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 6 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, 2.1). Let x be one such element, generating the subgroup $\langle x \rangle$ of order p. Let $y \in G - \langle x \rangle$, then $\langle y \rangle$ is also a group of order p. Then the group $\langle x, y \rangle \leq G$ has order $p^2 = \#G$, implying that $\langle x, y \rangle = G$ (trivially, $\langle x \rangle \leq G \wedge \langle y \rangle \leq G \implies \langle x, y \rangle \leq G$, and a subgroup of G with the same order as G must be G itself.) which generates a subgroup $\langle x \rangle$ of order p. In this case, $G = \langle x, y \rangle \cong Z_p \times Z_p$, and G is therefore 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 (**??**) to classify all abelian groups of order ≤ 15.

If we revisit the classification of 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. Consider the groups generated by these two elements:

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

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

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

In 2.7 above, we notice that $\langle a, b \rangle$ is isomorphic to D_6. We can demonstrate that $\langle a, b \rangle$ is also isomorphic to S_3 under the isomorphism:

$$\psi \colon \langle a, b \rangle \to S_3$$

$$\epsilon \mapsto \epsilon$$

$$a \mapsto (1\ 2)$$

$$b \mapsto (1\ 2\ 3)$$

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 $n \leq 9$.

4. Main Theorem

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

- 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. *[Hint: it has index p, so go through DF, section 4.2, Corollary 5, pp. 120–121.]* Write $P = \langle x \rangle$ and $Q = \langle y \rangle$ with $x, y \in G$.
- Show that $xyx^{-1} = y^k$ with $k \in \{1,$ $cdots, q-1\}$, and use this to define a group homomorphism

$$\phi \colon P \to (\mathbb{Z}/q\mathbb{Z})^\times$$

where $x \mapsto k$. *[Hint: use* $x^i y x^{-i} = y^{\phi(i)}$*.]* Conclude that either ϕ is the trivial homomorphism (mapping every element to 1) or phi is injective.

- If ϕ is trivial, prove that G is cyclic (DF, section 4.4, Exercise 2, p. 137).
- Show that ϕ is injective if and only if G is nonabelian and $p \mid (q-1)$. (In particular, observe that if $p \nmid (q-1)$ then G is abelian.)
- If $p \mid (q-1)$, exhibit a nonabelian group of order pq (following DF, Example, section 4.5, p. 143; see also DF, section 4.3, Exercise 34, p. 132). Show that when $p = 2$ we obtain the dihedral group D_{2q} of order $2q$ for $q \geq 3$ as a subgroup of S_q via the action on the vertices of a q-gon.
- Suppose that G is nonabelian and $p \mid (q-1)$. Show that P $/triangleleftteqG$ (DF, Example, section 4.5, p. 143), so there exists an injective homomorphism $G \hookrightarrow S_q$ whose image up to conjugation lies in the the normalizer of the cyclic subgroup generated by the q-cycle $(1\ 2$ $cdots\ q)$ (DF, section 4.3, Exercise 28, p. 132). When $p = 2$, show that this group is unique up to conjugation. *[Hint: show that there is a unique subgroup of* $(\mathbb{Z}/q\ Z)^\times$ *of order* 2*.]*

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 $Z_p \to \mathrm{Aut}(Z_q) \simeq (\mathbb{Z}/q\mathbb{Z})^\times = langleg\rangle$ mapping $x \mapsto g^{(q-1)/p}$ (DF, Example, section 5.5, pp. 181–182; section 5.5, Exercise 6, pp. 184–185).

5. Implications

(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

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

6. Conclusion

References

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