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 and every element is a generator of the group. Therefore, every group of prime order p is isomorphic to the cyclic group of order p, C_p . For the first 8 primes, these are:

Order	Group	Isomorphisms
1	C_1	Z_1, 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}	$\mathbb{Z}/13\mathbb{Z}$

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.

Contents. In section 2, we get set up by describing how the group operation naturally describes permutations of the elements of the group. We then prove Cayley's theorem in section 7. We then conclude in section 6 with some applications and next steps.

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.

We start with a motivating example. Recall the Cayley table for D_6, the dihedral group of order 6:

	1	r	r^2	s	sr	sr^2
1	1	r	r^2	s	sr	sr^2
r	r	r^2	1	sr^2	s	sr
r^2	r^2	1	r	sr	sr^2	s
s	s	sr	sr^2	1	r	r^2
sr	sr	sr^2	s	r^2	1	r
sr^2	sr^2	s	sr	r	r^2	1

We observed that Cayley table have the Sudoku property, as in the following lemma.

Lemma 2.1. Each row (and column) of the Cayley table of a finite group G contains all elements of G.

As a reminder, this lemma follows directly from the cancellation law.

Returning to the above example, if we pick off just one row—say the row sr—by this property we get a permutation of the set D_6:

$$\begin{pmatrix} 1 & r & r^2 & s & sr & sr^2 \\ sr & sr^2 & s & r^2 & 1 & r \end{pmatrix} \tag{2.2}$$

We denote this element $\sigma_{sr} \colon D_6 \to D_6$, since it is a symmetry that depends on sr: it is defined by $\sigma_{sr}(sr) = 1, \ldots,$ $\sigma_{sr}(sr^2) = r$, reading the input from the top row of the table and the output from the bottom row. This is visibly a bijection from D_6 to itself: each element of D_6 appears exactly once.

Recall that we write the set of bijections from a set A to itself as

$$\mathrm{Sym}(A) := \{\sigma \colon A \to A \text{ bijection}\}$$

and this forms a group under composition. This works for every set A, even though we mostly worked with $A = \{1, \ldots, n\}$ and then abbreviate $S_n = \mathrm{Sym}(\{1, \ldots, n\})$. There is no loss of generality here.

Lemma 2.3. If A is a finite set with $\#A = n$, then the groups $\mathrm{Sym}(A) \simeq S_n$ are isomorphic.

Proof. Since $\#A = n$, there is a bijection from A to $\{1, \ldots, n\}$. Each permutation of the elements of A gives a permutation of the elements $\{1, \ldots, n\}$ by how they are numbered. □

Putting these together, we can define a function

$$\begin{aligned}\sigma\colon D_6 &\to \mathrm{Sym}(D_6) \simeq S_6\\ 1 &\mapsto \sigma_1 = \begin{pmatrix} 1 & r & r^2 & s & sr & sr^2 \\ 1 & r & r^2 & s & sr & sr^2 \end{pmatrix}\\ &\vdots\\ sr^2 &\mapsto \sigma_{sr^2} = \begin{pmatrix} 1 & r & r^2 & s & sr & sr^2 \\ sr^2 & s & sr & r & r^2 & 1 \end{pmatrix}\end{aligned} \tag{2.4}$$

Usually we write functions like $f(x)$ with input x from the domain; but here the output is itself a function which wants input, so in order not to get confused, we use a subscript.

That is a start, but of course in group theory we want more than just a map of sets: we want to know it is a homomorphism! One case of the homomorphism property in this example would read

$$\sigma_{sr}\sigma_r \stackrel{?}{=} \sigma_{sr^2} \tag{2.5}$$

This is an equality we need to check on the right-hand side of (2.4). Composing the permutations, we see it checks out! Once we have a homomorphism, we can also see that the kernel of the map σ consists only of the identity: if an element maps to the identity permutation in $\mathrm{Sym}(D_6)$, it would come from a row of the Cayley table where they elements line up according to the identity, and that happens only for the top row. So we get an injective map $D_6 \hookrightarrow S_6$. By the fundamental homomorphism theorem, we see that D_6 is isomorphic to its image under this map; the following lemma reminds us of how this works in general.

Theorem 2.6 (Fundamental homomorphism theorem). Let $\phi\colon G \to H$ be a group homomorphism. Then $G/\ker\phi \simeq \phi(G) \leq H$.

Corollary 2.7. If $\phi\colon G \to H$ is an injective group homomorphism, then $G \simeq \phi(G)$.

Proof. If ϕ is injective, then $\ker\phi = \{1\}$, and then $G/\ker\phi \simeq G$ (the cosets of the identity are just the elements of G!). □

We conclude that D_6 is isomorphic to a subgroup of S_6. This is Cayley's theorem!

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

Cayley's theorem shows that we can see every finite group as a subgroup of some permutation group. There can be more than one way to realize a finite group G as a subgroup of permutations: already for D_6 we showed that $D_6 \simeq S_3$ by considering the action of the dihedral group on the vertices of the triangle.

Returning to our proof, we see that the arguments also work when G is an infinite group: we still get an injective group homomorphism $G \hookrightarrow \mathrm{Sym}(G)$; however, now $\mathrm{Sym}(G)$ consists of permutations of an infinite set, so it is not of the form S_n!

The homomorphism constructed in Proposition 7.3 arises naturally in the context of groups acting on themselves (by left multiplication): this is described in detail by Dummit–Foote (*1*, §4.2), with Cayley's theorem as a corollary (*1*, §4.2, Corollary 4, p. 120). Indeed, *group actions* allow us to see all homomorphisms from a finite group into permutation groups, whether that be on vertices of an n-gon, or on the cosets of a group.

7. Main result

We are now ready to prove Cayley's theorem, which we will prove in a slightly stronger form.

Theorem 7.1 (Cayley). Let G be a finite group of order $\#G = n$. Then G is isomorphic to a subgroup of S_n.

We follow what we observed in the case $G = D_6$ in the previous section one step at a time.

Throughout, let G be a finite group. First, we define the permutations that come from the rows of the Cayley table. Recall that in the row labelled a (for $a \in G$), with $b \in G$ the column we have entry ab (as usual suppressing $*$ and writing the group multiplicatively).

Lemma 7.2. Let $a \in G$. Define the map

$$\begin{aligned} \sigma_a \colon G &\to G \\ x &\mapsto ax \end{aligned}$$

Then σ_a is a bijection, i.e., $\sigma_a \in \mathrm{Sym}(G)$.

Proof. We proved this in class, showing it is both injective and surjective and then that it has inverse $\sigma_{a^{-1}} : G \to G$ defined by $b \mapsto a^{-1}b$. □

We then built on this considering all of these bijections at once.

Proposition 7.3. Define the map

$$\begin{aligned} \sigma \colon G &\to \mathrm{Sym}(G) \\ a &\mapsto \sigma_a \end{aligned}$$

Then σ is an injective group homomorphism.

Proof. We first show that the map is a homomorphism. Let $a, b \in G$. We want to check

$$\sigma_a \sigma_b \stackrel{?}{=} \sigma_{ab}.$$

These are two permutations of the set G. To show that two functions are equal, we show that they give the same outputs. So let $x \in G$. Then on the left-hand side, by definition

$$(\sigma_a \sigma_b)(x) = \sigma_a(\sigma_b(x)) = \sigma_a(bx) = a(bx) = abx.$$

This matches the right-hand side:

$$\sigma_{ab}(x) = (ab)x = abx.$$

Thus $(\sigma_a \sigma_b)(x) = \sigma_{ab}(x)$ for all $x \in G$, so then $\sigma_a \sigma_b = \sigma_{ab} \in \mathrm{Sym}(G)$ as functions.

To show that σ is injective, we show that $\ker \sigma \subseteq \{1\}$. Let $a \in G$ be such that a maps to the identity: $\sigma_a = \mathrm{id}_G$. Then for all $x \in G$ we have $\sigma_a(x) = \mathrm{id}_G(x)$, which means $ax = x$ for all $x \in G$. If we plug in $x = 1$ we get $a = 1$, as desired. □

We may now conclude.

Proof of Theorem 7.1. By Proposition 7.3, we have an injective group homomorphism $G \hookrightarrow \mathrm{Sym}(G)$. By Lemma 2.3, we have an isomorphism $\mathrm{Sym}(G) \simeq S_n$, so composing these we get an injective group homomorphism $G \hookrightarrow S_n$. Finally, by the fundamental homomorphism theorem (Corollary 2.7), we conclude that G is isomorphic to its image, a subgroup of S_n. □

References

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