Math 71: Algebra

Groups of Small Order

Amittai Siavava

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

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***Abstract Algebra*** by **David S. Dummit & Richard M. Foote**.

(b) ***Algebra*** by **Jacob K. Goldhaber & Gertrude Ehrlich**

1. Introduction

Motivate the classification of groups of small order up to isomorphism; quickly review the case of groups of prime order, providing context to why the factorization of the order $n = \#G$ is reflected in the list of possible groups of order n up to isomorphism.

In attempting to understand the structure of groups, it is often important to understand smaller structures within the group — and these may include kernels, orbits, and most-importantly subgroups. Since proper subgroups generally have smaller order, they can be more easily understood. But how do we find – for certain – *all* the *important* subgroups in a group? First, we must motivate the unique classification of groups. Some groups have similar structure — take, for instance, the two groups

$$S_2 = \{\epsilon, (1\ 2)\} \tag{1.1}$$

$$Z_2 = (\mathbb{Z}/2\mathbb{Z})^+ = \{0, 1\} \tag{1.2}$$

Through some experimentation, we notice that each group has order 2, is commutative, cyclic, and the non-identity element is in-fact its own inverse – i.e. it has order 2. Therefore, we can transfer any function from one to the other by mapping $\epsilon \leftrightarrow 0$ and $(1\ 2) \leftrightarrow 1$. We call such a map a *group isomorphism*, and we say S_2 and $(Z_2, +)$ are *isomorphic*. We often need to uniquely identify all groups of a given structure For instance, we may consider examples 1.1 and 1.2 above to be under the class C_2 , the cyclic groups of order 2. We can trivially show that there is a single cyclic group of order 2.

In example 1.2 above, we can note that the group has only two possible subgroups: the trivial group $\{\epsilon\}$ and the group itself. But is this always the case? Given a group G, when can we expect to find subgroups of other orders than 1 and $\#G$? Is there any fundamental difference between such groups that only have subgroups of order 1 and $\#G$, and those that have subgroups of different orders? Let us recall Lagrange's theorem:

Theorem 1.3 (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)

The first part of lagrange's theorem (1.3), while offering no guarantees on the existence of subgroups of given orders, tells us that the order of any subgroup $S \leq G$ divides the order of G. We can immediately pick out that all groups of prime order p must only have the trivial group as a proper subgroup, since their order p is only divisible by 1 and p. Furthermore, consider that the order of every element in the group must divide p. Since the order of non-identity elements is clearly greater than 1, we can conclude that the order of every non-identity element in the group is p, hence the group is cyclic.

Order	Group	Isomorphisms
1	C_1	$\{\epsilon\}$, S_1
2	C_2	$\mathbb{Z}/2\mathbb{Z}$, S_2
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. (Abelian) Groups of Prime Order $n \leq 15$

Theorem 1.4. Every cyclic group is abelian.

Proof. Recall that cyclic groups can be denoted as the powers of a single element, g, known as the *generator* of the group. Consider two elements, $x = g^a$ and $y = g^b$. Then, $xy = g^a g^b = g^{a+b} = g^b g^a = yx$. □

Therefore, every group of prime order p is cyclic and abelian. We call C_p the class of cyclic groups of order p, and every other group of order p is isomorphic to the C_p.

For groups of non-prime order $\#G = n$, Lagrange (Theorem 1.3) tells us that any subgroup $S \leq G$ must have an order $\#S$ equal to one of the divisors of n, and it follows that the left cosets of S in G is equal to $\frac{n}{\#S}$.

When groups are first introduced, they are described as sets equipped with a binary operation satisfying certain axioms (associativity, identity, inverses). As examples, we considered the symmetric groups S_n, the group of permutations of the set $\{1, \ldots, n\}$. However, these are not so far apart. Even for Galois (see Dummit–Foote (*1*, p. 14 (3))), groups were made of "substitutions"—i.e., Galois was working with permutation groups!

For now, we restrict attention to *finite* groups (but see section 7 below for infinite groups). So the symmetric groups S_n (for $n \geq 1$) are finite groups. Is every finite a group a permutation group? No: we have $\#S_n = n!$, so a group of order 4 cannot be isomorphic to S_n since $2! < 4 < 3!$. But if we all ourselves *subgroups* of permutation groups, the answer is yes. Our main result is as follows.

2. SETUP

(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.

Theorem 2.1 (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)

Theorem 2.2 (The Fundamental Theorem of Finitely Generated Abelian Groups). If a group G is a finitely generated abelian group, then:

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s} \tag{2.3}$$

where

(a) $r \geq 0$ and $n_j \geq 1$ for all j; and

(b) $n_{i+1} \mid n_i$ for all i.

And expression 2.3 is unique.

Theorem 2.4. If G is a finite group of order p^2 with p prime, then G is abelian.

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 1.3, we know that $\#Z(G) \mid \#G$. This implies that $\#Z(G) \in \{1, p, p^2\}$. Considering the following 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.

(c) Assuming G does not have an element of order p^2, then every non-identity element must have order p since it must divide p^2 (see 1.3) and it is greater than 1. Let x be one such element, generating the subgroup $\langle x \rangle$ of order p. Let $y \in G \setminus \langle x \rangle$, then $o(y) = p$ and $\langle y \rangle$ is also a group of order p. Furthermore, $\langle x \rangle$ intersects trivially with $\langle y \rangle$, and both $\langle x \rangle$ and $\langle y \rangle$ are cyclic (and therefore abelian). Now, consider the group $\langle x, y \rangle \simeq \langle x \rangle \times \langle y \rangle$. Since $x \in G$ and $y \in G$, $\langle x, y \rangle \subseteq G$. Furthermore, since x has order p and y has order p, $\langle x, y \rangle$ has order p^2, meaning $\langle x, y \rangle = G$ since *every element in* $\langle x, y \rangle$ *is in* G, and $\langle x, y \rangle$ *has the same number of elements as* G. Therefore, $\{x, y\}$ are generators of G and G is isomorphic to $\langle x \rangle \times \langle y \rangle$. since $\langle x \rangle$ and $\langle y \rangle$ are both abelian, their direct product, G, is therefore also abelian.

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	$C_2 \times C_2$	V_4
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	$C_4 \times C_2$	
	$2 \times 2 \times 2$	$C_2 \times C_2 \times C_2$	
9	9×1	C_9	$\mathbb{Z}/9\mathbb{Z}$
	3×3	$C_3 \times C_3$	
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	$C_6 \times C_2$	
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 2. Abelian Groups of order $n \leq 15$

□

Using the fundamental theorem, we now extend the earlier classification of groups of prime order (table 1) to classify all abelian groups of order ≤ 15. Look at this:

So far, we have classified the trivial group (order 1), all the groups of prime order $p \leq 15$, and all the groups of order $p^2 \leq 15$ where p is prime. This includes *every* group of order $n \in \{1, 2, 3, 4 = 2^2, 5, 7, 9 = 3^2, 11, 13\}$. We have also classified all abelian groups of order $n \leq 15$, including those or orders not listed above such as C_6 and C_8.

Now, let us exhaustively classify the all groups of order 6. Cauchy's theorem tells us that any group of order 6 must have an element a of order 2 and an element b of order 3, since $2, 3$ are both primes dividing 6. Let a be an element of order 2 and b be an element of order 3. Then, $a^2 = e$ and $b^3 = e$. Consider the groups generated by these two elements:

$$\langle a \rangle = \{\epsilon, a\} \tag{2.5}$$

$$\langle b \rangle = \{\epsilon, b, b^2\} \tag{2.6}$$

$$\langle a, b \rangle = \{\epsilon, b, b^2, a, ab, ab^2\} \tag{2.7}$$

Notice that in equation 2.7 above, we get a group of order 6. In this case, $ab \neq ba$, but;

(a) $a^2 = e$, therefore, $a^{-1} = a$.

(b) $b^3 = e$, therefore, $b^{-1} = b^2$ and $(b^2)^{-1} = b$.

(c) Since $xy = y^{-1}x^{-1}$, we have $ab = b^2a$ and $ab^2 = ba$.

If the group seems familiar, it should, because $\langle a, b \rangle$ is equivalent to D_3 (with $a = s, b = r$), which is itself isomorphic to S_3.

3. Further Analysis

(a) Show that every nonabelian group G of order 8 is isomorphic to either D_8 or Q_8, as follows.
- Show that G has an element $a \in G$ of order 4. *[Hint: what happens if every nonidentity element has order 2?]*
- Let $H := \langle a \rangle$ and let $b \notin H$. Observe that $H \trianglelefteq G$ is normal; argue that $bab^{-1} = a^3$ (the order under conjugation is preserved), and then that $G \simeq D_4, Q_8$ according as b has order 2 or 4.

(b) Pause to show we have classified groups of order $n \leq 9$.

Now, let us consider the nonabelian groups of order $n = 8$. Note that $8 = 2^3$. Let G be a nonabelian group of order 8. By Lagrange's theorem (1.3), non-identity elements of G may have orders $2, 4, 8$. If G has an element a of order 8, then G is cyclic, therefore abelian. On the other hand, if every nonidentity element $b_i \in G$ has order 2, then:

(a) For any $b_i \in G$, $\langle b_i \rangle \leq G$ is of prime order $p = 2$ and is therefore abelian.

(b) Taking $b_j \in G, b_j \notin \langle b_i \rangle$, then $\langle bj \rangle \leq G$ is also an abelian group of order 2. Then $\langle b_i, b_j \rangle \leq G$ is an abelian group of order 4 (direct product of abelian groups).

(c) Taking $b_k \in G, b_k \notin \langle b_i, b_j \rangle$, then $\langle b_k \rangle \leq G$ is also an abelian group of order 2. Then $\langle b_i, b_j, b_k \rangle \leq G$ is an abelian group of order 8 (direct product of abelian groups).

(d) Since $\#G = 8$ and $\#\langle b_i, b_j, b_k \rangle = 8$ yet $\langle b_i, b_j, b_k \rangle \leq G$, it must be the case that $\langle b_i, b_j, b_k \rangle = G$.

(e) Therefore, if every non-identity element in G has order 2, then G is abelian. Particularly, $G \cong C_2 \times C_2 \times C_2$.

Therefore, if G is a *nonabelian* group of order 8, then G must have an element of order 4. Let $a \in G$ be such an element, with $H := \langle a \rangle$. Then $\#H = 4$, and H is cyclic meaning $a^{-1} = a^3$. Let $b \in G, b \notin H$. Then b may have order 2 or order 4.

(a) If b has order 2, then $b^2 = 1$, and $bab^{-1} = b(ab^{-1}) = b^2a^3 = a^3 \in H$. Therefore $H \trianglelefteq G$ is normal in G and G is isometric to D_8.

(b) If b has order 4, then G is isomorphic to Q_8. Particularly, $G = \langle x, y, z \rangle$ where $x^2 = y^2 = z^2 = -1$, each of x, y, z has order 4, and $xy = z, yz = x, zx = y$ and $yx = -z, zy = -x, xz = -y$. It follows that $aba^{-1} = ab(-a) = c(-a) = -ca = -b$ for any permutations of $a, b, c \in \{x, y, z\}$. Therefore, any subgroup $H = \langle a \rangle = \{1, a, -1, -a\}$ having $a \in \{x, y, z\}$ is normal in G.

We have now classified all nonabelian groups of order 8, and all groups of order $n \leq 9$ (since $9 = 3^2$ is a square of a prime, it may only have the abelian group $C_3 \times C_3$ and C_9).

(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).

Moving on to groups of order 10; we may notice that $10 = 5 \cdot 2 = pq$ with $p = 2, q = 5$ prime.

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

Now, consider that C_p is a cyclic group of order p. Taking x as the minimal generator, then $C_p = \{0, x, x^2, x^3, \ldots, x^{p-2}, x^{p-1}\}$. Additionally,

$$x^{ip} = (x^p)^i = 0^i = 0 \ \forall i \in \mathbb{Z} \tag{4.1}$$

Now, consider any arbitrary element $x^\alpha \in C_p$ such that $\mathbf{gcd}\ (\alpha,\ p) = g > 1$. Then, we say α is not coprime to p. Define the *least common multiple* of p and α to be

$$\mathbf{lcm}\ (p,\ \alpha) = \frac{\alpha p}{g}$$

Since $g \mid \alpha$, then $\mathbf{lcm}\ (p,\ \alpha) = np$ for some $n \in \mathbb{Z}$. Therefore, $x^{\mathbf{lcm}\ (p,\ \alpha)} = x^{np} = 0$ (by equation 4.1). This means that, whenever $(a, p) \neq 1$, then $x^{\mathbf{lcm}\ (p,\ a)} = 0$, therefore ψ_a is not an automorphism (since it's kernel is not trivial, it's image does not equal C_p).

Consequently, $\psi_a \in \mathrm{Aut}(C_p) \Leftrightarrow (a,p) = 1$. We may also recognize that such elements $\psi_a \in \mathrm{Aut}(C_p)$ correspond to the units $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, and $|\mathrm{Aut}(C_p)| = |(\mathbb{Z}/p\mathbb{Z})^\times| = \phi(p)$. Therefore, $\mathrm{Aut}(C_p) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. When p is prime, then $\phi(p) = p-1$, in which case

$$\mathrm{Aut}(C_p) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq C_{p-1} \tag{4.2}$$

and $\mathrm{Aut}(C_p)$ is cyclic.

Consider the case that $\#G = pq$ having $p \nmid (q-1)$. Then, G is abelian (by DF Example 4.4.1, p. 135–136). Consider the center $Z(G) \leq G$. If $Z(G) \neq 1$, then Lagrange's theorem (1.3) forces $G/Z(G)$ to be cyclic. Furthermore, Lagrange's theorem tells us that the order of any element in G must divide the order of G, therefore the order may be $n \in \{1, p, q, pq\}$. Suppose $Z(G) = 1$. Then;

(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, if G contains an element x of order q.

(c) 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).

(d) 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).

(e) 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 (1.3), a contradiction of the assumption that $p \nmid (q-1)$. Therefore, G must be abelian .

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

Theorem 4.3 (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 4.3) 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. Let $P = \langle p \rangle$ and $Q = \langle q \rangle$. Note that $\mathrm{Aut}(Q) \simeq C_{q-1}$ is cyclic and $p \mid (q-1)$, 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 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 and $Q \rtimes_{\psi_0} P \simeq Q \times P$. This is an abelian group isomorphic to to $C_q \times C_p$.

(b) 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) .

(a) Classify groups of order $n \leq 15$ except $n = 12$.

5. Full Classification

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 note that $2 \mid (5-1)$. Let G be a group of order 10. There are two possibilities:

(a) If G contains an element of order 10, then G is isomorphic to C_{10}. Therefore, G is cyclic and abelian.

(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. If $p \in G, |p| = 2$ and $q \in G, |q| = 5$, then let's define $P = \langle p \rangle$ and $Q = \langle q \rangle$. Consider the set $\mathrm{Aut}(Q)$ of automorphisms of Q, with $Q \cong C_5$. As demonstrated by equation 4.2,

$$\mathrm{Aut}(Q) \simeq (Z/5Z)^{\times} \simeq C_4 \tag{5.1}$$

In this case, $\mathrm{Aut}(Q)$ contains the unique cyclic subgroup $2\mathbb{Z}/4\mathbb{Z} \simeq C_2$ of order 2. The homomorphism between the two groups is defined as:

$$\psi_i : C_2 \to 2\mathbb{Z}/4\mathbb{Z}$$

$$0 \mapsto 0$$

$$1 \mapsto 2$$

More generally, $\psi_i(y) = 2\gamma \sim \gamma^2$. Therefore, $i = 2$, and the homomorphism is nontrivial. This means $G \simeq C_5 \rtimes_{\psi_2} C_2$, making G nonabelian by b. This group is more commonly seen as the dihedral group D_{10}, generated by r as an element of order 5 with $Q = \langle r \rangle = \{1, r, r^2, r^3, r^4\}$, and s as an element of order 2 with $P = \langle s \rangle = \{1, s\}$. The homomorphism

For $n = 11$, remember that 11 is prime. Therefore, the only group of order 11 is C_{11}, which is abelian. Similarly, for $n = 13$, C_{13} is the only group of order 13.

For $n = 14$, note that $14 = 2 \cdot 7$, which is a product of primes, and $2 \mid (7 - 1)$. Let G be a group of order 14. Like above, there are two possibilities:

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

(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 $P = \langle p \rangle$ and $Q = \langle q \rangle$. Consider the set $\mathrm{Aut}(Q)$ of automorphisms of Q, with $Q \cong C_7$. As demonstrated by equation 4.2,

$$\mathrm{Aut}(Q) \simeq (Z/7Z)^{\times} \simeq C_6 \tag{5.2}$$

In this case, $\mathrm{Aut}(Q)$ contains the unique cyclic subgroup $3\mathbb{Z}/6\mathbb{Z} \simeq C_3$ of order 3. The homomorphism between the two groups is defined as:

$$\psi_i : C_2 \to 2\mathbb{Z}/6\mathbb{Z}$$

$$0 \mapsto 0$$

$$1 \mapsto 3$$

More generally, $\psi_i(y) = 3\gamma \sim \gamma^3$. Therefore, $i = 3$, and the homomorphism is nontrivial. This means $G \simeq C_7 \rtimes_{\psi_3} C_2$, making G nonabelian by b. This group is more commonly seen as the dihedral group D_{14} with r as an element of order 7 with $Q = \langle r \rangle = \{1, r, r^2, r^3, r^4, r^5, r^6\}$, and s as an element of order 2 with $P = \langle s \rangle = \{1, s\}$.

For $n = 15$, we once again have a product of primes, $15 = 3 \cdot 5$. However, $3 \nmid (5 - 1)$, so we have the case that any group of order 15 is abelian (as shown in e), therefore isometric to C_{15}.

(a) For +2 bonus, classify the groups of order 12. Let P_2 be a 2-Sylow subgroup (of order 4) and P_3 a 3-Sylow subgroup.

- Show that either $P_2 \trianglelefteq G$ is normal or $P_3 \trianglelefteq G$ is normal. *[Hint: if P_3 is not normal, count the number of elements of order* 3*.]* Conclude that in either case, $G = P_2P_3$.
- Show that if both P_2 and P_3 are normal, then $G \simeq P_2 \times P_3$ is abelian. *[Hint: either state and use the recognition theorem for direct products, DF, section 5.4, Theorem 9, p. 171–172; or understand the proof and apply the argument here directly.]*
- Proceeding by cases, first suppose that $P_2 \trianglelefteq G$ and $P_2 \; simeq Z_4$. Arguing as in (8), show that the homomorphism $P_3 \to \mathrm{Aut}(P_2)$ is trivial, so G is abelian and therefore cyclic. *[Hint:* $\#\,\mathrm{Aut}(Z_4) = \#(\mathbb{Z}/4\mathbb{Z})^\times = 2$*.]*
- Suppose $P_2 \trianglelefteq G$ and $P_2 \simeq Z_2 \times Z_2$ but $P_3 \; not \trianglelefteq G$. Show that there is an injective group homomorphism $G \; hookrightarrow S_4$, and conclude that $G \simeq A_4$.
- Suppose $P_3 \trianglelefteq G$ and $P_2 \simeq Z_4$ but $P_2 \; /trianglelefteq G$. Write $P_2 = \langle x \rangle$ and $P_3 = \langle y \rangle$ and show that $xyx^{-1} = y^{-1}$, then show that this uniquely determines the Cayley table of G, with presentation
$$G \simeq \langle x, y \,|\, x^4 = y^3 = 1, xyx^{-1} = y^{-1} \rangle.$$
- Finally, suppose $P_3 \trianglelefteq G$ and $P_2 \simeq Z_2 \times Z_2$ but $P_2 \not\trianglelefteq G$. Writing $P_3 = \langle y \rangle$, show that $P_2 = \; langle x_1 \rangle \times \langle x_2 \rangle$ for some $x_1, x_2 \in P_2$ with $x_1 y x_1^{-1} = y$ and $x_2 y x_2^{-1} = y^{-1}$. Conclude that $x_1 y$ has order 6 and then that $G \simeq D_{12}$, the dihedral group of order 12.

(a) Give a table of groups of order $n \leq 15$ up to isomorphism (DF, section 5.3, p. 168), giving the answer even if you don't do (10).

(b) As an application, identify in the table the three groups $G_1 = Z_2 \times D_6$,

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

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

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

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

7. Conclusion

References

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