lcm}\ (2, 2,\ =)2$. Let $x \in G_1, \langle x \rangle = \{0, x\}, y \in G_1, y = \{1, y, y^2, y^3, y^4.y^5\}$. Then,

$$G_1 = \langle x, y \rangle = \{1, y, y^2, y^3, y^4, y^5, x, xy, xy2, xy^3, xy^4, xy^5\}$$

G_1 is isomorphic to the Dihedral group D_{12}.

(b)

$$G_2 := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}/2\mathbb{Z} \right\} \leq \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$$

There are 2 possible values for each of a, b, c, so G_2 has order 8. Through matrix multiplication, we see that:

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 \tag{11.1}$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 = I \tag{11.2}$$

Therefore, G_2 has two elements of order 4 and 5 elements of order 2. Since isomorphisms preserve order. G_2 is isomorphic to D_8.

(c) $G_3 = S/Z(S)$ where

$$S = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}/3\mathbb{Z} \text{ and } ad - bc = 1 \right\} \leq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}).$$

There are 3 possible values for each of a, b, c, d without restriction. Since the first column must be nonzero, we have $3^2 - 1 = 8$ possible choices for the pair (a, c). However, after we have selected a and c, we can only choose b and d such that $ad \times bs = 1$. This limits the number of possible combinations to just 3. Therefore, $SL_2(\mathbb{Z}/3\mathbb{Z})$ has order 24.

Now consider the center of the group, $Z(S)$. Since $Z(S)$ must commute with all elements of S, then $Z(S)$ is limited to only the scalar matrices in S. These are:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

Therefore, the quotient group $S/Z(S)$ has order $24/2 = 12$, and is a subgroup of a group of order 24. It is therefore the alternating group A_4.

References

1. D. S. Dummit, R. M. Foote, *Abstract Algebra* (John Wiley & Sons, ed. 3, 2003).