1 Finite Groups

1.1. Show that for 2-cycles $(1a)(1b)(1a) = (ab)$.

We can show this by brute force by seeing where $(1a)(1b)(1a)$ takes a and b. Using arrows to represent the alterations made by successive cycles (where we multiply right to left), we see

$$a \to 1 \to b \to b \quad \text{and} \quad b \to b \to 1 \to a.$$

That is, $(1a)(1b)(1a)$ exchanges a and b, and so is equivalent to (ab).

1.2. Show that A_n for $n \geq 3$ is generated by 3-cycles, that is, any element can be written as the product of 3-cycles.

We know that all permutations may be broken into a product of 2-cycles. In the case of A_n, these products always consist of an even number of such cycles (being as they form the group of even permutations).

If there are two 2-cycles that share both numbers, i.e. there exists a term like $(ab)(ba)$, they can be removed from the product (being as they form the identity permutation). For 2-cycles sharing one element, such as $(ab)(cb)$, we can simply combine these into (abc). Lastly, 2-cycles sharing no elements may be rewritten by use of the identity,

$$(ab)(cd) = (ab)(bc)(cb)(cd) = (abc)(cdb).$$

All pairs in our 2-cycle representation of A_n have thus been converted into products of 3-cycles. A_1 is the identity and A_2 is not a group, being as there are no even permutations that make only one exchange by definition. Thus our above result holds only for $n \geq 3$.

1.3. Show that S_n is isomorphic to a subgroup of A_{n+2}. Write down explicitly how S_3 is a subgroup of A_5.

In order to show that S_n is isomorphic to a subgroup of A_{n+2}, we must produce a bijective homomorphism from one to the other.

It is clear that all even permutations within S_n can be mapped to themselves, as A_{n+2} contains these elements. For odd permutations, consider the mapping $\sigma \to \phi(\sigma) = \sigma(n+1, n+2)$. When applied to an even permutation τ, we define $\phi(\tau) = \tau$.

To check if this is a homomorphism, look at $\phi(\sigma\tau)$, where $\sigma, \tau \in S_n$. If σ and τ are both even, their product is even and we have $\phi(\sigma\tau) = \sigma\tau = \phi(\sigma)\phi(\tau)$. If they are both odd, their product is also even. In that case, we have

$$\phi(\sigma\tau) = \sigma\tau = \sigma(n+1, n+2)\tau(n+1, n+2) = \phi(\sigma)\phi(\tau).$$

In the case where one permutation is odd and the other even, their product is also odd. Their mapping becomes

$$\phi(\sigma\tau) = \sigma\tau(n+1, n+2) = \phi(\sigma)\phi(\tau).$$

Being as a homomorphism preserves the group structure, our image (contained within A_{n+2}) is a group.

Using the above, we see S_3 can be mapped to

$$\begin{aligned} I &\to I \\ (12) &\to (12)(45) \\ (13) &\to (13)(45) \\ (23) &\to (23)(45) \\ (123) &\to (123) \\ (132) &\to (132) \end{aligned}$$

where we have denoted the identity permutation by I.

1.4. List the partitions of 5. (We will need this later.)

The seven partitions of 5 are given by

$$\begin{gathered} 1+1+1+1+1 \\ 1+1+1+2 \\ 1+2+2 \\ 1+1+3 \\ 2+3 \\ 1+4 \\ 5 \end{gathered}$$

1.5. Count the number of elements with a given cycle structure.

We'll use a specific cycle structure to keep track of everything. The methods used are easily generalized to any cycle structure.

Consider the structure given on page 59,

$$(xxxxx)(xxxxx)(xxxx)(xx)(xx)(xx)(x)(x)(x)(x),$$

or $n_5 = 2$, $n_4 = 1$, $n_3 = 0$, $n_2 = 3$, and $n_1 = 4$ (with $n = 24$). How many cycles can represented using a similar structure?

There are $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20$ ways to populate the first cycle, but this is over counting by a factor of 5 (being as cycles such as (12345) and (23451) are really the same). The possibilities for the second cycle are found similarly: there are $(19 \cdot 18 \cdot 17 \cdot 16 \cdot 15)/5$ ways to fill it.

If we continued on and began counting the possible $(xxxx)$ cycles, we'd be missing another source of error: the first two cycles can be exchanged without altering our permutation. Indeed, if we continue without changing anything we'll be over counting each group of j elements by a factor of $n_j!$ Fixing this, we see there are

$$\frac{24 \cdot 23 \cdots 15}{5^2 \cdot 2!}$$

different ways of choosing the first two cycles. We can continue this to find the expression for the total number of elements with a given cycle structure is

$$\frac{n!}{\prod_j j^{n_j} \cdot n_j!}.$$

1.6. List the possible cycle structures in S_5 and count the number of elements with each structure.

Our answer to question 4 comes in handy here, as the partitions of n are related to the cycle structures of S_n. There are seven possible cycle structures,

$$\begin{gathered}(x)(x)(x)(x)(x)\\(x)(x)(x)(xx)\\(x)(xx)(xx)\\(x)(x)(xxx)\\(xx)(xxx)\\(x)(xxxx)\\(xxxxx)\end{gathered}$$

Using the above formula, we see that these have, respectively, 1, 60, 15, 40, 20, 30, and 24 associated permutations.

1.7. Show that $\mathcal{Q}$ forms a group.

Clearly, by Hamilton's multiplication rules our set is closed. It also has the identity, 1. Each element's inverse is given by

$$\begin{aligned}1^{-1} &= 1\\-1^{-1} &= -1\\i^{-1} &= -i\\-i^{-1} &= i\\j^{-1} &= -j\\-j^{-1} &= j\\k^{-1} &= -k\\-k^{-1} &= k\end{aligned}$$

Being as $\mathcal{Q}$ obeys these three properties, it forms a group.

1.8. Show that A_4 is not simple.

To show that A_4 is not simple, we need to find an invariant (or normal) subgroup. The subgroup $Z_2 \otimes Z_2$ is given as an example of one in the text, so we need only verify this. Explicitly, this subgroup takes the form

$$\{I, (12)(34), (13)(24), (14)(23)\} = Z_2 \otimes Z_2 \subset A_4,$$

i.e. it is the identity paired with all combinations of disjoint 2-cycles. The remaining elements in A_4 take the (disjoint) form of individual 3-cycles. Obviously, $g^{-1}Ig = I$ for all $g \in A_4$, so let's concentrate on the nontrivial elements.

Label $Z_2 \otimes Z_2$'s 2-cycles by σ_i and consider a 3-cycle in A_4 (denoted by τ). We must show that

$$\tau^{-1}\sigma_i\sigma_j\tau \subset Z_2 \otimes Z_2.$$

Inserting the identity between σ's leaves us with $\tau^{-1}\sigma_i\sigma_j\tau = \tau^{-1}\sigma_i\tau\tau^{-1}\sigma_j\tau$. Consider just $\tau^{-1}\sigma_i\tau$. If $\sigma_i : j \to k$, then

$$\tau^{-1}\sigma_i\tau : \tau^{-1}(j) \to \tau^{-1}(k).$$

This is because

$$\tau^{-1}\sigma_i\tau(\tau^{-1}(j)) = \tau^{-1}\sigma_i(j) = \tau^{-1}(k).$$

Because τ is injective, τ^{-1} defines a unique mapping. The result is that $\tau^{-1}\sigma_i\tau$ is disjoint from $\tau^{-1}\sigma_j\tau$ when $i \neq j$. But the product of two disjoint 2-cycles is a defining feature of $Z_2 \otimes Z_2$, and so $Z_2 \otimes Z_2$ is normal. This, of course, implies (by definition) that A_4 is not simple.

1.9. Show that A_4 is an invariant subgroup (in fact, maximal) of S_4.

The same argument can be made as above for general cycle structures. In particular, we can think of transformations like $g^{-1}hg$ for $g \in S_4$ and $h \in A_4$ as changes of basis (or relabeling procedures). That is, g renames element i to j, which is acted upon by h, which is then taken back to its original set. The elements of A_4 remain even permutations no matter what is fed to them.

1.10. Show that the kernel of a homomorphic map of a group G into itself is an invariant subgroup of G.

There are two parts to this. Given a set $\{g \in G | \phi(g) = e\}$, we must first show that the elements g form a group. Secondly, we must show that the given group is normal.

The set given contains the identity. Consider $\phi(e) = h$ for some $h \in G$. Then

$$e = \phi(e)\phi(e)^{-1} = \phi(e)\phi(e^{-1}) = \phi(e)\phi(e) = \phi(e \cdot e) = \phi(e) = h,$$

where $\phi(g)^{-1} = \phi(g^{-1})$ can be seen from the fact that $\phi(gg^{-1}) = \phi(g)\phi(g^{-1}) = e$. Furthermore, it is closed under multiplication: given g, h in our subset,

$$\phi(gh) = \phi(g)\phi(h) = e \cdot e = e.$$

Taken together, we see our set forms a group, and so is a subgroup of G. Now consider performing a similarity transformation on it by an element $h \in G$ that's *not* in our subgroup. Is this still in our subgroup? We have

$$\phi(h^{-1}gh) = \phi(h^{-1})\phi(g)\phi(h) = \phi(h)^{-1} \cdot e \cdot \phi(h) = \phi(h)^{-1}\phi(h) = e.$$

1.11. Calculate the derived subgroup of the dihedral group.

As detailed in the text,

$$D_n = \{I, R, R^2, \cdots, R^{n-1}, r, Rr, R^2r, \cdots, R^{n-1}r\}.$$

The derived subgroup of this is given by all elements of the form $\langle a, b\rangle = a^{-1}b^{-1}ab$ where $a, b \in D_n$, as well as products of these elements.

When a, b are pure rotations, $\langle a, b\rangle = I$. This is because

$$\langle R^i, R^j\rangle = R^{n-i}R^{n-j}R^iR^j = R^{2n-i-j+i+j} = R^{2n} = I.$$

When a is a rotation and b is a rotation and reflection, we have

$$\langle R^i, R^jr\rangle = R^{n-i}rR^{n-j}R^iR^jr = R^{n-i}rR^ir = R^{2(n-i)},$$

using the fact that $rRr = R^{-1}$. Swapping the order of these, we see

$$\langle R^jr, R^i\rangle = rR^{n-j}R^{n-i}R^jrR^i = rR^{-i}rR^i = R^{2i}.$$

Finally,

$$\langle R^ir, R^jr\rangle = rR^{n-i}rR^{n-j}R^irR^jr = R^iR^{n-j}R^iR^{n-j} = R^{2(n-j+i)},$$

so all elements of the form $\langle a, b\rangle$ are rotations. Clearly, products of these elements are also rotations. So our derived subgroup is given by

$$D = \{I, R, R^2, \cdots, R^{n-1}\}.$$

1.12. Given two group elements f and g, show that, while in general $fg \neq gf$, fg is equivalent to gf (That is, they are in the same equivalence class).

We have defined our equivalence classes as objects that can be related by similarity transformations, i.e. $g' \sim g$ if $g' = h^{-1}gh$ for some $h \in G$. In the case of fg, we see

$$gf \sim g^{-1}gfg = fg.$$

1.13. Prove that groups of even order contain at least one element (which is not the identity) that squares to the identity.

1.14. Using Cayley's theorem, map V to a subgroup of S_4. List the permutation corresponding to each element of V. Do the same for Z_4.

1.15. Map a finite group G with n elements into S_n a la Cayley. The map selects n permutations, known as "regular permutations," with various special properties, out of the $n!$ possible permutations of n objects.

(a) Show that no regular permutations besides the identity leaves an object untouched.

(b) Show that each of the regular permutations takes object 1 (say) to a different object.

(c) Show that when a regular permutation is resolved into cycles, the cycles all have the same length. Verify that these properties hold for what you got in exercise 14.

1.16. In a Coxeter group, show that if $n_{ij} = 2$, then a_i and a_j commute.

1.17. Show that for an invariant subgroup H, the left coset gH is equal to the right coset Hg.

A normal subgroup H obeys $g^{-1}Hg = H$ for all $g \in G$ (where $H \subset G$). Multiplying this condition by g from the left shows

$$Hg = gH.$$

1.18. In general, a group H can be embedded as a subgroup into a larger group G in more than one way. For example, A_4 can be naturally embedded into S_6 by following the route $A_4 \subset S_4 \subset S_5 \subset S_6$. Find another way of embedding A_4 into S_6. Hint: Think geometry!

1.19. Show that the derived subgroup of S_n is A_n. (In the text, with the remark about even permutations we merely showed that it is a subgroup of S_n.)

1.20. A set of real-valued functions f_i of a real variable x can also define a group if we define multiplication as follows: given f_i and f_j, the product $f_i \cdot f_j$ is defined as the function $f_i(f_j(x))$. Show that the functions $I(x) = x$ and $A(x) = (1-x)^{-1}$ generate a three-element group. Furthermore, including the function $C(x) = x^{-1}$ generates a six-element group.

With multiplication defined this way, it is clear that $I(x)$ is the identity, as

$$I(f(x)) = f(x) \quad \text{and} \quad f(I(x)) = f(x)$$

for an arbitrary $f(x)$. So, given $I(x)$ and $A(x)$, only $A(x)$ acts meaningfully change a group element. Composing $A(x)$ with itself gives

$$A(A(x)) = \frac{1}{1 - \frac{1}{1-x}} = \frac{1-x}{1-x-1} = \frac{x-1}{x}.$$

Denoting this by $B(x)$ and composing it with $A(x)$ gives

$$B(A(x)) = \frac{\frac{1}{1-x} - 1}{\frac{1}{1-x}} = \frac{1-(1-x)}{1} = x = I(x)$$

while composing $B(x)$ with itself gives

$$B(B(x)) = \frac{\frac{x-1}{x} - 1}{\frac{x-1}{x}} = \frac{x-1-x}{x-1} = \frac{1}{1-x} = A(x).$$

Finally, composing $A(x)$ with $B(x)$ results in

$$A(B(x)) = \frac{1}{1 - \frac{x-1}{x}} = \frac{x}{x-(x-1)} = x = I(x)$$

The complete multiplication table is

	$I(x)$	$A(x)$	$B(x)$
$I(x)$	$I(x)$	$A(x)$	$B(x)$
$A(x)$	$A(x)$	$B(x)$	$I(x)$
$B(x)$	$B(x)$	$I(x)$	$A(x)$

and it is consistent with the properties of a 3 element group.

Let us investigate the effect of the inclusion of $C(x) = x^{-1}$ in the original set of functions. Clearly, $C(x)$ is its own inverse. Other possible compositions are

$$\begin{aligned}
A(C(x)) &= \frac{1}{1-\frac{1}{x}} = \frac{x}{x-1} = \frac{1}{B(x)} \equiv D(x) \\
B(C(x)) &= \frac{\frac{1}{x}-1}{\frac{1}{x}} = 1-x = \frac{1}{A(x)} \equiv E(x) \\
C(A(x)) &= \frac{1}{A(x)} = E(x) \\
C(B(x)) &= \frac{1}{B(x)} = D(x)
\end{aligned}$$

All that is left is to check that the inclusion of the newly defined functions $D(x)$ and $E(x)$ leave the set closed under composition. With $D(x)$ on the left, we have

$$\begin{aligned}
D(A(x)) &= \frac{\frac{1}{1-x}}{\frac{1}{1-x}-1} = \frac{1}{1-(1-x)} = \frac{1}{x} = C(x) \\
D(B(x)) &= \frac{\frac{x-1}{x}}{\frac{x-1}{x}-1} = \frac{x-1}{x-1-x} = 1-x = E(x) \\
D(C(x)) &= \frac{\frac{1}{x}}{\frac{1}{x}-1} = \frac{1}{1-x} = A(x) \\
D(D(x)) &= \frac{\frac{x}{x-1}}{\frac{x}{x-1}-1} = \frac{x}{x-(x-1)} = x = I(x) \\
D(E(x)) &= \frac{1-x}{1-x-1} = \frac{x-1}{x} = B(x)
\end{aligned}$$

While a similar analysis of $E(x)$ reveals

$$\begin{aligned}
E(A(x)) &= 1-\frac{1}{1-x} = \frac{x}{x-1} = D(x) \\
E(B(x)) &= 1-\frac{x-1}{x} = \frac{1}{x} = C(x) \\
E(C(x)) &= 1-\frac{1}{x} = \frac{x-1}{x} = B(x) \\
E(D(x)) &= 1-\frac{x}{x-1} = \frac{1}{1-x} = A(x) \\
E(E(x)) &= 1-(1-x) = x = I(x)
\end{aligned}$$

With $D(x)$ and $E(x)$ as the inner function, we find

$$\begin{aligned}
A(D(x)) &= \frac{1}{1-\frac{x}{x-1}} = \frac{x-1}{x-1-x} = 1-x = E(x) \\
A(E(x)) &= \frac{1}{1-(1-x)} = \frac{1}{x} = C(x) \\
B(D(x)) &= \frac{\frac{x}{x-1}-1}{\frac{x}{x-1}} = \frac{x-(x-1)}{x} = \frac{1}{x} = C(x) \\
B(E(x)) &= \frac{(1-x)-1}{1-x} = \frac{x}{x-1} = D(x) \\
C(D(x)) &= \frac{1}{\frac{x}{x-1}} = B(x) \\
C(E(x)) &= \frac{1}{1-x} = A(x)
\end{aligned}$$

The complete multiplication table of this new group is

	$I(x)$	$A(x)$	$B(x)$	$C(x)$	$D(x)$	$E(x)$
$I(x)$	$I(x)$	$A(x)$	$B(x)$	$C(x)$	$D(x)$	$E(x)$
$A(x)$	$A(x)$	$B(x)$	$I(x)$	$D(x)$	$E(x)$	$C(x)$
$B(x)$	$B(x)$	$I(x)$	$A(x)$	$E(x)$	$C(x)$	$D(x)$
$C(x)$	$C(x)$	$E(x)$	$D(x)$	$I(x)$	$B(x)$	$A(x)$
$D(x)$	$D(x)$	$C(x)$	$E(x)$	$A(x)$	$I(x)$	$B(x)$
$E(x)$	$E(x)$	$D(x)$	$C(x)$	$B(x)$	$A(x)$	$I(x)$