Algebra Exercises

Andrew Kobach

(Dated: September 8, 2025)

D&F refers to Dummit and Foote's *Abstract Algebra*, 3rd Ed. JG refers to Gillian's *Contemporary Abstract Algebra*, 9th Ed. Artin refers to Artin's *Algebra*, 2nd Ed.

Contents

I. BASIC AXIOMS AND EXAMPLES

D&F Exercise 0.1.5

Determine whether the following functions f are well defined:

(a) $f : \mathbb{Q} \to \mathbb{Z}$ *defined by* $f(a/b) = a$.

(b) $f : \mathbb{Q} \to \mathbb{Q}$ *defined by* $f(a/b) = a^2/b^2$.

(a) Let f be the function $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(a/b) = a$, where $a, b \in \mathbb{Z}$. This function is not well defined. We can show this with an explicit counter example: $f(1/2) = 1$, but $f(2/4) = 2$, despite the fact that $1/2$ and $2/4$ are equivalent.

(b) Let f be the function $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$. This function is well defined. To show this, let $a, b, c, d \in \mathbb{Z}$, where $b \neq 0$ and $d \neq 0$, and such that the two fractions a/b and c/d are equivalent: $a/b = c/d$. Then $f(a/b) = a^2/b^2 = (a/b)^2 = (c/d)^2 = c^2/d^2 = f(c/d)$.

D&F Exercise 0.1.7

Let $f : A \to B$ be a surjective map of sets. Prove that the relation

$$a \sim b \text{ if an only if } f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of f.

First, we will show that $\sim$ is an equivalence relation because it satisfies the following three conditions:

- Let $a \in A$. Since $f(a) = f(a)$, then $\sim$ is reflexive.
- Let $a, b \in A$. Since $f(a) = f(b)$ implies $f(b) = f(a)$, then $\sim$ is symmetric.
- Let $a, b, c \in A$. Since if $f(a) = f(b)$ and $f(b) = f(c)$ implies $f(a) = f(c)$, then $\sim$ is transitive.

Second, we will show that the equivalence classes defined by $\sim$ are the fibers of f. Let $a \in A$. Here, a belongs to an equivalence class $\{x \in A | x \sim a\} = \{x \in A | f(x) = f(a)\}$. Now let $f(a) = c$. The fiber of f over c is the set $\{x \in A | f(x) = f(a) = c\}$, which, by the definition of $\sim$, is identical to the equivalence class $\{x \in A | x \sim a\}$.

II. PROPERTIES OF THE INTEGERS

D&F Exercise 0.2.1

For each of the following pairs of integers a and b, determine their greatest common divisor, their least common multiple, and write their greatest common divisor in the form of $ax + by$ for some integers x and y.

(a) $a = 20$, $b = 13$

(b) $a = 69$, $b = 372$

(c) $a = 792$, $b = 275$

(d) $a = 11391$, $b = 5673$

(e) $a = 1761$, $b = 1567$

(f) $a = 507885$, $b = 60808$

The algorithm shown in Exercise 0.2.9 was used to compute the following:

(a) gcd(20, 13) = 1 = (2)(20) + (-3)(13), lcm(20, 13) = 260

(b) gcd(372, 69) = 3 = (-5)(372) + (27)(69), lcm(372, 69) = 8556

(c) gcd(792, 275) = 11 = (8)(792) + (-23)(275), lcm(792, 275) = 19800

(d) gcd(11391, 5673) = 3 = (-126)(11391) + (253)(5673), lcm(11391, 5673) = 21540381

(e) gcd(1761, 1567) = 1 = (-105)(1761) + (118)(1567), lcm(1761, 1567) = 2759487

(f) gcd(507885, 60808) = 691 = (-17)(507885) + (142)(60808), lcm(507885, 60808) = 44693880

D&F Exercise 0.2.5

Determine the value $\varphi(n)$ for each integer $n \leq 30$ where φ denotes the Euler φ-function.

Consider the prime factorization of $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, where $p_1, p_2, \cdots p_s$ are the prime factors of n, and $\alpha_1, \alpha_2, \cdots \alpha_s$ are positive integers. We then have the following expression for φ:

$$\begin{aligned} \varphi(n) &= p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_s^{\alpha_s - 1}(p_s - 1) && (1) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right). && (2) \end{aligned}$$

The first line in the above equation is stated on p. 7 in D&F. We can use the above expression to compute the value of $\varphi(n)$ for $1 \leq n \leq 30$:

$$\begin{array}{llllll} \varphi(1) = 1, & \varphi(2) = 1, & \varphi(3) = 2, & \varphi(4) = 2, & \varphi(5) = 4, & \varphi(6) = 2, \\ \varphi(7) = 6, & \varphi(8) = 4, & \varphi(9) = 6, & \varphi(10) = 4, & \varphi(1) = 10, & \varphi(12) = 4, \\ \varphi(13) = 12, & \varphi(14) = 6, & \varphi(15) = 8, & \varphi(16) = 8, & \varphi(17) = 16, & \varphi(18) = 6, \\ \varphi(19) = 18, & \varphi(20) = 8, & \varphi(21) = 12, & \varphi(22) = 10, & \varphi(23) = 22, & \varphi(24) = 8, \\ \varphi(25) = 20, & \varphi(26) = 12, & \varphi(27) = 18, & \varphi(28) = 12, & \varphi(29) = 28, & \varphi(30) = 8. \end{array} \quad (3)$$

D&F Exercise 0.2.7

If p is a prime prove that there do not exist nonzero integers a and b such that $a^2 = pb^2$ (i.e., $\sqrt{p}$ is not a rational number).

Let a, b, and c be positive integers, and p be a prime number. To begin, we need to prove two smaller results:

(i) If $a|bc$ and $(a, b) = 1$, then $a|c$.

(ii) If p is prime and $p|ab$, then $p|a$ or $p|b$.

Proof of (i). Given $(a, b) = 1$, we can use Bézout's theorem to say that there exists integers x and y such that

$$ax + by = 1. \quad (4)$$

Multiplying both sides by c, we have:

$$acx + bcy = c. \quad (5)$$

Furthermore, since $a|bc$, there is a positive integer k such that $ak = bc$. Inserting this into the above equation:

$$a(cx + ky) = c. \quad (6)$$

Because $cx + ky$ is an integer, we can conclude that $a|c$.

Proof of (ii). Assume $p|ab$. We will consider two exhaustive cases: when $p|b$ and when $p \nmid b$. In the first case, we have assumed $p|b$, which completes the proof. In the second case, we assume $p \nmid b$, but this means $(p, b) = 1$ because p is prime, and we can use the result in (i) to conclude that $p|a$, which also proves the desired result.

Now to prove the original statement that $\sqrt{p}$ is not a rational number. We proceed using proof by contradiction. Assume $\sqrt{p}$ is a rational number, i.e., there exists integers a and b such that

$$\sqrt{p} = \frac{a}{b}, \tag{7}$$

where we also assume, without loss of generality, that a and b have no common factors, i.e., the fraction is fully reduced. Squaring both sides of the above equation and multiplying both sides by b^2, we have:

$$pb^2 = a^2. \tag{8}$$

So, $p|a^2$. Using (ii), we can conclude $p|a$, i.e., there exists an integer k such that $pk = a$, which can be inserted into the above equation:

$$pb^2 = p^2k^2 \tag{9}$$
$$b^2 = pk^2. \tag{10}$$

So, $p|b^2$. Using (ii), we can conclude $p|b$. Therefore, we have claimed that both $p|a$ and $p|b$, which is contrary to our assumption that a and b have no common factors. Therefore, $\sqrt{p}$ is not rational.

D&F Exercise 0.2.8

Let p be a prime, $n \in \mathbb{Z}^+$. Find a formula for the largest power of p which divides $n! = n(n-1)(n-2)\cdots 2\cdot 1$ (it involves the greatest integer function).

Let p be a prime, $n \in \mathbb{Z}^+$. Our aim will be to find a formula for a largest power of p which divides $n!$. To quickly illustrate the method of solution, we can decompose $n!$ as a series of multiplications of every integer less than or equal to n:

$$n! = 1 \cdot 2 \cdot 3 \cdots n \tag{11}$$

We can think of this multiplicative decomposition as a list of integers $[1, 2, 3, \cdots, n]$. If we were to decompose the each item in the list into multiplicative factors, we want to know how many factors of p appear in the list in total. We can proceed by asking the following series of questions. First, which items in the list have at least one factor of p? The answer is all the multiples of p. The number of multiples of p in the list is $\lfloor n/p \rfloor$. Next, which items in the list have at least 2 factors of p? The answer is all the multiples of p^2. The number of multiples of p^2 in the list is $\lfloor n/p^2 \rfloor$. We can keep asking this question, asking which items in the list have at least one factor of p^k, increasing k every time, until k is large enough were we can stop. At what value of k do we stop? That is, we want to know the maximum value of k such that $p^k \leq n$. We can take the log of both sides, and the inequality if preserved, since log is a monotonic function, yielding $k \leq \log_p n$. But since k is an integer, we can preserve this inequality by using the floor function, $k \leq \lfloor \log_p n \rfloor$. So, the total number of factors of p in $n!$ is:

$$\alpha := \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^{\lfloor \log_p n \rfloor}} \right\rfloor = \sum_{i=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^i} \right\rfloor \tag{12}$$

Since α is the total number of factors of p in $n!$, then α is the largest power of p that divides $n!$.

We will find it useful later on to derive an upper bound on α. To do so, we can note the following:

$$\sum_{i=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^i} \right\rfloor \leq \sum_{i=1}^{\lfloor \log_p n \rfloor} \frac{n}{p^i} = \frac{n}{p-1}\left(1 - p^{-\lfloor \log_p n \rfloor}\right) \leq \frac{n}{p-1}\left(1 - p^{-\log_p n}\right) = \frac{n-1}{p-1} \tag{13}$$

The summarize, the number of factors of p in $n!$ can be no greater than $(n-1)/(p-1)$.

D&F Exercise 0.2.9

Write a computer program to determine the greatest common divisor (a, b) of two integers a and b and to express (a, b) in the form $ax + by$ for some integers x and y.

Below is a PYTHON function that takes a and b as inputs, and prints their greatest common divisor (gcd), their least common multiple (lcm), and a (non-unique) expression for the gcd in the form $ax + by$, where x and y are integers.

The main idea behind this algorithm is the recursive expression for the remainder after each step in the Euclidean algorithm:

$$r_n = r_{n-2} - qr_{n-1} \tag{14}$$

where $q = \lfloor r_{n-2}/r_{n-1} \rfloor$. This can be easily derived by writing down subsequent steps in the algorithm, noting that the equations require the initial conditions $r_{-2} = a$ and $r_{-1} = b$.

```
def eulidean_algorithm(a:int, b:int) -> None:

    # ensure both a and b are integers
    if (a % 1 != 0) or (b % 1 != 0):
        print("Error! Please input integers.")
        return

    # choose b to be the smaller integer
    b, a = sorted([a,b])

    # initial conditions
    x, x_old = 0, 1
    y, y_old = 1, 0
    r, r_old = b, a

    # Euclidean algorithm
    while r > 0:
        q = r_old // r
        x, x_old = x_old - q*x, x
        y, y_old = y_old - q*y, y
        r, r_old = r_old - q*r, r

    gcd, x, y = r_old, x_old, y_old
    lcm = int(a*b/gcd)

    print(f"gcd({a}, {b}) = {gcd} = ({x})({a}) + ({y})({b})")
    print(f"lcm({a}, {b}) = {lcm}")
```

Results using this algorithm can be found in Exercise 0.2.1.

D&F Exercise 0.2.10

Prove for any given positive integer N there exist only finitely many integers n with $\varphi(n) = N$ where φ denotes the Euler φ-function. Conclude in particular that $\varphi(n)$ tends to infinity as n tends to infinity.

[Unsolved]

III. $\mathbb{Z}/n\mathbb{Z}$: THE INTEGERS MODULO n

D&F Exercise 0.3.4

Compute the remainder when 37^{100} is divided by 29.

In the following, mod 29 is implied:

$$\begin{aligned}
37 &\equiv 8 && (15)\\
37^2 &\equiv 8^2 = 64 \equiv 6 && (16)\\
37^4 &= (37^2)^2 \equiv 6^2 = 36 \equiv 7 && (17)\\
37^8 &= (37^4)^2 \equiv 7^2 = 49 \equiv 20 && (18)\\
37^{16} &= (37^8)^2 \equiv 20^2 = 400 \equiv 23 && (19)\\
37^{32} &= (37^{16})^2 \equiv 23^2 = 529 \equiv 7 && (20)\\
37^{64} &= (37^{32})^2 \equiv 7^2 = 49 \equiv 20 && (21)\\
37^{100} &= 37^{64} \cdot 37^{32} \cdot 37^4 \equiv 20 \cdot 7 \cdot 7 = 980 \equiv 23 && (22)
\end{aligned}$$

In summary, $37^{100} \equiv 23 \pmod{29}$.

D&F Exercise 0.3.6

Prove that the square of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\overline{0}$ and $\overline{1}$.

We will square each element of $\mathbb{Z}/4\mathbb{Z}$, i.e., $\overline{0}, \overline{1}, \overline{2}$, and $\overline{3}$, and show explicitly that they are either equal to $\overline{0}$ or $\overline{1}$:

$$\begin{aligned}
\overline{0}^2 &\equiv \overline{0^2} \equiv \overline{0} && (23)\\
\overline{1}^2 &\equiv \overline{1^2} \equiv \overline{1} && (24)\\
\overline{2}^2 &\equiv \overline{2^2} \equiv \overline{4} \equiv \overline{0} && (25)\\
\overline{3}^2 &\equiv \overline{3^2} \equiv \overline{9} \equiv \overline{1} && (26)
\end{aligned}$$

D&F Exercise 0.3.7

Prove for any integers a and b that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4 (use the previous exercise).

Let $a, b \in \mathbb{Z}$. To determine whether $a^2 + b^2$ can ever have a remainder of 3 when divided by 4, it suffices to ask whether $a^2 + b^2 \stackrel{?}{\equiv} 3 \pmod{4}$. To show that this is not possible, we can use modular arithmetic mod 4:

$$\overline{a^2 + b^2} \equiv \overline{a^2} + \overline{b^2} \equiv \overline{a}^2 + \overline{b}^2 \equiv \begin{cases} \overline{0}, \text{ if } \overline{a}^2 = \overline{0},\ \overline{b}^2 = \overline{0} \\ \overline{1}, \text{ if } \overline{a}^2 = \overline{1},\ \overline{b}^2 = \overline{0} \\ \overline{1}, \text{ if } \overline{a}^2 = \overline{0},\ \overline{b}^2 = \overline{1} \\ \overline{2}, \text{ if } \overline{a}^2 = \overline{1},\ \overline{b}^2 = \overline{1} \end{cases} \tag{27}$$

The last step uses the result from the previous problem, i.e., that the square of elements of $\mathbb{Z}/4\mathbb{Z}$ are either $\overline{0}$ or $\overline{1}$. Therefore, $a^2 + b^2$ cannot have a remainder of 3 when divided by 4, it can only have a remainder of 0, 1, or 2.

D&F Exercise 0.3.8

Prove that the equation $a^2 + b^2 = 3c^2$ has no solutions in nonzero integers a, b, and c. [Consider the equation mod 4 as in the previous two exercises and show that a, b, and c would all have to be divisible by 2. Then each a^2, b^2, and c^2 has a factor of 4 and by dividing through by 4 show that there would be a smaller set of solutions to the original equation. Iterate to reach a contradiction.]

Let a, b, c be nonzero integers. To prove that the equation $a^2 + b^2 = 3c^2$ has no solutions, we'll begin by considering this equation mod 4:

$$\overline{a^2 + b^2} \equiv \overline{3c^2} \tag{28}$$

$$\overline{a}^2 + \overline{b}^2 \equiv 3\overline{c}^2 \tag{29}$$

In the previous exercises, two things were shown: (i) square of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\overline{0}$ and $\overline{1}$, and (ii) $a^2 + b^2$ can only ever be $\overline{0}$, $\overline{1}$, or $\overline{2}$. Using (i), $\overline{c}^2$ must be either $\overline{0}$ or $\overline{1}$, so $3\overline{c}^2$ can be only $\overline{0}$ or $\overline{3}$. Using (ii), if $\overline{a}^2 + \overline{b}^2 \equiv 3\overline{c}^2$, then $\overline{a}^2 + \overline{b}^2$ and $\overline{c}^2$ must be congruent to $\overline{0}$. This means that the quantities $a^2 + b^2$ and c^2 are both divisible by 4. So, we can define new variables $a' = a/4$, $b' = b/4$, and $c' = c/4$, yielding an equation of the same form: $a'^2 + b'^2 = 3c'^2$. But then we can perform the same steps to conclude that a', b', and c' themselves are divisible by 4, yielding new variables $a'' = a'/4$, $b'' = b'/4$, $c'' = c'/4$, and this process can be repeated ad infinitum. However, this is not possible, since one cannot divide a nonzero integer by 4 an arbitrary number of times, yielding an integer every time. Therefore, there are no nonzero integer solutions to $a^2 + b^2 = 3c^2$.

D&F Exercise 0.3.10

Prove that the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$ where φ denotes the Euler φ-function.

The elements of $\mathbb{Z}/n\mathbb{Z}$ are in a one-to-one correspondence with the nonnegative integers less than n. On the one hand, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ only contains the elements $\overline{a}$ of $\mathbb{Z}/n\mathbb{Z}$ for which $(a, n) = 1$. On the other hand, $\varphi(n)$ is the number of nonnegative integers a that are less than n for which $(a, n) = 1$. Because of this correspondence, the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$.

D&F Exercise 0.3.12

Let $n \in \mathbb{Z}$, $n > 1$, and $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if a and n are not relatively prime, there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 \pmod{n}$, and deduce that there cannot be an integer c such that $ac \equiv 1 \pmod{n}$.

Let $n \in \mathbb{Z}$, $n > 1$, and $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Since a and n are not relatively prime, i.e., $(a, n) \neq 1$, let $(a, n) = d$, where $d > 1$. Then there exist integers q and b such that $a = qd$ and $n = bd$, where $1 \leq q < a$ and $1 \leq b < n$. Solving for d in both of these equations, and setting them equal yields $a/q = n/b$, or rather, $ab = qn$, which is just the statement that $ab \equiv 0 \pmod{n}$.

We have shown that there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 \pmod{n}$. Suppose there is an integer c such that $ac \equiv 1 \pmod{n}$. Multiplying both sides by b, we have $abc \equiv b \pmod{n}$. But $ab \equiv 0 \pmod{n}$, so this implies $0 \equiv b \pmod{n}$, which means that b is a multiple of n. However, this is contrary to our assumption that $1 \leq b < n$. Therefore, there cannot be an integer c such that $ac \equiv 1 \pmod{n}$.

D&F Exercise 0.3.13

Let $n \in \mathbb{Z}$, $n > 1$, and $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if a and n are relatively prime then there is an integer c such that $ac \equiv 1 \pmod{n}$ [use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers.]

Let $n \in \mathbb{Z}$, $n > 1$, and $a \in \mathbb{Z}$ with $1 \leq a \leq n$. According to Bézout's theorem, there exists integers c and q such that $ac + nq = (a, n)$. This equation can be rearranged as $ac = -nq + (a, n)$, which is the same as $ac \equiv (a, n) \pmod{n}$. Since $(a, n) = 1$, then we have $ac \equiv 1 \pmod{n}$.

IV. GROUPS: DEFINITION AND EXAMPLES

D&F Exercise 1.1.1

Determine which of the following binary operations are associative:

(a) the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$

(b) the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$

(c) the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \dfrac{a+b}{5}$

(d) the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$

(e) the operation $\star$ on $\mathbb{Q} - \{0\}$ defined by $a \star b = \dfrac{a}{b}$

(a) $\star$ is not associative. As an example, let $a = 1$, $b = 2$, $c = 3$. Then $(a \star b) \star c = (1 - 2) - 3 = -4$, but $a \star (b \star c) = 1 - (2 - 3) = 2$.

(b) $(a \star b) \star c = a + b + c + ab + ac + bc + abc$, and $a \star (b \star c) = a + b + c + ab + ac + bc + abc$, so this operation is associative.

(c) $\star$ is not associative. As an example, let $a = 1$, $b = 2$, $c = 3$. Then $(a \star b) \star c = \dfrac{\frac{a+b}{5} + c}{5} = \dfrac{\frac{1+2}{5} + 3}{5} = \dfrac{18}{25}$, but $a \star (b \star c) = \dfrac{a + \frac{b+c}{5}}{5} = \dfrac{1 + \frac{2+3}{5}}{5} = \dfrac{2}{5}$.

(d) $((a, b) \star (c, d)) \star (e, f) = (adf + bcf + bde, bdf)$, and $(a, b) \star ((c, d) \star (e, f)) = (adf + bcf + bde, bdf)$, so $\star$ is associative.

(e) $\star$ is not associative. As an example, let $a = 1$, $b = 2$, $c = 3$. Then $(a \star b) \star c = \dfrac{a}{bc} = \dfrac{1}{(2)(3)} = \dfrac{1}{6}$, but $a \star (b \star c) = \dfrac{ac}{b} = \dfrac{(1)(3)}{2} = \dfrac{3}{2}$.

D&F Exercise 1.1.5

Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

The set $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes because $\overline{0}$ does not have an inverse in $\mathbb{Z}/n\mathbb{Z}$. To show this, we will proceed via proof by contradiction. Assume that $\mathbb{Z}/n\mathbb{Z}$ is a group under multiplication of residue classes, call it G. First, it must contain an identity element $\overline{1}$ with the property that for any $\overline{a} \in G$, that $\overline{a} \cdot \overline{1} = \overline{a}$. This follows from the definition of a group. Second, G contains an element $\overline{0}$ with the property that for any $\overline{a} \in G$, that $\overline{a} \cdot \overline{0} = \overline{0}$. This follows from the properties of $\mathbb{Z}/n\mathbb{Z}$.

On the one hand, $\overline{0} \cdot \overline{1} = \overline{0} \neq \overline{1}$, so we can conclude that $\overline{0}$ is not the identity. (Since $n > 1$, we can be assured that there are at least two elements in G, i.e., $\overline{1}$ and $\overline{0}$.) On the other hand, $\overline{0}$ must have an inverse $\overline{b} \in G$, i.e., $\overline{b} \cdot \overline{0} = \overline{1}$. But since $\overline{b} \cdot \overline{0} = \overline{0}$, then $\overline{1} = \overline{0}$, which is in contradiction to the previous conclusion that $\overline{1} \neq \overline{0}$. Therefore, $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

D&F Exercise 1.1.6

Determine which of the following sets are groups under addition:

(a) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd

(b) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even

(c) the set of rational numbers of absolute value < 1

(d) the set of rational numbers of absolute value ≥ 1 together with 0

(e) the set of rational numbers with denominators equal to 1 or 2

(f) the set of rational numbers with denominators equal to 1, 2, or 3.

(a) The set G of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd is a group under addition. To show this, we will demonstrate that G has the following four properties:

- G is closed under addition. Let $a, b \in G$, where a and b can be expressed as fractions in lowest terms $a = c/d$ and $b = e/f$ with odd denominators, where c, d, e, f are integers, $(c, d) = 1$, $(e, f) = 1$, and d and f are odd. Under addition, $a + b = c/d + e/f = (cf + ed)/(df)$. To show that G is closed, we need to show that $(cf + ed)/(df)$ has an odd denominator when this fraction is expressed in lowest terms. Let $(cf + ed)/(df) = x/y$, where the fraction x/y is in lowest terms. This means $y|df$. But d and f are both odd, so df is also odd. But no even number can divide an odd number, so y cannot be even. Therefore, y is odd, and this means G is closed under addition.
- G contains and identity. The identity element is $0/1$, since $a + 0/1 = a$ for all $a \in G$.
- All elements of G have an inverse in G. The inverse of an element $a \in G$ is $-a$ since $-a \in G$, and $a - a = -a + a = 0/1$.
- G is associative. Let $a, b, c \in G$. Associativity of G follows from the associativity over the rational numbers.

(b) The set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even is not a group under addition. To show this, consider rational numbers $a = 1/2$ and $b = 1/2$, both of which are in lowest terms and have denominators that are even. However, $a + b = 1/2 + 1/2 = 1/1$, which is a rational number in lowest terms with an odd denominator. So, this set is not closed under addition and is therefore not a group.

(c) The set of rational numbers of absolute value < 1 is not a group under addition. To show this, consider rational numbers $a = 1/2$ and $b = 3/4$, both of which have absolute value < 1. Under addition, $a + b = 1/2 + 3/4 = 5/4$, which has absolute value > 1. So, this set is not closed under addition, so it cannot be a group.

(d) The set of rational numbers of absolute value ≥ 1 together with 0 is not a group under addition. To show this, consider rational numbers $a = 3/2$ and $b = -1$, both of which have absolute value ≥ 1. Under addition, $a + b = 3/2 - 1 = 1/2$, which has absolute value < 1. This set is not closed under addition, so it cannot be a group.

(e) The set G of rational numbers with denominators equal to 1 or 2 under addition is a group. To show this, we will demonstrate that it has the four following properties. In the following, let $a, b, c \in \mathbb{Z}$ and $m, n, \ell \in \{1, 2\}$.

- G is closed under addition. Here, a/n and b/m are elements of G. Under addition, $a/n+b/m = (am+bn)/(mn)$. Here, we will need to show that this fraction, has a denominator that is equal to 1 or 2. Because m and n can each take on values 1 or 2, mn can take on three values: 1, 2, or 4. If $mn = 1$ or 2, then this is still a fraction with denominators equal to 1 or 2, so these are elements of G. If $mn = 4$, then this only occurs when $m = n = 2$, and therefore $(am+bn)/(mn) = (a+b)/2$, which is a fraction with denominator 2, so it is also an element of G. Therefore, this G is closed under addition.
- G contains an identity. The identity is element is $0/1$, since $a/n + 0/1 = a/n$.
- All elements of G have an inverse in G. The inverse of an element a/n is $-a/n$, since $-a/n \in G$ and $a/n - a/n = -a/n + a/n = 0/1$.
- G is associative. Here, a/n, b/m, and c/ℓ are elements of G. Associativity of G follows from associativity of addition over the rational numbers.

(f) The set G of rational numbers with denominators equal to 1, 2, or 3 under addition is not a group. To show this, consider rational numbers $a = 1/2$ and $b = 1/3$, which have denominators equal to 2 and 3, respectively. Under addition, $a + b = 1/2 + 1/3 = 5/6$, which is a fraction that cannot be expressed as a fraction with denominator equal to 1, 2, or 3. So, this set is not close under addition, and it cannot be a group.

D&F Exercise 1.1.7

Let $G = \{x \in \mathbb{R} | 0 \leq x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$ (i.e., $x \star y = x + y - [x + y]$ where $[a]$ is the greatest integer less than or equal to a). Prove that $\star$ is a well defined binary operation on G and that G is an abelian group under $\star$ (called the "real numbers mod 1").

Let $G = \{x \in \mathbb{R} | 0 \leq x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$.

First, we will show that $\star$ is a well defined binary operation on G. Let $a, b \in G$, and consider the quantity $a+b$, which lies in the range $0 \leq a+b < 2$. Then we can consider two cases: (1) if $0 \leq a+b < 1$, then $[a+b] = 0$, so $a \star b = a + b \in G$, and (2) if $1 \leq a + b < 2$, then $[a+b] = 1$, so $a \star b = a + b - 1 \in G$. Therefore, $\star$ is a well defined binary operation on G.

Second, we will show that G is an abelian group under $\star$. For G to be an abelian group under $\star$, it must satisfy the following five requirements:

- $\star$ must be a well defined binary operation on G. This was shown in the previous paragraph.
- G contains the identity element. Here, the identity element is $0 \in G$, since $a \star 0 = a + 0 - [a] = a$ for all $a \in G$, since $[a] = 0$.
- All elements of G have an inverse also in G. To show this, let $a \in G$, then the inverse of a is $(1 - a) \in G$, since $a \star (1 - a) = a + 1 - a - [a + 1 - a] = 1 - [1] = 0$ and $(1 - a) \star a = 1 - a + a - [1 - a + a] = 1 - [1] = 0$ for all $a \in G$, since $[1] = 0$.
- G is associative under $\star$. This follows from the associativity of the real numbers under addition.
- G is abelian under $\star$. Let $a, b \in G$. Then $a \star b = a + b - [a + b]$ and $b \star a = b + a - [b + a] = a + b - [a + b] = a \star b$, for all $a, b \in G$.

Note: Here, $\star$ reminds me of adding angles that represent points on a circle, and G seems like it may be isomorphic to the Lie group $U(1)$.

D&F Exercise 1.1.8

Let $G = \{x \in \mathbb{C} | z^n = 1$ for some $n \in \mathbb{Z}^+\}$.

(a) Prove that G is a group under multiplication (called the group of roots of unity in $\mathbb{C}$).

(b) Prove that G is not a group under addition.

Let $G = \{z \in \mathbb{C} | z^n = 1$ for some $n \in \mathbb{Z}^+\}$.

(a) To prove that G is a group under multiplication, we must show the following four properties:

- G contains the identity element of $(\mathbb{C}, \cdot)$, i.e., 1. Here, $1 \in G$, since $z \cdot 1 = z$ for all $z \in G$.
- G is closed under multiplication. To show this, let $y, z \in G$. Specifically, this means both y and z are nth roots of unity, i.e., $y^n = z^n = 1$. We can note that $(yz)^n = y^n z^n$, which follows from the fact that multiplication is commutative over $\mathbb{C}$. From this, we can conclude that $(yz)^n = y^n z^n = 1$. Therefore $(yz)^n$ is also a nth root of unity, so G is closed under multiplication.
- All elements of G have an inverse also in G. To show this, let $z \in G$. The inverse of $z \in G$ is z^{n-1}, since $z^{n-1} \in G$ and $zz^{n-1} = z^{n-1}z = z^n = 1$.
- Associativity follows from the fact that multiplication is associative over $\mathbb{C}$.

(b) To prove that G is not a group under addition, consider adding the element 1 to itself: $1 + 1 = 2$, but 2 is not an element of G, since $2^n \neq 1$ for any $n \in \mathbb{Z}^+$.

D&F Exercise 1.1.9

Let $G = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\}$.

(a) Prove that G is a group under addition.

(b) Prove that the nonzero elements of G are a group under multiplication. ["Rationalize the denominators" to find the multiplicative inverses.]

Let $G = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\}$.

(a) To prove that G is a group under addition, we must show the following four properties:

- The element $0 = 0 + 0\sqrt{2}$ is the identity element of G. This follows since $0 \in \mathbb{Q}$, and letting $g = a + b\sqrt{2} \in G$, where $a, b \in \mathbb{Q}$, and we can note that $g + 0 = a + b\sqrt{2} + 0 = a + b\sqrt{2} = g$. This holds for all $g \in G$, so 0 is the identity element.
- G is closed under addition. To show this, let $g, g' \in G$, such that $g = a + b\sqrt{2}$ and $g' = c + d\sqrt{2}$, where $a, b, c, d \in \mathbb{Q}$. Here, $g + g' = a + b\sqrt{2} + c + d\sqrt{2} = (a + b) + (c + d)\sqrt{2}$. Since $a + b \in \mathbb{Q}$ and $c + d \in \mathbb{Q}$, then $g + g' \in G$ for all $g, g' \in G$.
- Every element of G has an inverse also in G. Here, the inverse of an element $g = a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$, is $-g = -a - b\sqrt{2} \in G$. This follows since $-a, -b \in \mathbb{Q}$, and since $g - g = a + b\sqrt{2} - a - b\sqrt{2} = 0$ and $-g - g = -a - b\sqrt{2} + a + b\sqrt{2} = 0$.
- Associativity follows from the associativity of addition on $\mathbb{R}$.

(b) Let G' consist of the nonzero elements of G, i.e., $G' = G - \{0\}$. To prove that G' is a group under multiplication, we must show the following four properties:

- The element $1 = 1 + 0\sqrt{2}$ is the identity element of G'. To show this, we can note that $1 = 1 + 0\sqrt{2} \in G'$, and letting $g = a + b\sqrt{2} \in G$, where $a, b \in \mathbb{Q}$, we can also note that $g \cdot 1 = a + b\sqrt{2} = g$. Since this holds for all $g \in G$, then 1 is the identity.
- G' is closed under multiplication. To show this, let $g, g' \in G'$, such that $g = a + b\sqrt{2}$ and $g' = c + d\sqrt{2}$, where $a, b, c, d \in \mathbb{Q}$. Here, $gg' = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$. Since $ac + 2bd \in \mathbb{Q}$ and $ad + bc \in \mathbb{Q}$, then $gg' \in G'$.
- Every element of G' has an inverse also in G'. Let $g = a + b\sqrt{2} \in G$, where $a, b \in \mathbb{Q}$. The multiplicative inverse of g is

$$g^{-1} = \frac{a}{a^2 - 2b^2} - \left(\frac{b}{a^2 - 2b^2}\right)\sqrt{2}. \tag{30}$$

  Here, the property $gg^{-1} = g^{-1}g = 1$ can be easily verified. The following will show that $g^{-1} \in G'$. We can note that if $a^2 - 2b^2 \neq 0$, then $a/(a^2 - 2b^2) \in \mathbb{Q}$ and $b/(a^2 - 2b^2) \in \mathbb{Q}$, and therefore $g^{-1} \in G'$. To show that it is always the case that $a^2 - 2b^2 \neq 0$, we can use the result from D&F Exercise 0.2.7 (which states that there are no integer solutions for x, y to the equation $x^2 - 2y^2 = 0$). In order to use this previous result, we will proceed by contradiction. Assume $a^2 - 2b^2 = 0$. Let the rational numbers a and b have a fractional representation $a = c/d$ and $b = e/f$, where $c, d, e, f \in \mathbb{Z}$ and $d, f \neq 0$. Multiplying both sides of the equation by $(df)^2$, we have $(adf)^2 - 2(bdf)^2 = 0$. Now let $x = adf$ and $y = bdf$, yielding $x^2 - 2y^2 = 0$, noting that $x, y \in \mathbb{Z}$. Since according to D&F Exercise 0.2.7 there are no integer solutions x, y to the equation $x^2 - 2y^2 = 0$, then $a^2 - 2b^2 \neq 0$. Therefore, $g^{-1} \in G'$.
- G' is associative under multiplication. This follows from the associativity of multiplication over $\mathbb{R}$.

D&F Exercise 1.1.11

Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

The order of an element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ under addition is the lowest value of $k \in \mathbb{Z}$ such that $ak \equiv 0 \pmod{n}$. A closed-form expression for the order of $\overline{a}$ is $n/(a, n)$. Another way to illustrate this is to add $\overline{a}$ to itself repeatedly until it yields a multiple of 12. The orders of each element of $\mathbb{Z}/12\mathbb{Z}$ are as follows:

$\overline{n}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\lvert\overline{n}\rvert$	1	12	6	4	3	12	2	12	3	4	6	12

(31)

D&F Exercise 1.1.12

Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{7}, \overline{-7}, \overline{13}$.

The order of an element of the multiplicative group $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ is the lowest value of $k \in \mathbb{Z}^+$ such that $\overline{a}^k \equiv 1 \pmod{n}$. When $n = 12$, the following elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ are found by brute force:

$\overline{n}$	$\overline{1}$	$\overline{-1}$	$\overline{5}$	$\overline{7}$	$\overline{-7}$	$\overline{13}$
$\lvert n\rvert$	1	2	2	2	2	1

(32)

D&F Exercise 1.1.16

Let x be an element of G. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

Let $x \in G$. If $|x| = 1$, then $x = 1$, and $x^2 = 1$. Otherwise, if $|x| = 2$, then $x^2 = 1$, by definition. Conversely, if $x^2 = 1$, then either x is the identity (in which case $|x| = 1$) or $|x| = 2$ (by definition).

D&F Exercise 1.1.17

Let x be an element of G. Prove that if $|x| = n$ for some positive integer n, then $x^{-1} = x^{n-1}$.

Let $x \in G$, where $|x| = n$ for $n \in \mathbb{Z}^+$. The inverse of x is x^{n-1}, i.e., $x^{-1} = x^{n-1}$. To show this, $xx^{n-1} = 1$ and $x^{n-1}x = 1$.

D&F Exercise 1.1.21

Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.

Let $x \in G$, where $x^n = 1$. If n is odd, then one can let $n = 2k - 1$, where $k \in \mathbb{Z}^+$. Then $x^n = x^{2k-1} = x^{2k}x^{-1} = 1$. Multiplying on the right by x, we have $x^{2k} = x$. Therefore, $x = (x^2)^k$, as desired.

D&F Exercise 1.1.22

If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Let $x, g \in G$, where $|x| = n$. We will now find the order of $g^{-1}xg \in G$ by evaluating $(g^{-1}xg)^n$:

$$(g^{-1}xg)^n = \underbrace{(g^{-1}xg)(g^{-1}xg)\cdots(g^{-1}xg)}_{n \text{ times}} \tag{33}$$

$$= g^{-1}x^ng \tag{34}$$

$$= g^{-1}g \tag{35}$$

$$= 1. \tag{36}$$

From this calculation, we can conclude that $(g^{-1}xg)^n = 1$. This implies $|g^{-1}xg| \leq n$. To prove that indeed $n = |g^{-1}xg|$, we will proceed by contradiction. Assume $|g^{-1}xg| = k$, where $1 \leq k < n$. Therefore $x^k = gg^{-1}x^kgg^{-1} = g(g^{-1}xg)^kg^{-1} = g(1)g^{-1} = 1$. But this implies $|x| \leq k$, which is impossible, since $k < n$ and $|x| = n$. Therefore, $k = n$, and $|g^{-1}xg| = n$.

We will now deduce that $|ab| = |ba|$ for all $a, b \in G$. Let a, b be arbitrary elements of G. Now let $x = ab$ and $g = a$. Then $|x| = |ab|$ and $|g^{-1}xg| = |ba|$. Since $|x| = |g^{-1}xg|$, then $|ab| = |ba|$.

D&F Exercise 1.1.25

Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

Let G be a group where all $x \in G$ satisfy $x^2 = 1$. We will show that G is abelian. To begin, let $x, y \in G$, where by definition of G, $x^2 = y^2 = 1$. Importantly, the element $xy \in G$ also satisfies $(xy)^2$=1, by definition of G. This means $x^{-1} = x$, $y^{-1} = y$, and $(xy)^{-1} = xy$. Therefore, $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Therefore, G is abelian.

D&F Exercise 1.1.31

Prove that any finite group G of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G | g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G - t(G)$ has order 2.]

Let G be a finite group of even order. We will show that G must contain at least one element of order 2. We begin by defining the set $t(G) = \{g \in G | g \neq g^{-1}\}$, i.e., the set of elements of G that are not their own inverses. We will begin by first proving three smaller results:

(i) $|G - t(G)|$ is even. To prove this, note that none of the elements of $t(G)$ is its own inverse, so this means the elements of $t(G)$ can be grouped into pairs, where the pairs are comprised of an element and its unique inverse. This means $|t(G)|$ is even. Since $|G|$ is also even, therefore $|G - t(G)|$ is even.

(ii) $G - t(G)$ contains the identity. To prove this, note that the identity element is its own inverse, so the identity is not contained in $t(G)$, but it must be contained in G, since G is a group. Therefore, $G - t(G)$ contains the identity.

(iii) The nonidentity elements of $G - t(G)$ have order 2. To prove this, note that $G - t(G)$ only contains elements that are their own inverses. Using the result from Exercise 1.1.16, such elements have orders either 1 or 2. Since only the identity element has order 1, then the nonidentity elements of $G - t(G)$ has order 2.

Combining (i) with (ii), we can conclude that $|G - t(G)| \geq 2$. But one of these elements of $G - t(G)$ must be the identity, according to (ii). So therefore there are a nonzero number of remaining nonidentity elements in $G - t(G)$, and, according to (iii), these elements must have order 2.

D&F Exercise 1.1.32

If x is an element of finite order n in G, prove that the elements $1, x, x^2, \cdots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

Let G be a finite group, and $x \in G$, where $|x| = n$. We will prove that $1, x, x^2, \cdots, x^{n-1}$ are all distinct. Suppose to the contrary that there exist elements x^ℓ and x^m which are not distinct, i.e., $x^\ell = x^m$, where $1 \leq \ell < m \leq n - 1$. Then we would have $x^n = x^\ell x^{n-\ell} = x^m x^{n-\ell} = x^n x^{m-\ell}$, which implies $x^{m-\ell} = 1$, and $|x| \leq m - \ell$. But $m - \ell < n$, which is a contradiction. Therefore, the elements $1, x, x^2, \cdots, x^{n-1}$ are all distinct.

Since $1, x, x^2, \cdots, x^{n-1}$ are all distinct, and there are n such elements, we can conclude that $n \leq |G|$. Since $|x| = n$, then $|x| \leq G$.

V. DIHEDRAL GROUPS

D&F Exercise 1.2.4

If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}.

Consider the group $D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$, where $n = 2k$ and $k \in \mathbb{Z}^+$, such that $k \geq 2$. Let $z = r^k$. This problem will be broken up in to the following results:

(a) z is an element of order 2. To show this, we can note that r has order n, which implies $r^n = r^{2k} = (r^k)^2 = 1$. Using the result from D&F Exercise 1.1.16, we can conclude that r^k has order 1 or 2. Now, if r^k has order 1, then $r^k = 1$ even though $k < n$. But this is impossible (cf D&F Exercise 1.1.32), since it would imply that $1 = r^0$ and r^k are not distinct. Therefore r^k has order 2.

(Note: $(r^k)^2 = 1$ if and only if $r^k = r^{-k}$.)

(b) z commutes with all elements of D_{2n}. To show this, note that elements of D_{2n} fall into two categories: (1) elements that can be represented as r^ℓ, where $\ell \in \mathbb{Z}$ and $0 \leq \ell \leq n-1$, and (2) elements that can be represented as $r^\ell s$, where $\ell \in \mathbb{Z}$ and $0 \leq \ell \leq n-1$. z commutes with elements in the first category, since $zr^\ell = r^k r^\ell = r^{k+\ell} = r^\ell r^k = r^\ell z$. z also commutes with elements in the second category, since $z(r^\ell s) = r^k r^\ell s = r^\ell r^k s = r^\ell s r^{-k} = r^\ell s r^k = (r^\ell s)z$. Therefore z commutes with all elements of D_{2n}.

(c) z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}. To show this, we will first need to prove the following result:

(i) Let x be a element of finite order n in G. If $n = 2a$ for $a \in \mathbb{Z}^+$, and $1 \leq i < n$, then $x^i = x^{-i}$ only if $i = a$ (cf D&F Exercise 1.1.33b). To show this, we can consider two cases:

(1) Let $i \neq a$. Because n is even, then $i \neq n - i$. Since $x^i \neq x^{n-i}$ and $x^{n-i} = x^{-i}$, therefore $x^i \neq x^{-i}$.

(2) Let $i = a$. We can follow the same line of reasoning in part (a) of this problem to conclude that x^i has order 2 when $i = a$. Therefore $(x^i)^2 = 1$, and $x^i = x^{-i}$.

Therefore, $x^i = x^{-i}$ *only* when $i = a$.

Continuing with the proof, consider that there is some element, call it z', which commutes with all elements of D_{2n}. We can represent z' as $s^m r^\ell$, where $m = 0$ or 1, and $\ell \in \mathbb{Z}$, where $0 \leq \ell \leq n-1$. We will now see what conditions are imposed on m and ℓ by requiring that z' commutes $s \in D_{2n}$. We will find it useful to consider the cases $m = 0$ and $m = 1$ separately. Assume $m = 0$, i.e., $z' = r^\ell$. Here, $z's = r^\ell s = sr^{-\ell}$. If z' is to commute with s, i.e., $z's = sz'$, then this requires $r^{-\ell} = r^\ell$. Using the result from (i) above, then it must be the case that $\ell = k$, i.e., $z' = z$. Now assume $m = 1$, i.e., $z' = sr^\ell$. Here, $z's = sr^\ell s = s(sr^{-\ell})$. Again, if z' is to commute with s, then this requires $r^{-\ell} = r^\ell$, which means $\ell = k$, and therefore $z' = z$. So, z is the only element of D_{2n} that commutes with s. Noting the result from (b), we can conclude z is the *only* element of D_{2n} that commutes with all elements of D_{2n}.

D&F Exercise 1.2.8

Find the order of the cyclic subgroup of D_{2n} generated by r.

The order of the cyclic subgroup of D_{2n} generated by r is n. To show this, note that the elements of this cyclic subgroup are r^k, where $k \in \mathbb{Z}$ and $0 \leq k \leq n-1$. So, r has order n. Finally, we can use the result from D&F Exercise 1.1.32 to conclude that r^k are distinct, so the order of the cyclic subgroup of D_{2n} generated by r is n.

D&F Exercises 1.2.9 - 1.2.13

In these problems, we are asked to find the order of the group G of rigid rotations in $\mathbb{R}^3$ of the five Platonic solids. The solutions will utilize the fact that the Platonic solids all have the symmetry that if an edge is rotated to the location of another edge, this leaves the shape invariant. Therefore, since each edge has two orientations, the number of such rigid rotations is twice the total number of edges.

- The tetrahedron has 6 edges, so $|G| = 12$.
- The cube has 12 edges, so $|G| = 24$.
- The octahedron has 12 edges, so $|G| = 24$.

- The dodecahedron has 30 edges, so $|G| = 60$.
- The icosahedron has 30 edges, so $|G| = 60$.

D&F Exercise 1.2.18

Let $Y = \langle u, v | u^4 = v^3 = 1, uv = v^2u^2 \rangle$.

(a) Show that $v^2 = v^{-1}$. [Use the relation $v^3 = 1$.]

(b) Show that v commutes with u^3. [Show that $v^2u^3v = v^3$ by writing the left hand side as $(v^2u^2)(uv)$ and using the relations to reduce this to the right hand side. Then use part (a).]

(c) Show that v commutes with u. [Show that $u^9 = u$ and then use part (b).]

(d) Show that $uv = 1$. [Use part (c) and the last relation.]

(e) Show that $u = 1$, deduce that $v = 1$, and conclude that $Y = 1$. [Use part (d) and the equation $v^4v^3 = 1$.]

(a) Starting with the relation $v^3 = 1$, we can multiply both sides by v^{-1}, so therefore $v^2 = v^{-1}$.

(b) We can deduce the following relation: $v^2u^3v = (v^2u^2)(uv) = (uv)(uv) = (uv)(v^2u^2) = uv^3u^2 = u^3$, i.e., $v^2u^3v = u^3$. Using (a), we have $v^{-1}u^3v = u^3$, so therefore $u^3v = vu^3$.

(c) Starting with $u^4 = 1$, we can multiply both sides by u^5, i.e., $u^9 = u^5 = (u^4)u = u$. Using this result and the one from part (b), we can deduce $uv = u^9v = u^3u^3u^3v = vu^9 = vu$, so v and u commute.

(d) Starting with the relation $uv = v^2u^2$, we can then use (c) to say say $vu = v^2u^2$, which implies $vu = uv = 1$.

(e) We can make the following relation given those we have already found: $1 = u^4v^3 = u^3(uv)v^2 = u^3v^2 = u^2(uv)v = u^2v = u(uv) = u$. Therefore $u = 1$, and since $uv = 1$, then $v = 1$. So, since u and v are both the identity, then the group Y is the trivial one, which contains only one element, i.e., the identity.

VI. SYMMETRIC GROUPS

D&F Exercise 1.3.1

Let σ be the permutation

$$1 \mapsto 3 \qquad 2 \mapsto 4 \qquad 3 \mapsto 5 \qquad 4 \mapsto 2 \qquad 5 \mapsto 1 \tag{37}$$

and let τ be the permutation

$$1 \mapsto 5 \qquad 2 \mapsto 3 \qquad 3 \mapsto 2 \qquad 4 \mapsto 4 \qquad 5 \mapsto 1 \tag{38}$$

Find the cycle decomposition of each of the following permutations: σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

(a) $\sigma = (135)(24)$

(b) $\tau = (15)(23)$

(c) $\sigma^2 = (135)(24)(135)(24) = (153)$

(d) $\sigma\tau = (135)(24)(15)(23) = (2534)$

(e) $\tau\sigma = (15)(23)(135)(24) = (1243)$

(f) $\tau^2\sigma = (15)(23)(15)(23)(135)(24) = (135)(24) = \sigma$.

D&F Exercise 1.3.3

For each of the permutations whose cycle decompositions were computed in [D&F Exercise 1.3.1] compute its order.

(a) $\sigma = (135)(24)$ has order 6, since it is the smallest power such that σ raised to that power is unity, i.e., $\sigma^6 = (\sigma^2)^3 = (153)(153)(153) = 1$.

(b) $\tau = (15)(23)$ has order 2, since is the smallest power such that τ raised to that power is unity, i.e., $\tau^2 = (15)(23)(15)(23) = 1$.

(c) $\sigma^2 = (153)$ has order 3, since is the smallest power such that σ^2 raised to that power is unity, i.e., $(\sigma^2)^3 = \sigma^6 = 1$.

(d) $\sigma\tau = (2534)$ has order 4, since is the smallest power such that $\sigma\tau$ raised to that power is unity, i.e., $(\sigma\tau)^4 = (2534)(2534)(2534)(2534) = 1$.

(e) $\tau\sigma = (1243)$ has order 4, since is the smallest power such that $\tau\sigma$ raised to that power is unity, i.e., $(\tau\sigma)^4 = (1243)(1243)(1243)(1243) = 1$.

(f) $\tau^2\sigma = (135)(24)$ has order 6, since $\tau^2\sigma = \sigma$.

D&F Exercise 1.3.4

Compute the order of each of the elements in the following groups: (a) S_3, (b) S_4.

(a) The group elements of S_3 and their orders can be found below:

$g \in S_3$	$\lvert g\rvert$
1	1
(12)	2
(13)	2
(23)	2
(123)	3
(132)	3

(39)

(b) The group elements of S_4 and their orders can be found below:

$g \in S_4$	$\lvert g \rvert$
1	1
(12)	2
(13)	2
(14)	2
(23)	2
(24)	2
(34)	2
(123)	3
(132)	3
(234)	3
(243)	3
(134)	3
(143)	3
(124)	3
(142)	3
(1234)	4
(1342)	4
(1432)	4
(1423)	4
(1324)	4
(1243)	4
(12)(34)	2
(13)(24)	2
(14)(23)	2

(40)

D&F Exercise 1.3.5

Find the order of (1 12 8 10 4)(2 13)(5 11 7)(6 9).

The order of a permutation is the least common multiple of the lengths of the cycles in its cycle decomposition (cf D&F Exercise 1.3.15). Since this permutation has cycles of lengths 5, 2, and 3, it therefore has order 30.

D&F Exercise 1.3.6

Write out the cycle decomposition of each element of order 4 in S_4.

See solution to D&F Exercise 1.3.4(b).

D&F Exercise 1.3.7

Write out the cycle decomposition of each element of order 2 in S_4.

See solution to D&F Exercise 1.3.4(b).

D&F Exercise 1.3.8

Prove that if $\Omega = \{1, 2, 3, \cdots\}$ then S_Ω is an infinite group (do not say $\infty! = \infty$).

Let $\Omega = \{1, 2, 3, \cdots\}$. We will prove that S_Ω has an infinite number of elements. To do this, consider a subset of elements $\sigma_n \in S_\Omega$ where σ_n are the 2-cycles $(n\ n+1)$. There is a one-to-one correspondence between the set of these 2-cycles $\Sigma = \{\sigma_1, \sigma_2, \sigma_3, \cdots\}$ and the positive integers $\{1, 2, 3, \cdots\}$. Since the set of positive integers is an infinite set, and Σ is a subset of S_Ω, then S_Ω has an infinite number of elements.

D&F Exercise 1.3.9

(a) Let σ be the 12-cycle (1 2 3 4 5 6 7 8 9 10 11 12). For which positive integers i is σ^i also a 12-cycle?

(b) Let τ be the 8-cycle (1 2 3 4 5 6 7 8). For which positive integers i is τ^i also an 8-cycle?

(c) Let ω be the 14-cycle (1 2 3 4 5 6 7 8 9 10 11 12 13 14). Which positive integers i is ω^i also a 14-cycle?

In the following, we will use the result from D&F Exercise 1.3.11, which states that given a m-cycle σ, that σ^i is also an m-cycle if and only if i is relatively prime to m.

(a) For the given 12-cycle σ, the positive integers i where σ^i is also a 12-cycle will be the integers i such that $(i, 12) = 1$.

(b) For the given 8-cycle τ, the positive integers i where τ^i is also a 8-cycle will be the integers i such that $(i, 8) = 1$.

(c) For the given 14-cycle ω, the positive integers i where ω^i is also a 14-cycle will be the integers i such that $(i, 14) = 1$.

D&F Exercise 1.3.11

Let σ be an m-cycle $(1\ 2 \cdots\ m)$. Show that σ^i is also an m-cycle if and only if i is relatively prime to m.

Let σ be an m-cycle and i be a positive integer. We will show that σ^i is also an m-cycle if and only if i is relatively prime to m.

Assume i and m are relatively prime, i.e., $(i, m) = 1$. We will show that σ^i is an m-cycle. Since σ is an m-cycle, $1 = \sigma^m = (\sigma^m)^i = (\sigma^i)^m$, which implies $|\sigma^i| \leq m$. Proceeding by contradiction, now assume that $|\sigma^i| = k$, where $1 \leq k < m$. Since now $(\sigma^i)^k = \sigma^{ik} = 1$, and $|\sigma| = m$, then $m|ik$. Because $(i, m) = 1$, this implies $m|k$ (cf D&F Exercise 0.2.7). However, since $k < m$, m cannot divide k, which is a contradiction. Therefore, $|\sigma^i| = m$, and σ^i is an m-cycle.

Conversely, assume σ^i is an m-cycle, so $|\sigma^i| = m$. We will show that i is relatively prime to m. To do this, let d be a common divisor of m and i, so m/d and i/d are both integers. We can note that $1 = \sigma^m = (\sigma^m)^{i/d} = (\sigma^i)^{m/d}$, which implies $|\sigma^i| \leq m/d$. But $|\sigma^i| = m$, so d can only equal 1. If the only common divisor between i and m is 1, then $(i, m) = 1$, and i is relatively prime to m.

D&F Exercise 1.3.15

Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.

Consider σ is a permutation of order m that has the cycle decomposition $\sigma = \sigma_1\sigma_2 \cdots \sigma_k$, where each σ_i are disjoint cycles of order m_i and $1 \leq i \leq k$. We will show that m is the least common multiple of

all m_i. To show this, we can note that because these cycles are disjoint, $\sigma^m = \sigma_1^m \sigma_2^m \cdots \sigma_k^m = 1$. So, for each cycle, $\sigma_i^m = 1$. This implies $m_i | m$, i.e., m is a common multiple of all m_i. Because $|\sigma| = m$, then m is the smallest integer such that $\sigma^m = 1$. Therefore, m is the least common multiple of all m_i.

D&F Exercise 1.3.16

Show that if $n \geq m$ then the number of m-cycles in S_n is given by

$$\frac{n(n-1)(n-2)\cdots(n-m+1)}{m}. \tag{41}$$

[Count the number of ways of forming an m-cycle and divide by the number of representations of a particular m-cycle.]

We will count the number of m cycles in S_n, where $m \leq n$. For a given m cycle, one has n choices where to place the first element, $n-1$ choices to place the second element, etc., until one reaches the final element, i.e., the m'th element, for which there is no choice. Thus, the number of such positions is $n(n-1)(n-2)\cdots(n-m+1)$. Furthermore, each m cycle has m different equivalent representations, so the total number of distinct m cycles is

$$\frac{n(n-1)(n-2)\cdots(n-m+1)}{m}. \tag{42}$$

VII. MATRIX GROUPS

D&F Exercise 1.4.1

Prove that $|GL_2(\mathbb{F}_2)| = 6$.

We will show that $|GL_2(\mathbb{F}_2)| = 6$. To do this, we can use the fact stated in D&F Sec. 1.4 that if F is a field, $n \in \mathbb{Z}^+$, and $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2)\cdots(q^n - q^{n-1})$. Here, $|\mathbb{F}_2| = 2$ and $n = 2$, so $|GL_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = 6$.

An alternative approach is to explicitly represent the elements of $|GL_2(\mathbb{F}_2)|$ and show there are six of them. Here, the elements of $|GL_2(\mathbb{F}_2)|$ have the following representation:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{43}$$

where $a, b, c, d \in \mathbb{F}_2$, and $ad - bc \neq 0$. The matrices that satisfy these constraints are

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{44}$$

Indeed, there are 6 such elements.

D&F Exercise 1.4.3

Show that $GL_2(\mathbb{F}_2)$ is non-abelian.

Using the results in D&F Exercise 1.4.1, we can verify that there exists two elements that do not

commute:

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \tag{45}$$

but

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \tag{46}$$

so $GL_2(\mathbb{F}_2)$ is non-abelian.

D&F Exercise 1.4.4

Let $n \in \mathbb{Z}^+$. Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Let $n \in \mathbb{Z}^+$. We will show that if n is not prime, then $\mathbb{Z}/n\mathbb{Z}$ is not a field. Specifically, we will show that $\mathbb{Z}/n\mathbb{Z}$ does not have a multiplicative inverse for all elements unless n is prime. Let $a \in \mathbb{Z}/n\mathbb{Z}$. The multiplicative inverse of a, call it c, must satisfy $ac \equiv 1 \pmod{n}$. However, we can use the result of D&F Exercise 0.3.12 to conclude that c only exists if $(a, n) = 1$. So, if all elements of $\mathbb{Z}/n\mathbb{Z}$ are to have multiplicative inverses, n must be relatively prime to all integers a in the range $0 \leq a < n$, i.e., n must be prime. Therefore, if n is not prime, then $\mathbb{Z}/n\mathbb{Z}$ cannot be a field.

D&F Exercise 1.4.5

Let F be a field and $n \in \mathbb{Z}^+$. Show that $GL_n(F)$ is a finite group if an only if F has a finite number of elements.

Let F be a field and $n \in \mathbb{Z}^+$. We will show that $GL_n(F)$ is a finite group if an only if F has a finite number of elements. First, if F is finite, then there can only be a finite number of matrices of size $n \times n$ that contain elements in F, so $GL_n(F)$ must be a finite group.

Conversely, we will show that if $GL_n(F)$ is a finite group, then $|F|$ is finite. To do this, we will prove the contrapositive: if $|F|$ is infinite, then $GL_n(F)$ is an infinite group. To begin, assume $|F|$ is infinite and consider the identity element of $GL_n(F)$, i.e., $\mathbb{1}$. Let $a \in F$, where $a \neq 0$. Then $a\mathbb{1} \in GL_n(F)$ because $a\mathbb{1}$ is invertible. Since there are an infinite number of such elements a, then there are an infinite number of such elements $a\mathbb{1} \in GL_n(F)$. Therefore, $GL_n(F)$ is an infinite group.

D&F Exercise 1.4.6

Let F be a field and let $n \in \mathbb{Z}^+$. If $|F| = q$ is finite prove that $|GL_n(F)| < q^{n^2}$.

Let F be a field and let $n \in \mathbb{Z}^+$. We will show that if $|F| = q$ is finite, then $|GL_n(F)| < q^{n^2}$. To do this, we can use the fact stated in D&F Sec. 1.4 that if F is a field, $n \in \mathbb{Z}^+$, and $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$. Since $q > 0$, we can note the inequality $(q^n - q^a) < q^n$, for $0 \leq a < n$. So,

$$|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) < (q^n)^n = q^{n^2}. \tag{47}$$

Therefore, $|GL_n(F)| < q^{n^2}$.

D&F Exercise 1.4.7

Let p be prime. Prove that the order of $GL_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$ (do not just quote the order formula in this section). [Subtract the number of 2×2 matrices which are not invertible from the total number of 2×2 matrices over $\mathbb{F}_p$. You may use the fact that a 2×2 matrix is not invertible if and only if one row is a multiple of the other.]

Let p be prime. We will prove that the order of $GL_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$. To do so, we will count the total number of 2×2 matrices with entries in $\mathbb{F}_p$, then subtract the number of such matrices that are not invertible. Specifically, we use the fact that a 2×2 matrix is not invertible if and only if one row is a multiple of the other. To begin, we can note that there are a total of p^4 2×2 matrices whose matrix elements are elements of $\mathbb{F}_p$. In order to found the number of non-invertible 2×2 matrices, we will consider the following cases:

- Matrices of the form:

$$\begin{pmatrix} a & b \\ ca & cb \end{pmatrix} \tag{48}$$

  where $a, b, c \in \mathbb{F}_p$ and $a, b, c \neq 0$. Since a, b and c can take on $p - 1$ values each, there are $(p-1)^3$ such matrices.

- Matrices of the form:

$$\begin{pmatrix} 0 & a \\ 0 & ca \end{pmatrix} \tag{49}$$

  where $a, c \in \mathbb{F}_p$ and $a, c \neq 0$. Since a and c can each take on $p - 1$ values, there are $(p-1)^2$ such matrices.

- Matrices of the form:

$$\begin{pmatrix} a & 0 \\ ca & 0 \end{pmatrix} \tag{50}$$

  where $a, c \in \mathbb{F}_p$ and $a, c \neq 0$. Since a and c can each take on $p - 1$ values, there are $(p-1)^2$ such matrices.

- Matrices of the form:

$$\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \tag{51}$$

  where $a, b \in \mathbb{F}_p$. Since a and b can each take on p values, there are p^2 such matrices.

- Matrices of the form:

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \tag{52}$$

  where $a, b \in \mathbb{F}_p$. Since a and b can each take on p values, there are p^2 such matrices.

All of these matrix categories are disjoint, with one exception: the last two categories both contain the matrix of all zeros. So, when subtracting the number of non-invertible matrices in the above categories,

one will have to add back in the matrix with all zero entries, since it is counted twice. The total number of elements of $GL_n(\mathbb{F}_p)$ is:

$$p^4 - (p-1)^3 - 2(p-1)^2 - 2p^2 + 1 = p^4 - p^3 - p^2 + p, \tag{53}$$

as desired.

D&F Exercise 1.4.11

The Heisenberg group over a field F is defined as

$$H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in F \right\}, \tag{54}$$

and let X and Y be elements of $H(F)$, where

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \qquad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}. \tag{55}$$

(a) Compute the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).

(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.

(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative.)

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

(e) Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

(a) The matrix product XY is

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \tag{56}$$

Here, $H(F)$ is closed under matrix multiplication since $a + c \in F$, $e + af + b \in F$, and $f + c \in F$. Finally, $H(F)$ is always non-abelian, since for any field F,

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \in H(F), \tag{57}$$

and yet

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq 0. \tag{58}$$

(b) An explicit formula for X^{-1} is

$$X^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \tag{59}$$

It is straightforward to verify that $X^{-1}X = \mathbb{1}$. Since $-a, ac-b, -c \in F$, then $H(F)$ is closed under inverses.

(c) I'm skipping the solution that shows $H(F)$ is associative, since it's a bit laborious. However, it is straightforward to prove that $|H(F)| = |F|^3$. To show this, we can note that there are three matrix elements in each element of $H(F)$ that can each take on $|F|$ values. If $|F|$ is finite, then there are $|F|^3$ such matrices, and $|H(F)| = |F|^3$.

(d) There are 8 elements of $|H(\mathbb{F}_2)|$. To save space, define

$$H(a,b,c) := \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \tag{60}$$

Then

$g \in H(F)$	$\lvert g\rvert$
$H(0,0,0)$	1
$H(1,0,0)$	2
$H(0,1,0)$	2
$H(0,0,1)$	2
$H(1,1,0)$	2
$H(1,0,1)$	4
$H(0,1,1)$	2
$H(1,1,1)$	4

(61)

(e) We will prove that any nonidentity element of the group $H(\mathbb{R})$ has infinite order. To begin, let $a, b, c \in \mathbb{R} - \{0\}$ and

$$g = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in H(\mathbb{R}). \tag{62}$$

We then claim the following for $n \in \mathbb{Z}^+$:

$$g^n = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb + n(n-1)ac/2 \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} \in H(\mathbb{R}). \tag{63}$$

Given this, we can conclude $g^n \neq \mathbb{1}$ for all $n \in \mathbb{Z}^+$, and therefore, all non-identity elements of $H(\mathbb{R})$ have infinite order. All that is remains is to prove Eq. (63). To do so, we will proceed by induction.

The base case is when $n = 1$, and

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & b + (1-1)ac/2 \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}, \tag{64}$$

as desired. Let $k \in \mathbb{Z}^+$, and assume that

$$g^k = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & ka & kb + k(k-1)ac/2 \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}. \tag{65}$$

We aim to prove that the result holds for $k + 1$. That is, we wish to show that

$$g^{k+1} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{k+1} = \begin{pmatrix} 1 & (k+1)a & (k+1)b + (k+1)kac/2 \\ 0 & 1 & (k+1)c \\ 0 & 0 & 1 \end{pmatrix}. \tag{66}$$

To do this, we begin with the expression on the left, and we apply the induction hypothesis to the matrix multiplication, and after multiplying the matrices we get the result on the right:

$$g^{k+1} = g^k g = \begin{pmatrix} 1 & ka & kb + k(k-1)ac/2 \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (k+1)a & (k+1)b + (k+1)kac/2 \\ 0 & 1 & (k+1)c \\ 0 & 0 & 1 \end{pmatrix} \tag{67}$$

as desired. Therefore, by induction,

$$g^n = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb + n(n-1)ac/2 \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}. \tag{68}$$

VIII. SUBGROUPS: DEFINITION AND EXAMPLES

D&F Exercise 2.1.2

In each (a) - (e) prove that the specified subset is not a subgroup of the given group:

(a) the set of 2-cycles in S_n for $n \geq 3$

(b) the set of reflections in D_{2n} for $n \geq 3$

(c) for n a composite integer > 1 and G a group containing an element of order n, the set $\{x \in G \big| |x| = n\} \cup \{1\}$

(d) the set of (positive and negative) odd integers in $\mathbb{Z}$ together with 0

(e) the set of real numbers whose square is a rational number (under addition).

(a) The set of 2-cycles in S_n for $n \geq 3$ is not a subgroup of S_n. This is because this set does not contain the identity of S_n, since the identity is a 1-cycle, not a 2-cycle.

(b) The set of reflections in D_{2n} for $n \geq 3$ is not a subgroup of D_{2n}. This is because this set does not contain the identity of D_{2n}, since the identity is not a reflection.

(c) For a group G and composite integer $n > 1$, the set $\{x \in G \big| |x| = n\} \cup \{1\}$ is not a subgroup of G. This is because the set is not closed under multiplication. For example, consider the element x of the set in question, where $|x| = n$, and n is composite such that $n = ab$, where $a, b \in \mathbb{Z}^+$ and $1 < a \leq b < n$. Multiplying x by itself a times, we obtain the element x^a. Note that $x^a \neq 1$, since $a < n$. Now, $(x^a)^b = x^{ab} = x^n = 1$, so $|x^a| \leq b$. However, $b < n$, so $|x^a| < n$, which means x^a is not a part of the set $\{x \in G \big| |x| = n\} \cup \{1\}$, and therefore this set is not closed under multiplication.

(d) The set of odd integers together with 0 is not a subgroup of $(\mathbb{Z}, +)$. This is because the set is not closed under addition. To show this, consider the odd integer 1. Adding 1 to itself yields $1+1 = 2$, which is not an odd integer, therefore the set is not closed under addition.

(e) The set of real numbers whose square is a rational number (under addition) is not a group. This is because the set is not closed under addition. To show this, consider two elements x and y of this set: $x = \sqrt{2}$ and $y = 1$. Adding these elements yields $x + y = \sqrt{2} + 1$. However, the square of $x + y$ is not a rational number, i.e., $(x + y)^2 = x^2 + y^2 + 2xy = 3 + 2\sqrt{2}$, so this set is not closed under addition.

D&F Exercise 2.1.3

Show that the following subsets of the dihedral group D_8 are actually subgroups: (a) $\{1, r^2s, sr^2\}$, (b) $\{1, r^2, sr, sr^3\}$.

(a) We can use the Subgroup Criterion to verify that the subset $H = \{1, r^2s, sr^2\}$, where $|r| = 4$, is a subgroup of D_8:

$x \in H$	$y \in H$	xy^{-1}	yx^{-1}
r^2s	r^2s	1	1
r^2s	sr^2	1	1
sr^2	sr^2	1	1

(69)

where trivial multiplications with the identity were removed for brevity. Since all elements in the xy^{-1} and yx^{-1} columns are all elements of H, therefore H is a subgroup of D_8.

(b) We can use the Subgroup Criterion to verify that the subset $H = \{1, r^2, sr, sr^3\}$ is a subgroup of D_8:

$x \in H$	$y \in H$	xy^{-1}	yx^{-1}
r^2	r^2	1	1
r^2	sr	sr^3	sr^3
r^2	sr^3	sr	sr
sr	sr	1	1
sr	sr^3	r^2	r^2
sr^3	sr^3	1	1

(70)

where trivial multiplications with the identity were removed for brevity. Since all element sin the xy^{-1} and yx^{-1} columns are all elements of H, therefore H is a subgroup of D_8.

D&F Exercise 2.1.4

Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G.

Let $G = (\mathbb{R}, \times)$ and consider the set $H = \mathbb{Z} - \{0\}$ under multiplication. Here, H is a subset of G, and H is closed under multiplication. However, H is not closed under inverses. For example, consider the element $x = 2$ in H. Since there is no element $y \in H$ where $xy = 1$, then the set is not closed under inverses, and it is not a subgroup of G.

D&F Exercise 2.1.5

Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Let G be a group where $|G| > 2$, and let H be a subset of G, where $|H| = n - 1$. We will show that H cannot be a subgroup of G. We will proceed by contradiction. Assume that H is a subgroup of G. Because $|G| = n$ and $|H| = n - 1$, let $x \in G$ be the single element not contained in H. Let h be any non-identity element in H. Such an element h is guaranteed to exist, since $n > 2$.

We will now show that $xh \notin H$ by way of contradiction. Assume $xh \in H$. If xh were in H, then $(xh)h^{-1} \in H$, since both xh and h^{-1} would be in H. However, $(xh)h^{-1} = x \notin H$, which is a contradiction. Therefore, $xh \notin H$.

However, if $xh \notin H$, then there is only one such element left in G: x itself. So then $xh = x$, which implies h can *only* be the identity element. But we assumed h is a nonidentity element of H, So this is a contradiction. Therefore, H is not a subgroup of G.

D&F Exercise 2.1.6

Let G be an abelian group. Prove that $\{g \in G \big| |g| < \infty\}$ is a subgroup of G (called the torsion subgroup of G). Given an explicit example where this set is not a subgroup when G is non-abelian.

Let G be an abelian group. We will prove that a set $H = \{g \in G \big| |g| < \infty\}$ is a subgroup of G. To do this, we will consider different cases:

- H contains only the identity of G. Here, H is a trivial subgroup of G.
- $|H| \geq 2$. Let $x, y \in H$, where $|x| = n$ and $|y| = m$ are finite. This implies $x^n = 1$ and $y^{-m} = 1$. Because G is abelian, we can note the following relation: $1 = (x^n)^m(y^{-m})^n = (xy^{-1})^{nm}$, which implies $|xy^{-1}| \leq nm < \infty$, so $xy^{-1} \in H$. Since x and y were arbitrary, then H is a subgroup of G according to the Subgroup Criterion.

D&F Exercise 2.1.7

Fix some $n \in \mathbb{Z}$ with $n > 1$. Find the torsion subgroup (cf. the previous exercise) of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. Show that the set of elements of infinite order together with the identity is not a subgroup of this direct product.

Let $n \in \mathbb{Z}$ with $n > 1$. We will show the following results:

(a) The torsion subgroup of $G = \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ under addition is $H = \{(0, g) \big| g \in \mathbb{Z}/n\mathbb{Z}\}$. To show this, we can note that all nonzero integers have infinite order, so any element of G with finite order must have the form form $(0, ...)$. Furthermore, all elements of $\mathbb{Z}/n\mathbb{Z}$ have finite order, so let $H = \{(0, g) \big| g \in \mathbb{Z}/n\mathbb{Z}\}$. We know H is a subgroup, due to the result in D&F Exercise 2.1.6. Therefore, H is the torsion subgroup of G.

(b) Let H be the set of elements of infinite order together with the identity is not a subgroup of G. Here, H is not a subgroup of G, since it is not closed under addition. To show this, we can note that $g_1 = (1, 1) \in H$ and $g_2 = (-1, 0) \in H$. However, $g_1 + g_2 = (0, 1)$, which is of finite order, so it is not an element of H. Therefore, H is not a subgroup of G.

D&F Exercise 2.1.8

Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Let H and K be subgroups of G. We will prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

To do this, first assume that $H \cup K$ is a subgroup of G. Consider the following cases:

- If $H \subseteq K$, then we are done.
- If $K \subseteq H$, then we are done.
- If $K \not\subseteq H$ and $H \not\subseteq K$, then this is inconsistent with $H \cup K$ being a subgroup of G. To see why, we will proceed by contradiction. Assume $K \not\subseteq H$ and $H \not\subseteq K$, so there are elements $x \in K$ and $y \in H$, but $x \notin H$ and $y \notin K$. Now, the product $xy \in H \cup K$, so $xy \in H$ or $xy \in K$. We will now consider these two cases:

  (i) Assume $xy \in H$. Then the product $(xy)y^{-1}$ must be in H, since $xy \in H$ and $y^{-1} \in H$. However, $(xy)y^{-1} = x$, and x was assumed to not to be in H, which is a contradiction. Therefore $xy \notin H$.

  (ii) Assume $xy \in K$. Then the product $x^{-1}(xy)$ must be in K, since $xy \in K$ and $x^{-1} \in K$. However, $x^{-1}(xy) = y$, and y was assumed to not to be in K, which is a contradiction. Therefore $xy \notin K$.

  From this, $xy \notin K$ and $xy \notin H$, which is a contradiction. So, there are no elements $x \in K$ and $y \in H$ such that $x \notin H$ and $y \notin K$. Therefore, the case when $K \not\subseteq H$ and $H \not\subseteq K$ is inconsistent with $H \cup K$ being a subgroup of G.

Therefore, if $H \cup K$ is a subgroup of G, then either $H \subseteq K$ or $K \subseteq H$.

Conversely, assume that either $H \subseteq K$ or $K \subseteq H$. If so, then either $H \cup K = K$ or $K \cup H = H$, and since K and H are both subgroups, then $H \cup K$ is also a subgroup.

D&F Exercise 2.1.12

Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:

(a) $\{a^n | a \in A\}$

(b) $\{a \in A | a^n = 1\}$.

Let A be an abelian group, and fix some $n \in \mathbb{Z}$. We will prove that the following sets are subgroups of A:

(a) Let $H = \{a^n | a \in A\}$. To show that H is a subgroup of A, we can first note that the identity of A, i.e., $1 \in A$, is contained in H, since $1 = 1^n \in H$. Next, let $x, y \in H$. This means $x = a^n$ and $y = b^n$ for some $a, b \in A$. Now, consider the element xy^{-1}. Here, $xy^{-1} = a^n(b^n)^{-1} = a^n(b^{-1})^n = (ab^{-1})^n$. The last equality is due to the fact that A is abelian. Because $(ab^{-1})^n$ is an n'th power, then $(ab^{-1})^n \in H$, so therefore $(ab^{-1})^n = xy^{-1} \in H$. According to the Subgroup Criterion, H is a subgroup of A.

(b) Let $H = \{a \in A | a^n = 1\}$. To show that H is a subgroup of A, we can first note that the identity of A, i.e., $1 \in A$, is contained in H, since $1 = 1^n \in H$. Now, let $a, b \in H$. This means $a^n = b^n = 1$. Now, consider the element $ab^{-1} \in A$. By raising this element to the power n, we have $(ab^{-1})^n = a^n(b^n)^{-1} = 1$, because A is abelian. But since $(ab^{-1})^n = 1$, then $ab^{-1} \in H$, by definition, and according to the Subgroup Criterion, H is a subgroup of A.

D&F Exercise 2.1.13

Let H be a subgroup of the additive group of rational numbers with the property that $1/x \in H$ for every nonzero element x of H. Prove that $H = 0$ or $\mathbb{Q}$.

Let H be a subgroup of the additive rational numbers with the property that $1/x \in H$ for every nonzero element x of H. Here, $H \subseteq \mathbb{Q}$, by definition. We will prove that $H = 0$ or $\mathbb{Q}$.

First, if H only contains 0, i.e., the identity of G, then H is the trivial subgroup of G, and we are done.

Next, assume that H does not only contain the identity. We will prove that $\mathbb{Q} \subseteq H$. To do this, we will use the following result:

(i) Let x be an element of H and n be an integer. Then $nx \in H$. If x is the identity element, then this result is trivial, since $n \cdot 0 = 0 \in H$ for any $n \in \mathbb{Z}$. If $n = 0$, then the result is also trivial, since $0 \cdot x = 0 \in H$ for any $x \in H$. If x is a nonidentity element of H and n is nonzero, then we can consider the following two cases:

- $n > 0$. Here, we can add the element x to itself n times, yielding the element nx. Since H is closed under addition, then $nx \in H$.
- $n < 0$. Here, we can subtract the element x to itself $|n|$ times, yielding the element $-|n|x$. Since H is closed under inverses, then $-|n|x = nx \in H$.

Therefore, $nx \in H$.

First we will show that $1 \in H$. To do this, let $x \in H$. Because H contains only rational numbers, then $x = a/b$, where $a, b \in \mathbb{Z}$, where $a \neq 0$ and $b \neq 0$. According to (i), then $bx = b(a/b) = a \in H$. By the definition of H, then $1/a \in H$. Using (i) again, $a(1/a) = 1 \in H$.

Next, we will show that any nonzero rational number q is contained in H. Here, $q = c/d$, where $c, d \in \mathbb{Z}$ and $c \neq 0$ and $d \neq 0$. Since $1 \in H$, we can use (i) to conclude that $d \cdot 1 = d \in H$. Then $1/d \in H$, by definition. Using (i) again, $c(1/d) = c/d = q \in H$. So, for all nonzero $q \in \mathbb{Q}$, then $q \in H$. Since H also contains 0, therefore $\mathbb{Q} \subseteq H$.

We have shown $\mathbb{Q} \subseteq H$, and since $H \subseteq \mathbb{Q}$ by definition, then $H = \mathbb{Q}$.

D&F Exercise 2.1.14

Show that $\{x \in D_{2n} | x^2 = 1\}$ is not a subgroup of D_{2n} (here $n \geq 3$).

Let $n \geq 3$. We will show that $H = \{x \in D_{2n} | x^2 = 1\}$ is not a subgroup of D_{2n}. To begin, we will consider two elements of D_{2n}: s and sr^{n-1}. Both of these elements square to unity, i.e., $s^2 = 1$ and $(sr^{n-1})^2 = (sr^{n-1})(sr^{n-1}) = sr^{n-1}r^{-(n-1)}s = s^2 = 1$, so both elements are members of H. However, their product $(s)(sr^{n-1}) = r^{n-1}$ is not in H since its does not square to unity, i.e., $(r^{n-1})^2 = r^{2(n-1)} = r^{2n}r^{-2} = r^{-2} = r^n r^{-2} = r^{n-2} \neq 1$. Therefore, H is not closed under multiplication, and H cannot be a subgroup of D_{2n}.

IX. HOMOMORPHISMS AND ISOMORPHISMS

D&F Exercise 1.6.1

Let G and H be groups, and let $\varphi : G \to H$ be a homomorphism.

(a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.

(b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

Let G and H be groups, and let $\varphi : G \to H$ be a homomorphism.

(a) We will use induction to prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$. The base case is when $n = 1$, so $\varphi(x) = \varphi(x)$, as desired. Next, let $k \in \mathbb{Z}^+$, and assume that $\varphi(x^k) = \varphi(x)^k$. We aim to prove that the result holds for $k + 1$. That is, we wish to show that $\varphi(x^{k+1}) = \varphi(x)^{k+1}$. To do this, we begin with the induction hypothesis, $\varphi(x^k) = \varphi(x)^k$, and multiply by $\varphi(x)$ on both sides on the right, yielding $\varphi(x^k)\varphi(x) = \varphi(x)^{k+1}$. The left hand side of this equation can be further simplified using the fact that φ is a homomorphism, so $\varphi(x^k)\varphi(x) = \varphi(x^{k+1})$. Using this, then we have the relation $\varphi(x^{k+1}) = \varphi(x)^{k+1}$, as desired. Therefore, by induction, $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.

(b) We will prove that when $n = -1$, then $\varphi(x^{-1}) = \varphi(x)^{-1}$, and from this deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$. To begin, we will denote the identities for groups G and H as 1_G and 1_H, respectively. Because φ is a homomorphism, $\varphi(1_G)\varphi(1_G) = \varphi(1_G)$, which implies $\varphi(1_G) = 1_H$. Letting $x \in G$, we then have $1_H = \varphi(1_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x)$, so we can conclude that $\varphi(x^{-1}) = \varphi(x)^{-1}$, as desired. From here, we can raise both sides of the equation to the power $n \in \mathbb{Z}^+$, i.e., $\varphi(x^{-1})^n = \varphi(x)^{-n}$, and use the result from part (a) to conclude $\varphi(x^{-n}) = \varphi(x)^{-n}$. Therefore, $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

D&F Exercise 1.6.2

If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?

Let $\varphi : G \to H$ be an isomorphism. We will show the following three results:

(a) $|\varphi(x)| = |x|$ for all $x \in G$. To show this, we need to first prove the following two results:

(i) Let $\phi : G \to H$ be a homomorphism. Let 1_G be the identity of G and 1_H be the identity of H. We will show that $\phi(1_G) = 1_H$. To do this, note $\phi(1_G) = \phi(1_G 1_G) = \phi(1_G)\phi(1_G)$, which implies $\phi(1_G) = 1_H$.

(ii) Let $\phi : G \to H$ be an isomorphism, $x \in G$, and let 1_G and 1_H denote the identity elements of G and H, respectively. Then $\phi(x) = 1_H$ if and only if $x = 1_G$. To show this, assume $x = 1_G$. Then by (i), $\phi(x) = 1_H$. Conversely, if $\phi(x) = 1_H$, then we can immediately conclude that $x = 1_G$, because φ is a bijection, so there is only one element in G that gets mapped to 1_H, and we already showed that it was 1_G.

Let $x \in G$, $|x| = n$, and let 1_G and 1_H denote the identity elements of G and H, respectively. Using the result from D&F Exercise 1.6.1, then we can claim $\varphi(x^n) = \varphi(x)^n$. Since $x^n = 1_G$, and using the line of reasoning in (i), $\varphi(x^n) = \varphi(1_G) = 1_H$. So, $1_H = \varphi(x)^n$, and from this we can say $|\varphi(x)| \leq n$. We will now show that indeed $|\varphi(x)| = n$ by way of contradiction. Suppose $|\varphi(x)| = k$, where $1 \leq k < n$. So, $\varphi(x)^k = 1_H$, and because $\varphi(x)^k = \varphi(x^k)$, then $\varphi(x^k) = 1_H$. Using the result from (i), we can conclude that $x^k = 1_G$, but this is a contradiction, since $k < n$ and n is the smallest integer such that $x^n = 1_G$. Therefore, $|\varphi(x)| = n$, and $|\varphi(x)| = |x|$.

(b) Any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. This follows from (a), since there is a bijective mapping between the elements of G and the elements of H.

(c) The result in (b) does not hold if φ is only assumed to be a homomorphism. To show this, consider the trivial map $\varphi : G \to H$, where $\phi(G) = 1_H$. Here, for $x, y \in G$, we have $\varphi(x) = 1_H$, $\varphi(y) = 1_H$, and $\varphi(xy) = 1_H$, so $\varphi(xy) = \varphi(x)\varphi(y)$, which implies φ is indeed a homomorphism. However, φ is not an isomorphism, because φ is not a bijection between the elements of G and H. So, given that φ is a homomorphism but not an isomorphism, we can now see why (b) does not hold, since $|\varphi(x)| = 1$ for all $x \in G$, despite the possibility that x has order greater than one.

D&F Exercise 1.6.3

If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?

We will show the following two results:

(a) Let $\varphi : G \to H$ be an isomorphism. Then G is abelian if and only if H is abelian. To show this, first assume G is abelian. Let $a, b \in H$. Since φ is a bijection, then there are unique elements $x, y \in G$ such that $a = \varphi(x)$ and $b = \varphi(y)$. Because φ is a homomorphism and G is abelian, we have $ab = \varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x) = ba$. Therefore, H is abelian.

Conversely, assume H is abelian. Here, let $x, y \in G$. Then we can evaluate $\varphi(xy) = \varphi(x)\varphi(y) = \varphi(y)\varphi(x) = \varphi(yx)$. Since φ is injective, the fact that $\varphi(xy) = \varphi(yx)$ implies $xy = yx$, so G is abelian.

We conclude that G is abelian if and only if H is abelian.

(b) Let $\varphi : G \to H$ be a homomorphism where G is abelian. Only the additional requirement that φ is surjective is sufficient to conclude that H is also abelian. To show this, let $a, b \in H$. Then, since φ is surjective, the preimages $\varphi^{-1}(a)$ and $\varphi^{-1}(b)$ are non-empty sets. So, let $x \in \varphi^{-1}(a)$ and $y \in \varphi^{-1}(b)$. Since G is abelian, $xy = yx$. This implies $\varphi(xy) = \varphi(yx)$, and since φ is a homomorphism, then $\varphi(xy) = \varphi(x)\varphi(y)$ and $\varphi(yx) = \varphi(y)\varphi(x)$, so therefore $\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$. Since $\varphi(x) = a$ and $\varphi(y) = b$, this means $ab = ba$. Therefore H is abelian.

D&F Exercise 1.6.6

Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

We will prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic. To show this, we will proceed by way of contradiction. Assume $\varphi : \mathbb{Q} \to \mathbb{Z}$ is an isomorphism. We will note the following result:

(i) $\varphi(1) = 0$. To show this, let $\varphi(1) = n$, where $n \in \mathbb{Z}$. However, because φ is a homomorphism, we have $n = \varphi(1) = \varphi(\frac{1}{2} + \frac{1}{2}) = \varphi(\frac{1}{2}) + \varphi(\frac{1}{2})$, so $n = 2\varphi(\frac{1}{2})$, which implies $2|n$. Again, $n = \varphi(1) = \varphi(\frac{1}{3} + \frac{1}{3} + \frac{1}{3}) = \varphi(\frac{1}{3}) + \varphi(\frac{1}{3}) + \varphi(\frac{1}{3})$, so $n = 3\varphi(\frac{1}{3})$, which implies $3|n$. This process can be repeated in order to conclude that all positive integers divide n. The only integer for which is this true is $n = 0$. This is true since if $|n| > 1$, there is always an integer larger in magnitude than n that does not divide n. So, only $n = 0$ satisfies $k|n$, where $k \in \mathbb{Z}$.

Therefore, $\varphi(1) = 0$.

Using (i), we have $\varphi(1) = 0$. But using the line of reasoning in the solution to D&F Exercise 1.6.2, we also have $\varphi(0) = 0$. But then φ is not injective, so φ is not bijective, and φ cannot be a isomorphism, which is a contraction. Therefore, the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

D&F Exercise 1.6.7

Prove that D_8 and Q_8 are not isomorphic.

The groups D_8 and Q_8 are not isomorphic. To show this, we note the results from D&F Exercise 1.6.2(b), which claims that if two groups are isomorphic, they have the same number of elements with the same order. Here, Q_8 only has one element of order 2, i.e., -1. But D_8 has multiple elements of order 2, e.g., r^2 and s are two examples. Since there are not the same number of elements with the same order, D_8 and Q_8 are not isomorphic.

D&F Exercise 1.6.9

Prove that D_{24} and S_4 are not isomorphic.

The groups D_{24} and S_4 are not isomorphic. To show this, we note the results from D&F Exercise 1.6.2(b), which claims that if two groups are isomorphic, they have the same number of elements with the same order. Here, D_{24} has an element that is order 12, i.e., r. But there are no elements in S_4 that have order 12 (see D&F Exercise 1.3.4(b)). Since there are not the same number of elements with the same order, D_{24} and S_4 are not isomorphic.

D&F Exercise 1.6.11

Let A and B be groups. Prove that $A \times B \cong B \times A$.

Let A and B be groups. We will prove that $A \times B \cong B \times A$. We do this by proving that the map $\varphi : A \times B \to B \times A$ where $\varphi(a, b) = (b, a)$ is an isomorphism for $a \in A$ and $b \in B$. First, we will show that φ is a homomorphism. Let $a, c \in A$ and $b, d \in B$. We can note that combination rule $(a, b)(c, d) = (ac, bd)$, so $\varphi((a, b)(c, d)) = \varphi(ac, bd) = (bd, ac) = (b, a)(d, c) = \varphi(a, b)\varphi(c, d)$, so φ is indeed a homomorphism. Second, we will show that φ is a bijection. Here, φ is surjective, since for any element $(b, a) \in B \times A$, there is a corresponding element in $A \times B$, namely (a, b), such that $\varphi(a, b) = (b, a)$. Also, φ is injective, since if $\varphi(a, c) = \varphi(b, d)$, this implies $(a, c) = (b, d)$. Since φ is both injective and surjective, then it is bijective. Therefore, since φ is a homomorphism and bijective, then it is an isomorphism, i.e., $A \times B \cong B \times A$.

D&F Exercise 1.6.13

Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the image of φ, $\varphi(G)$, is a subgroup of H. Prove that if φ is injective then $G \cong \varphi(G)$.

Let G and H be groups and let $\varphi : G \to H$ be a homomorphism and $\varphi(G)$ be the image of φ. We will show the following two results:

(a) The image of φ is a subgroup of H. To begin, we can note that $\varphi(G)$ contains the identity of H, since φ is a homomorphism and it maps the identity of G to the identity of H (cf D&F Exercise 1.6.1).

Next, let $x, y \in \varphi(G)$. We will show $xy^{-1} \in \varphi(G)$. Since φ is surjective, let $a \in \varphi^{-1}(x)$ and $b \in \varphi^{-1}(y)$. Now, since $a, b \in G$, then $ab^{-1} \in G$, and therefore $\varphi(ab^{-1}) \in \varphi(G)$. Since φ is

a homomorphism, $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = xy^{-1}$. Since $\varphi(ab^{-1}) \in \varphi(G)$, then $xy^{-1} \in \varphi(G)$.

Therefore, according to the Subgroup Criterion, $\varphi(G)$ is a subgroup of H.

(b) If φ is injective then $G \cong \varphi(G)$. To show this, define the restricted homomorphism $f : G \to \varphi(G)$. Here, f is surjective, by definition. But if φ is injective, then so is f. Therefore, f is both a bijection and a homomorphism, so there is an isomorphism between G and $\varphi(G)$, i.e., $G \cong \varphi(G)$.

D&F Exercise 1.6.14

Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Define the kernel of φ to be $\{g \in G | \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H, i.e., is the fiber over the identity of H). Prove that the kernel of φ is a subgroup of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.

Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. We will show the following results:

(a) The kernel of φ is a subgroup of G. Let $x, y \in \ker\varphi$, i.e., $\varphi(x) = \varphi(y) = 1_H$. We will show that xy^{-1} is also in the kernel of φ, so we can conclude that $\ker\varphi$ is a subgroup of G by using the Subgroup Criterion.

First, we can note that because $1_H = \varphi(y)\varphi(y)^{-1} = \varphi(y)\varphi(y^{-1})$, and since $\varphi(y) = 1_H$, then $\varphi(y^{-1}) = 1_H$. So, $y^{-1} \in \ker\varphi$. We can use this result to also note that because φ is a homomorphism $1_H = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1})$, and therefore $xy^{-1} \in \ker\varphi$. Since x and y were arbitrary, then according to the Subgroup Criterion, $\ker\varphi$ is a subgroup of G.

(b) The map φ is injective if and only if the kernel of φ is the identity subgroup of G.

To show this, first assume φ is injective. We will show that $\ker\varphi = 1_G$. Because φ is injective, there can be at most one element of G that gets mapped on to 1_H, and we have shown in D&F Exercise 1.6.1 that if φ is a homomorphism, that such an element must exist, namely 1_G. Therefore, $\ker\varphi = 1_G$.

Conversely, assume $\ker\varphi = 1_G$, and let $x, y \in G$. We will show that if $\varphi(x) = \varphi(y)$, then $x = y$, i.e., φ is injective. To begin, assume $\varphi(x) = \varphi(y) = h$. Then we have $1_H = hh^{-1} = \varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1})$. So, we have deduced $1_H = \varphi(xy^{-1})$. Because $\ker\varphi = 1_G$, then $xy^{-1} = 1_G$, which implies $x = y$. So, if $\varphi(x) = \varphi(y)$, then this implies $x = y$ for all $x, y \in G$, and therefore φ is injective.

D&F Exercise 1.6.17

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Let G be any group and $\varphi : G \to G$ where $\varphi(g) = g^{-1}$ for $g \in G$. We will show that φ is a homomorphism if and only if G is abelian.

First, assume φ is a homomorphism. We will show that G is abelian. Let $x, y \in G$. Because φ is a homomorphism, $\varphi(x)\varphi(y) = \varphi(xy)$, which implies $x^{-1}y^{-1} = (xy)^{-1}$. But $(xy)^{-1} = y^{-1}x^{-1}$, so $x^{-1}y^{-1} = y^{-1}x^{-1}$, i.e., $xy = yx$. Therefore G is abelian.

Conversely, assume G is abelian. We will show that φ is a homomorphism. Let $x, y \in G$. Since G is abelian, $x^{-1}y^{-1} = y^{-1}x^{-1}$. But $y^{-1}x^{-1} = (xy)^{-1}$, so $x^{-1}y^{-1} = (xy)^{-1}$, which implies $\varphi(x)\varphi(y) = \varphi(xy)$. Therefore φ is a homomorphism.

D&F Exercise 1.6.20

Let G be a group and let Aut(G) be the set of all isomorphisms from G to G. Prove that Aut(G) is a group under function composition (called the automorphism group of G and the elements of Aut(G) are called automorphisms of G).

Let G be a group. We will show that $\mathrm{Aut}(G)$ is a group under function composition. To do this, we must show the following:

- $\mathrm{Aut}(G)$ contains an identity. The identity element $\mathbb{1}$ is the trivial isomorphism $G \to G$ that maps every element to itself.

- $\mathrm{Aut}(G)$ is closed under function composition. This follows from the fact that under function composition, two isomorphisms $\varphi_1, \varphi_2 \in \mathrm{Aut}(G)$ form an isomorphism when combined, i.e., $(\varphi_1 \circ \varphi_2) \in \mathrm{Aut}(G)$. To show this, we will prove that $\varphi_1 \circ \varphi_2$ is both a bijection and a homomorphism. We can first note that because φ_1 and φ_2 are both bijections, then $\varphi_1 \circ \varphi_2$ is a bijection. To show $\varphi_1 \circ \varphi_2$ is a homomorphism, we can note that because φ_2 is a homomorphism, then $\varphi_2(a)\varphi_2(b) = \varphi_2(ab)$, for $a, b \in G$. Applying φ_1 to both sides of the equation, we have $\varphi_1(\varphi_2(a)\varphi_2(b)) = \varphi_1(\varphi_2(ab))$. But since φ_1 is also a homomorphism, then $\varphi_1(\varphi_2(a)\varphi_2(b)) = \varphi_1(\varphi_2(a))\varphi_1(\varphi_2(b))$. Therefore, $\varphi_1(\varphi_2(a))\varphi_1(\varphi_2(b)) = \varphi_1(\varphi_2(ab))$, i.e., $(\varphi_1 \circ \varphi_2)(a)(\varphi_1 \circ \varphi_2)(b) = (\varphi_1 \circ \varphi_2)(ab)$, so $\varphi_1 \circ \varphi_2$ is an homomorphism. Because $\varphi_1 \circ \varphi_2$ is a bijection and a homomorphism, then it is an isomorphism, so $(\varphi_1 \circ \varphi_2) \in \mathrm{Aut}(G)$, and therefore $\mathrm{Aut}(G)$ is closed under function composition.

- $\mathrm{Aut}(G)$ is closed under inverses. To show this, let $\varphi \in \mathrm{Aut}(G)$. Here, φ is an isomorphism, so it is a bijection, and therefore it is guaranteed that φ^{-1} exists and φ^{-1} is itself a bijection. We want to prove that $\varphi^{-1} \in \mathrm{Aut}(G)$. Since φ^{-1} is a bijection, all that remains in order to prove that φ^{-1} is a isomorphism (and therefore $\varphi^{-1} \in \mathrm{Aut}(G)$) is to show that φ^{-1} is a homomorphism. Let $a, b \in G$. Define $a' = \varphi^{-1}(a)$, $b' = \varphi^{-1}(b)$, and $(ab)' = \varphi^{-1}(ab)$, where $a', b', (ab)' \in G$. Equivalently, $\varphi(a') = a$, $\varphi(b') = b$, and $\varphi((ab)') = ab$. Since φ is a homomorphism, $\varphi(a')\varphi(b') = \varphi(a'b')$. But this implies $ab = \varphi(a'b')$. But then we have both $\varphi(a'b') = ab$ and $\varphi((ab)') = ab$, so $\varphi(a'b') = \varphi((ab)')$. Since φ is injective, this implies that $a'b' = (ab)'$. Expressing this equation in terms of φ^{-1}, it becomes $\varphi^{-1}(a)\varphi^{-1}(b) = \varphi^{-1}(ab)$, so therefore φ^{-1} is a homomorphism, as desired. Therefore, $\mathrm{Aut}(G)$ is closed under inverses.

- $\mathrm{Aut}(G)$ is associative. This follows from the associativity of function composition.

Therefore, $\mathrm{Aut}(G)$ is a group under function composition.

D&F Exercise 1.6.23

Let G be a finite group which possesses an automorphism σ (cf. Exercise 20) such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism σ is called fixed point free of order 2). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]

Let G be a finite group which possesses an automorphism σ with the property that $\sigma(g) = g$ if and only if $g = 1$. We will show that if σ^2 is the identity map from G to G, then G is abelian. To do this, we will first prove two smaller results:

(i) Any element $a \in G$ can be written as $a = x^{-1}\sigma(x)$, where $x \in G$. To prove this statement, it is sufficient to prove that the map $\varphi : G \to G$ where $\varphi(x) = x^{-1}\sigma(x)$ is an a bijection.

To prove this, we will first show that φ is injective, i.e., if $\varphi(x) = \varphi(y)$ then $x = y$ for any $x, y \in G$. Suppose $\varphi(x) = \varphi(y)$. By the definition of φ, then this implies $x^{-1}\sigma(x) = y^{-1}\sigma(y)$. Multiplying on

the left by x, we have $\sigma(x) = xy^{-1}\sigma(y)$. Acting on both sides by σ, and noting that $\sigma(\sigma(x)) = x$ and that σ is a homomorphism, we then have $x = \sigma(xy^{-1})y$. Multiplying both sides on the right by y^{-1}, we have $xy^{-1} = \sigma(xy^{-1})$. Since σ is fixed point free of order 2, this implies that $xy^{-1} = 1$, i.e., $x = y$. Therefore, φ is injective. Finally, we note that any injective map from a finite group to itself is also a bijection.

[Note: we have *not* proved that φ is an homomorphism. We only know that for any element $a \in G$, there is a unique $x \in G$ such that $a = \varphi(x) = x^{-1}\sigma(x)$. At this point, it is unknown whether φ preserves the group structure.]

(ii) The automorphism σ maps an element $a \in G$ to its inverse, i.e., $\sigma(a) = a^{-1}$. To show this, let $a \in G$, and using (i), we can write $a = x^{-1}\sigma(x)$, for some $x \in G$. Since σ is a homomorphism and $\sigma(\sigma(x)) = x$ by definition, then $\sigma(a) = \sigma(x^{-1}\sigma(x)) = \sigma(x^{-1})\sigma(\sigma(x)) = \sigma(x^{-1})x = \sigma(x)^{-1}x$. So, $\sigma(a) = \sigma(x)^{-1}x$. Now we can note $a\sigma(a) = x^{-1}\sigma(x)\sigma^{-1}(x)x = x^{-1}x = 1$. Therefore, $\sigma(a) = a^{-1}$.

Let $a, b \in G$. Using (ii), we have the identities $\sigma(ab) = (ab)^{-1} = b^{-1}a^{-1}$ and $\sigma(a)\sigma(b) = a^{-1}b^{-1}$. Because σ is a homomorphism, $\sigma(ab) = \sigma(a)\sigma(b)$, so therefore $b^{-1}a^{-1} = a^{-1}b^{-1}$, which is equivalent to $ab = ba$. Therefore, G is abelian.

[From here, one could then use the fact that G is abelian to deduce that φ is an homomorphism, and therefore a isomorphism.]

X. GROUP ACTIONS

D&F Exercise 1.7.1

Let F be a field. Show that the multiplicative group of nonzero elements of F (denoted by $F^\times$) acts on the set F by $g \cdot a$, where $g \in F^\times$, $a \in F$ and ga is the usual product in F of the two field elements (state clearly which axioms in the definition of a field are used).

Let F be a field. Consider the map $f : F^\times \times F \to F$ defined as $(g, a) \mapsto ga$, where $g \in F^\times$ and $a \in F$. To prove that f is a group action, we must show the following two results:

- $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, where $g_1, g_2 \in F^\times$ and $a \in F$. To show this, we can note that because of the associativity of multiplication in F, we have $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a) = g_1(g_2 a) = (g_1 g_2)a = (g_1 g_2) \cdot a$, as desired.

- $1 \cdot a = a$, where $a \in F$ and 1 is the identity of $F^\times$. Because the identity of $F^\times$ is the same as the multiplicative identity of F, then we have $1 \cdot a = 1a = a$, which follows from the axiom of the multiplicative identity of F.

Therefore, f is a group action.

D&F Exercise 1.7.3

Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

Consider the map $f : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$, defined as $(r, (x, y)) \mapsto (x + ry, y)$ where $x, y, r \in \mathbb{R}$. We will show that f is a group action. To do this, we must show the following two results:

- $r_1 \cdot (r_2 \cdot (x, y)) = (r_1 r_2) \cdot (x, y)$, where $r_1, r_2 \in \mathbb{R}$ and $(x, y) \in \mathbb{R}^2$. To show this, we can note $r_1 \cdot (r_2 \cdot (x, y)) = r_1 \cdot (x + r_2 y, y) = (x + r_1 y + r_2 y, y) = (x + (r_1 + r_2)y, y) = (r_1 + r_2) \cdot (x, y)$, as desired.

- $0 \cdot (x, y) = (x, y)$, where $(x, y) \in \mathbb{R}^2$ and 0 is the additive identity of $\mathbb{R}$. To show this, we can note that $0 \cdot (x, y) = (x + 0y, y) = (x, y)$, as desired.

Therefore, f is a group action.

D&F Exercise 1.7.4

Let G be a group action on the A and fix some $a \in A$. Show that the following sets are subgroups of G (cf. D&F Exercise 1.1.26):

(a) the kernel of the action,

(b) $\{g \in G | ga = a\}$ – this subgroup is called the stabilizer of a in G.

Let f be the group action of a group G on A, i.e., $f : G \times A \to A$. We will show the following two results:

(a) *Claim:* The kernel of f, i.e., $\ker f = \{g \in G | g \cdot a = a, \text{ for all } a \in A\}$, is a subgroup of G.

Proof: We will show that for every $a \in A$, that (1) $1 \cdot a = a$, and (2) if $x \cdot a = a$ and $y \cdot a = a$, where $x, y \in G$, then $xy^{-1} \cdot a = a$. Let $a \in A$. We can first note that since f is a group action, $1 \cdot a = a$. Next, suppose $x \cdot a = a$ and $y \cdot a = a$, where $x, y \in G$. Here, $(xy^{-1}) \cdot a = (xy^{-1}) \cdot (y \cdot a) = x \cdot (y^{-1} \cdot (y \cdot a)) = x \cdot ((y^{-1}y) \cdot a) = x \cdot (1 \cdot a) = x \cdot a = a$, so therefore $xy^{-1} \cdot a = a$. According to the Subgroup Criterion, $\ker f$ is a subgroup of G.

(b) *Claim:* For a fixed element $a \in A$, the stabilizer of a in G, i.e., $\text{Stab}_G(a) = \{g \in G | g \cdot a = a\}$, is a subgroup of G.

Proof: We will show that for a fixed $a \in A$, that (1) $1 \cdot a = a$, and (2) if $x \cdot a = a$ and $y \cdot a = a$, where $x, y \in G$, then $xy^{-1} \cdot a = a$. To show this, fix $a \in A$. We can first note that since f is a group action, $1 \cdot a = a$. Next, suppose $x \cdot a = a$ and $y \cdot a = a$, where $x, y \in G$. Here, $(xy^{-1}) \cdot a = (xy^{-1}) \cdot (y \cdot a) = x \cdot (y^{-1} \cdot (y \cdot a)) = x \cdot ((y^{-1}y) \cdot a) = x \cdot (1 \cdot a) = x \cdot a = a$, so therefore $xy^{-1} \cdot a = a$. According to the Subgroup Criterion, $\text{Stab}_G(a)$ is a subgroup of G.

D&F Exercise 1.7.5

Prove that the kernel of an action of a group G on the set A is the same as the kernel of the corresponding permutation representation $G \to S_A$.

Let f be a group action of the group G on A, i.e., $f : G \times A \to A$, and let φ be the corresponding permutation representation of the group action $\varphi : G \to S_A$, so $g \mapsto \sigma_g$, where $g \in G$ and σ_g is a permutation on A. The term "corresponding permutation representation" means $g \cdot a = \sigma_g(a)$ (cf. D&F Sec. 1.7, p. 42).

The kernel of f is $\ker f = \{g \in G | g \cdot a = a, \text{ for all } a \in A\}$ and the kernel of φ is $\ker \varphi = \{g \in G | \sigma_g(a) = a, \text{ for all } a \in A\}$. Since $g \cdot a = \sigma_g(a)$, therefore $\ker f = \ker \varphi$.

D&F Exercise 1.7.6

Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.

We will prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity. Here, "faithfully" means that distinct elements of G induce distinct

permutations of A. To show this, let f be the group action $f : G \times A \to A$, and φ be the homomorphism $\varphi : G \to S_A$.

First, suppose that f is faithful. We will show that $\ker f$ is the set consisting only of the identity. First, we can note that because f is faithful, then φ maps distinct elements of G to distinct elements of S_A, i.e., φ is injective. Since φ is an injective homomorphism, we can use the result in D&F Exercise 1.6.14 to claim that $\ker \varphi = \{1\}$. Then according to D&F Exercise 1.7.5, we can conclude that $\ker f = \{1\}$.

Conversely, suppose that the $\ker f$ contains only the identity. We will show that f is faithful. First, we can note the result in D&F Exercise 1.7.5, and claim that if $\ker f = \{1\}$, then $\ker \varphi = \{1\}$, and then use the result from D&F Exercise 1.6.14 to claim that if $\ker \varphi = \{1\}$, then φ is injective. This means φ maps distinct elements in G to distinct elements in S_A. Therefore, f is faithful, by definition.

Therefore, a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.

D&F Exercise 1.7.8

Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, \cdots, a_k\} = \{\sigma(a_1), \cdots, \sigma(a_k)\}$.

(a) Prove that this is a group action.

(b) Describe explicitly how the elements (12) and (123) act on the six 2-element subsets of $\{1, 2, 3, 4\}$.

Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. Let B be the set consisting of all subsets of A of cardinality k by $\{a_1, \cdots, a_k\}$. Let f be the map $f : S_A \times B \to B$ defined as $\sigma \cdot \{a_1, \cdots, a_k\} \mapsto \{\sigma(a_1), \cdots, \sigma(a_k)\}$.

(a) The map f is a group action. To show this, we must show the following two results:

- $\sigma_1 \cdot (\sigma_2 \cdot \{a_1, \cdots, a_k\}) = (\sigma_1\sigma_2) \cdot \{a_1, \cdots, a_k\}$, where $\sigma_1, \sigma_2 \in S_A$. To show this, we can note $\sigma_1 \cdot (\sigma_2 \cdot \{a_1, \cdots, a_k\}) = \sigma_1 \cdot \{\sigma_2(a_1), \cdots, \sigma_2(a_k)\} = \{\sigma_1(\sigma_2(a_1)), \cdots, \sigma_1(\sigma_2(a_k))\} = \{(\sigma_1\sigma_2)(a_1), \cdots, (\sigma_1\sigma_2)(a_k)\} = (\sigma_1\sigma_2) \cdot \{a_1, \cdots, a_k\}$, as desired.
- $1 \cdot \{a_1, \cdots, a_k\} = \{a_1, \cdots, a_k\}$. To show this, we have $1 \cdot \{a_1, \cdots, a_k\} = \{1(a_1), \cdots, 1(a_k)\} = \{a_1, \cdots, a_k\}$, as desired.

Therefore, this is a group action.

(b) The following is how $\sigma = (12)$ and (123) act on the six 2-element subsets of $\{1, 2, 3, 4\}$:

$$\begin{aligned}
(12) \cdot \{1,2\} &= \{2,1\} \\
(12) \cdot \{1,3\} &= \{2,3\} \\
(12) \cdot \{1,4\} &= \{2,4\} \\
(12) \cdot \{2,3\} &= \{1,3\} \\
(12) \cdot \{2,4\} &= \{1,4\} \\
(12) \cdot \{3,4\} &= \{3,4\} \\
(123) \cdot \{1,2\} &= \{2,3\} \\
(123) \cdot \{1,3\} &= \{2,1\} \\
(123) \cdot \{1,4\} &= \{2,4\} \\
(123) \cdot \{2,3\} &= \{3,1\} \\
(123) \cdot \{2,4\} &= \{3,4\} \\
(123) \cdot \{3,4\} &= \{1,4\}
\end{aligned} \tag{71}$$

D&F Exercise 1.7.11

Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements of D_8 given by the action D_8 on the vertices of a square (where the vertices of the square are labeled as in Section 2).

Let φ be the homomorphism $\varphi : D_8 \to S_4$ associated with the permutation representation of D_8 acting on the vertices of a square. The vertices of the square are labeled in Fig. 1. Here, r is a clockwise rotation of the square by $\pi/2$ radians, and s is a reflection about the line of symmetry through vertex 1 and the origin. The correspondence between the elements of D_8 and S_4 are tabulated below:

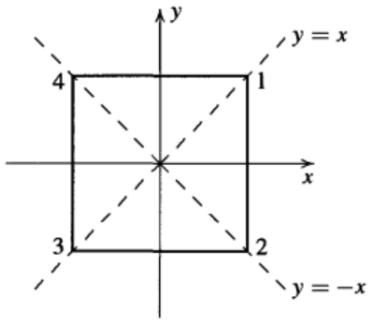


FIG. 1 The square from Section 1.2

$g \in D_8$	$\varphi(g) \in S_4$
1	1
r	(1234)
r^2	(13)(24)
r^3	(1432)
s	(24)
sr	(14)(23)
sr^2	(13)
sr^3	(12)(34)

(72)

D&F Exercise 1.7.12

Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n-gon. Find the kernel of this action (label vertices as usual).

Consider a regular n-gon, where n is even, and label the vertices of the regular n-gon in clockwise fashion, beginning with 1, as in the previous problem. The set of containing a vertex label k along with its opposite partner can be denoted $a_k := \{k, k+n/2\}$, where $1 \leq k \leq n/2$. Importantly, the magnitude of the numerical difference of the two elements in the set a_k is always $n/2$ – this is the definition of "opposite vertices." Let A be the set of all such opposite pairs, i.e., $A = \{a_1, a_2, \cdots, a_{n/2}\}$.

Let f be the map $f : D_{2n} \times A \to A$. Here, $r \in D_{2n}$ is defined as a clockwise rotation by $2\pi/n$ radians, and $s \in D_{2n}$ is a reflection about the line of symmetry through vertex n and the origin. Here, we will show explicitly how the elements of D_{2n} act on a_k. We will consider two types of elements of D_{2n}: ones of the form r^ℓ and ones of the form sr^ℓ, where $\ell \in \mathbb{Z}$ in the range $0 \leq \ell \leq n-1$. Elements of D_{2n} act on elements of A as follows:

$$r^\ell \cdot a_k = r^\ell \cdot \{k, k+n/2\} = \{k+\ell, k+\ell+n/2\} \pmod n = a_{k+\ell \pmod n} \tag{73}$$

$$sr^\ell \cdot a_k = sr^\ell \cdot \{k, k+n/2\} = \{n-k-\ell, n-k-\ell-n/2\} \pmod n = a_{n-k-\ell \pmod n} \tag{74}$$

Here, we are identifying the vertex with label n with the 0 element of $\mathbb{Z}/n\mathbb{Z}$. Note that the above actions on elements of A does not change the fact that they are pairs of opposite vertices. Therefore, the action of elements of D_{2n} on elements of A induces a permutation of the elements of A, which we can denote as $g \cdot a_k = \sigma_g(a_k)$, for each $g \in D_{2n}$.

Now we will show that f is a group action. To do so, we can show the following two results:

- $g_1 \cdot (g_2 \cdot a_k) = (g_1 g_2) \cdot a_k$ for $g_1, g_2 \in D_{2n}$ and $a_k \in A$. To see this, we can note $g_1 \cdot (g_2 \cdot a_k) = g_1 \cdot \sigma_{g_2}(a_k) = \sigma_{g_1}(\sigma_{g_2}(a_k)) = (\sigma_{g_1} \circ \sigma_{g_2})(a_k) = (g_1 g_2) \cdot a_k$, as desired.
- $1 \cdot a_k = a_k$, for $a_k \in A$. This follows from Eq. (73) when $\ell = 0$.

Therefore, f is a group action.

Claim: The kernel of the action contains only the identity and $r^{n/2}$.

Proof: The condition that an element $g \in G$ is in the kernel of f is the requirement that $g \cdot a_k = a_k$, for all $a_k \in A$. We can use Eqs. (73) and (74) to solve for the elements of G that satisfy this condition. Using Eq. (73), we have the following condition:

$$\{k+\ell, k+\ell+n/2\} \equiv \{k, k+n/2\} \tag{75}$$

which can be satisfied only if $\ell \equiv 0$ or $\ell \equiv n/2$. Likewise using Eq. (74), we have the following condition:

$$\{n-k-\ell, n-k-\ell-n/2\} \equiv \{k, k+n/2\} \tag{76}$$

for which there is no solution in ℓ. Therefore, $\ker f = \{1, r^{n/2}\}$.

D&F Exercise 1.7.13

Find the kernel of the left regular action.

Let G be a group. The kernel of the left regular action is defined as $\{g \in G | ga = a, \text{ for all } a \in G\}$. The only element that satisfies the requirements for this set is the identity. To show this, let $a \in G$. For $g \in G$ to be in the kernel of the left regular action, this requires $ga = a$. Multiplying on the right by a^{-1} on both sides of this equation, we have $g = aa^{-1} = 1$. So only $g = 1$ is in the kernel of the left regular action.

D&F Exercise 1.7.14

Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g, a \in G$ do not satisfy the axioms of a (left) group action of G on itself.

Let G be a group and let $A = G$, and consider the map $f : G \times A \to A$, defined as $g \cdot a = ag$ for $g, a \in G$.

Claim: If G is non-abelian, then f cannot be a (left) group action.

Proof: We will proceed by contradiction. Assume f is a group action. Let $g_1, g_1 \in G$ and $a \in A$. Then we have $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$. Given the definition of the group action, we this implies $ag_2 g_1 = ag_1 g_2$. Multiplying on the left by a^{-1} on both sides of the equation, this yields $g_2 g_1 = g_1 g_2$. However, this is a contradiction, since G is non-abelian. Therefore, f is not a (left) group action.

D&F Exercise 1.7.15

Let G by any group and let $A = G$. Show that the maps defined by $g \cdot a = ag^{-1}$ for all $g, a \in G$ do satisfy the axioms of a (left) group action of G on itself.

Let G be a group and let $A = G$, and consider the map $f : G \times A \to A$, defined as $g \cdot a = ag^{-1}$ for $g, a \in G$. We will show that f is a group action by proving the following two requirements:

- Let $g_1, g_2, a \in G$. We will show $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$. To see this, note $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (ag_2^{-1}) = ag_2^{-1} g_1^{-1} = a(g_1 g_2)^{-1} = (g_1 g_2) \cdot a$, as desired.
- $1 \cdot a = a$. This follows from the properties of the identity: $1 \cdot a = a1 = a$.

Therefore f is a group action.

D&F Exercise 1.7.16

Let G by any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ for all $g, a \in G$ do satisfy the axioms of a (left) group action (this action of G on itself is called a conjugation).

Let G be a group and let $A = G$, and consider the map $f : G \times A \to A$, defined as $g \cdot a = gag^{-1}$ for $g, a \in G$. We will show that f is a group action by proving the following two requirements:

- Let $g_1, g_2, a \in G$. We will show $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$. To see this, note $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1 g_2 a g_2^{-1} g^{-1} = (g_1 g_2) a (g_1 g_2)^{-1} = (g_1 g_2) \cdot a$, as desired.
- $1 \cdot a = a$. This follows from the properties of the identity: $1 \cdot a = 1a1 = a$.

Therefore f is a group action.

D&F Exercise 1.7.17

Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by $x \mapsto gxg^{-1}$. For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself (i.e., is an automorphism of G – cf. D&F Exercise 1.6.20). Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset of A of G, $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1} | a \in A\}$).

Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by $x \mapsto gxg^{-1}$. We will show the following results:

(a) For fixed $g \in G$, conjugation by g is an isomorphism from G onto itself. To show this, let $g \in G$ be fixed, and let φ_g be the map $\varphi_g : G \to G$ defined by $x \mapsto gxg^{-1}$ for $x \in G$.

First, we will show that φ_g is a homomorphism. Here, let $x_1, x_2 \in G$, and we can note $\varphi_g(x_1 x_2) = g x_1 x_2 g^{-1} = g x_1 (g^{-1} g) x_2 g^{-1} = (g x_1 g^{-1})(g x_2 g^{-1}) = \varphi_g(x_1)\varphi_g(x_2)$. Therefore, φ_g is a homomorphism.

Next, we will show that φ_g is injective. To do this, let $x_1, x_2 \in G$ such that $\varphi_g(x_1) = \varphi_g(x_2)$. This implies $g x_1 g^{-1} = g x_2 g^{-1}$. Multiplying on the right by g and on the left by g^{-1} on both sides of the equation, this yields $x_1 = x_2$. Therefore, φ_g is injective.

Finally, we will show that φ_g is surjective. Let $y \in G$. Then we can always construct the element $x = g^{-1} y g$. Solving for y, we have $y = gxg^{-1}$, i.e., $\varphi_g(x) = y$. Therefore, φ_g is surjective.

So, since φ_g is a bijective homomorphism from G to itself, it is therefore an automorphism.

(b) x and gxg^{-1} have the same order for all x in G. This is the same as D&F Exercise 1.1.22, and the solution can be found there.

(c) $|A| = |gAg^{-1}|$, where A be any subset of G and $g \in G$. Here, $gAg^{-1} = \{gag^{-1} | a \in A\}$. To show this, let $g \in G$. From part (a), it was shown that the map $G \mapsto gGg^{-1}$ is bijective, so therefore the map for any subset A of G, $A \mapsto gAg^{-1}$, will also be a bijection. Therefore, $|A| = |gAg^{-1}|$.

D&F Exercise 1.7.18

Let H be a group action on a set A. Prove that the relation $\sim$ on A defined by

$$a \sim b \qquad \text{if and only if} \qquad a = hb \quad \text{for some } h \in H$$

is an equivalence relation. (For each $x \in A$ the equivalence class x under $\sim$ is called the orbit of x under the action H. The orbits under the action of H partition the set A.)

Let $f : H \times A \to A$ be the group action of H acting on the set A. Let $a, b \in H$. We will show that the relation $\sim$ on A defined by $a \sim b$ if and only iff $a = hb$ for some $h \in H$ is an equivalence relation. To do this, we must show the following three results:

- $\sim$ is reflexive. To see this, let $a \in A$. Since $a = 1a$, and $1 \in H$, then $\sim$ is reflexive.

- $\sim$ is symmetric. To see this, let $a, b \in A$ where $a \sim b$, i.e., $a = hb$ for some $h \in H$. Here, $a = hb$ implies $b = h^{-1}a$. Since $h^{-1} \in H$, then $b \sim a$. Therefore, $\sim$ is symmetric.
- $\sim$ is transitive. To see this, let $a, b, c \in A$, where $a \sim b$ and $b \sim c$, i.e., $a = hb$ and $b = h'c$ for some $h, h' \in H$. We can note $a = hb = h(h'c) = (hh')c$, and since $hh' \in H$, then this implies $a \sim c$. Therefore, $\sim$ is transitive.

Since $\sim$ is reflective, symmetric, and transitive, it is therefore an equivalence relation.

D&F Exercise 1.7.19

Let H be a subgroup of a finite group G and let H act on G (here $A = G$) by left multiplication. Let $x \in G$ and let $\mathcal{O}$ be the orbit of x under the action of H. Prove that the map

$$H \to \mathcal{O} \quad \textit{defined by} \quad h \mapsto hx$$

is a bijection (hence all orbits have cardinality $|H|$). From this and the preceding exercise, deduce Lagrange's Theorem:

if G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

Let H be a subgroup of a finite group G and let H act on G by left multiplication. Let $x \in G$ and let $\mathcal{O}_x$ be the orbit of x under the action of H.

Let φ_x be the map $\varphi_x : H \to \mathcal{O}_x$ defined by $\varphi_x(h) = hx$, where $h \in H$. Here, we will show φ_x is a bijection. To do this, we will first show that it is injective. Let $h_1, h_2 \in H$ such that $\varphi_x(h_1) = \varphi_x(h_2)$. This implies $h_1 x = h_2 x$, and after multiplying on the right by x^{-1}, we have $h_1 = h_2$. Therefore, φ_x is injective. Next, we can note that φ_x is surjective by definition, since $\mathcal{O}_x$ is comprised of only elements that are in the image of φ_x. Therefore, φ_x is a bijection.

Since $H \to \mathcal{O}_x$ is a bijection, we can immediately conclude that $|H| = |\mathcal{O}_x|$. This result holds for any element $x \in G$. So, all orbits of elements of G under the action of H have the same cardinality, equal to $|H|$.

From here, we can use the result in D&F Exercise 1.7.18, which states that the orbits produced by the action of H on G partition the set. Combined with the result in the previous paragraph, all of these orbit partitions have the same cardinality, i.e., $|H|$. Therefore, $|H|$ must divide $|G|$.

D&F Exercise 1.7.20

Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup of S_4.

Let G be the group of rigid motions of a tetrahedron. Let the set $A = \{1, 2, 3, 4\}$ contain the labels for each vertex of the tetrahedron. Since the motions are rigid, this means elements $g \in G$ acting on elements $a \in A$ can be represented as permutations on A, i.e., $g \cdot a = \sigma_g(a)$. This means we can define the map $\varphi : G \to S_4$, defined as $\varphi(g) = \sigma_g$.

First, we can note that φ is a homomorphism, which is proven on p. 42 of D&F.

Next, we will show that φ is injective. To do this, we can note that the only element of G that does not alter the location of any of the tetrahedron's vertices is the identity of G. Therefore, the kernel of φ only contains the identity. We can use the result from D&F Exercise 1.6.14, which states that φ is injective if and only if the kernel of φ is the identity subgroup of G. Therefore, φ is injective.

Finally, we can use the results from D&F Exercise 1.6.13 to conclude: (1) if φ is a homomorphism, $\varphi(G)$ is subgroup of S_4, and (2) if φ is an injective homomorphism, then G is isomorphic to $\varphi(G)$. Using these, then G is isomorphic to a subgroup of S_4.

D&F Exercise 1.7.21

Show that the group of rigid motions of a cube is isomorphic to S_4. [This group acts on the set of four pairs of opposite vertices.]

Let G be the group of rigid motions of a cube. From D&F Exercise 1.2.8, we know $|G| = 24$. We consider that G acts on the four pairs of opposite vertices, and we can denote the set of pairs of opposite vertices as $A = \{a_1, a_2, a_3, a_4\}$. Since the motions of the cube are rigid, this means elements of G acting on elements of A will induce a permutation of the elements of A, i.e., $g \cdot a = \sigma_g(a)$, where $a \in A$. This means we can define the map $\varphi : G \to S_4$, defined as $\varphi(g) = \sigma_g$.

We can following the same line of reasoning as in the previous problem, D&F Exercise 1.7.20, concluding that $\varphi(G)$ is isomorphic to a subgroup of S_4. However, for the case of the cube, $|G| = 24$ and $|S_4| = 24$, so $\varphi(G)$ is in fact isomorphic to S_4 itself.

XI. CENTRALIZERS AND NORMALIZERS, STABILIZERS AND KERNELS

D&F Exercise 2.2.1

Prove that $C_G(A) = \{g \in G | g^{-1}ag = a \text{ for all } a \in A\}$.

Let G be a group, and A be a nonempty subset of G. We will show that $C_G(A) = \{g \in G | g^{-1}ag = a \text{ for all } a \in A\}$. To see this, by definition the centralizer of A in G is $C_G(A) = \{g \in G | gag^{-1} = a \text{ for all } a \in A\}$. One can note that $gag^{-1} = a$ is equivalent to $g^{-1}ag = a$ by multiplying both sides of the equation on the left by g^{-1} and on the right by g. Therefore, $C_G(A) = \{g \in G | g^{-1}ag = a \text{ for all } a \in A\}$.

D&F Exercise 2.2.2

Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Let G be a group. We will show the following:

(a) *Claim:* $C_G(Z(G)) = G$.

Proof: We will show $C_G(Z(G))$ contains all elements of G. To show this, we can note that $C_G(Z(G)) = \{g \in G | gzg^{-1} = z \text{ for all } z \in Z(G)\}$. But $z \in Z(G)$ commutes with all elements of $g \in G$, so the condition $gzg^{-1} = z$ is satisfied for all $g \in G$, since $gzg^{-1} = gg^{-1}z = z$. Therefore, $C_G(Z(G))$ contains all elements of G.

(b) *Claim:* $N_G(Z(G)) = G$.

Proof: Since $C_G(Z(G)) \leq N_G(Z(G))$ (cf. D&F Section 2.2), and from part (a) we proved $C_G(Z(G)) = G$, then $N_G(Z(G)) = G$.

D&F Exercise 2.2.3

Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Let A and B be subsets of G, where $A \subseteq B$. We will show $C_G(B)$ is a subgroup of $C_G(A)$. To begin, let $g \in C_G(B)$. By definition, g commutes with all elements of B. Since $A \subseteq B$, then g also commutes with all elements of A. So, by definition, $g \in C_G(A)$. Therefore $C_G(B) \subseteq C_G(A)$. Since $C_G(B)$ and $C_G(A)$ are both groups, we can conclude $C_G(B) \leq C_G(A)$.

D&F Exercise 2.2.5

In each of parts (a) to (c) show that for the specified group G and subgroup A of G, $C_G(A) = A$ and $N_G(A) = G$.

(a) $G = S_3$ *and* $A = \{1, (123), (132)\}$.

(b) $G = D_8$ *and* $A = \{1, s, r^2, sr^2\}$.

(c) $G = D_{10}$ *and* $A = \{1, r, r^2, r^3, r^4\}$.

We will show the following results:

(a) Let $A = \{1, (123), (132)\}$.

Claim: $C_{S_3}(A) = A$.

Proof: First we can note that A is a subgroup, since it satisfies the conditions for a group. Furthermore, it is abelian. Therefore, $A \leq C_{S_3}(A)$. We also know that $C_{S_3} \leq S_3$. Since $|A| = 3$ and $|S_3| = 6$, we can use Lagrange's theorem to conclude that $|C_{S_3}(A)|$ is either 3 or 6. However, we know that $|C_{S_3}(A)|$ cannot be 6, since, for example, $(12)(123)(12)^{-1} = (13) \neq (123)$. Therefore, $|C_{S_3}(A)| = 3$. Since $A \leq C_{S_3}(A)$, we therefore can conclude that $C_{S_3}(A) = A$.

Claim: $N_{S_3}(A) = S_3$.

Proof: Since $C_{S_3}(A) \leq N_{S_3}(A) \leq S_3$, and we concluded that $|C_{S_3}(A)| = 3$, we can deduce from Lagrange's theorem that $|N_{S_3}(A)|$ is 3 or 6. Now, we can note that because $(13)(123)(13) = (132) \in A$, then $(13) \in N_{S_3}(A)$. So, $N_{S_3}(A) > 3$, and we can conclude $|N_{S_3}(A)| = 6$. Since $|S_3| = 6$, therefore $N_{S_3}(A) = S_3$.

(b) Let $A = \{1, s, r^2, sr^2\}$.

Claim: $C_{D_8}(A) = A$.

Proof: First we can note that A is a subgroup, since it satisfies the conditions for a group. Furthermore, it is abelian. Therefore, $A \leq C_{D_8}(A)$. We also know that $C_{D_8} \leq D_8$. Since $|A| = 4$ and $|D_8| = 8$, then we can conclude via Lagrange's theorem that $|C_{D_8}|$ is either 4 or 8. However, we know that $|C_{D_8}(A)|$ cannot be 8, since, for example, $r(s)r^{-1} = r^2 \neq s$. Therefore, $|C_{D_8}(A)| = 4$. Since $A \leq C_{D_8}(A)$, we therefore can conclude that $C_{D_8}(A) = A$.

Claim: $N_{D_8}(A) = D_8$.

Proof: Since $C_{D_8}(A) \leq N_{D_8}(A) \leq D_8$, and we concluded that $|C_{D_8}(A)| = 4$, we can deduce from Lagrange's theorem that $|N_{D_8}(A)|$ is 4 or 8. Now, we can note that because $r(s)r^{-1} = r^2 \in A$, then $r \in N_{D_8}(A)$. So, $N_{D_8}(A) > 4$, and we can conclude $|N_{D_8}(A)| = 8$. Since $|D_8| = 8$, therefore $N_{D_8}(A) = D_8$.

(c) Let $A = \{1, r, r^2, r^3, r^4\}$.

Claim: $C_{D_{10}}(A) = A$.

Proof: First we can note that A is a subgroup, since it satisfies the conditions for a group. Furthermore, it is abelian. Therefore, $A \leq C_{D_{10}}(A)$. We also know that $C_{D_{10}} \leq D_{10}$. Since $|A| = 5$ and $|D_{10}| = 10$, then we can conclude via Lagrange's theorem that $|C_{D_{10}}|$ is either 5 or 10. However, we know that $|C_{D_{10}}(A)|$ cannot be 10, since, for example, $(sr)(s)(sr)^{-1} = sr^2 \neq s$. Therefore, $|C_{D_{10}}(A)| = 5$. Since $A \leq C_{D_{10}}(A)$, we therefore can conclude that $C_{D_{10}}(A) = A$.

Claim: $N_{D_{10}}(A) = D_{10}$.

Proof: Since $C_{D_{10}}(A) \leq N_{D_{10}}(A) \leq D_{10}$, and we concluded that $|C_{D_{10}}(A)| = 5$, we can deduce from Lagrange's theorem that $|N_{D_{10}}(A)|$ is 5 or 10. Now, we can note that because $(sr)(s)(sr)^{-1} = sr^2 \in A$, then $sr \in N_{D_{10}}(A)$. So, $N_{D_{10}}(A) > 5$, and we can conclude $|N_{D_{10}}(A)| = 10$. Since $|D_{10}| = 10$, therefore $N_{D_{10}}(A) = D_{10}$.

D&F Exercise 2.2.6

Let H be a subgroup of the group G.

(a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.

(b) Show that $H \leq C_G(H)$ if and only if H is abelian.

First we will prove the following Lemma:

(i) *Lemma:* Let H be a group and $h \in H$. Then $hHh^{-1} = H$. (Conjugation of an entire group by any of its elements gives back the original group.)

Proof:

Let $h \in H$.

First, we will show that given an element $x \in hHh^{-1}$ then $x \in H$. To show this, let $x \in hHh^{-1}$. This means there there exists an element $h' \in H$ such that $x = hh'h^{-1}$. But $hh'h^{-1} \in H$, since H is closed under the group operation. Therefore $x \in H$.

Second, we will show that given an element $x \in H$, then $x \in hHh^{-1}$. To begin, let $x \in H$. Then we have $x = h(h^{-1}xh)h^{-1} \in H$, since h, h^{-1}, and $h^{-1}xh$ are all element of H.

Therefore, since $hHh^{-1} \subseteq H$ and $H \subseteq hHh^{-1}$, then $hHh^{-1} = H$, as desired.

Now back to the original problem. Let H be a subgroup of the group G. We will show the following:

(a) *Claim:* $H \leq N_G(H)$.

Proof: We will first show that $H \subseteq N_G(H)$. Let $h \in H$. Given the result from (i), we have $hHh^{-1} = H$. By definition, this means $h \in N_G(H)$. Therefore, since $h \in H$ implies $h \in N_G(H)$, we have $H \subseteq N_G(H)$. Next, because both H and $N_G(H)$ are subgroups of G, then $H \leq N_G(H)$, as desired.

Note: if H is not a subgroup, then this result does not necessarily hold. For example, let A be the subset $\{(12), (13)\}$ of S_3. Here, A is not a group. So, while $(12) \in A$, we can note that $(12) \notin N_G(A)$ since $(12)(13)(12)^{-1} = (23) \notin A$. So, $A \not\subseteq N_G(A)$.

(b) *Claim:* $H \leq C_G(H)$ if and only if H is abelian.

Proof: First, assume that H is abelian. We will show $H \leq C_G(H)$. Let $h, h' \in H$. Because H is abelian, we have $hh' = h'h$. But this is equivalent to $hh'h^{-1} = h'$. Because this holds for all $h' \in H$, then by definition $h \in C_G(H)$. Since this holds for any arbitrary element $h \in H$, then $H \subseteq C_G(H)$. Since H and $C_G(H)$ are both groups, we conclude $H \leq C_G(H)$.

Conversely, assume $H \leq C_G(H)$. We will show H is abelian. Let $h \in H$. Since $H \leq C_G(H)$, then $h \in C_G(H)$. This means $hh'h^{-1} = h'$ for all $h' \in H$. This implies h commutes with all elements of H. Since h is an arbitrary element of H, then we can conclude that all elements of H commute with all elements of H. Therefore, H is abelian.

D&F Exercise 2.2.8

Let $G = S_n$, fix an $i \in \{1, 2, \cdots, n\}$ and let $G_i = \{\sigma \in G | \sigma(i) = i\}$ (the stabilizer of i in G). Use group actions to prove that G_i is a subgroup of G. Find $|G_i|$.

Let $G = S_n$ and $A = \{1, 2, \cdots, n\}$. Consider a group action of G on A, i.e., $f : G \times A \to A$, defined by $g \cdot i = \sigma_g(i)$, where $g \in G$ and $i \in A$. Here, we fix some $i \in A$. The proof that the stabilizer of i in G, i.e., G_i, is a subgroup of G can be found in D&F Exercise 1.7.4(b).

Here, $|G_i| = (n-1)!$. This comes from the fact that if the element i remains unchanged under the action of S_n, then there are $(n-1)!$ elements of the S_n that do not affect i.

D&F Exercise 2.2.10

Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$ then $H \leq Z(G)$.

Let H be a subgroup of order 2 in G. We will show the following:

(a) *Claim:* $N_G(H) = C_G(H)$.

Proof: We will show that when $|H| = 2$, the definitions for $C_G(H)$ and $N_G(H)$ are identical. To begin, we can note that because H only has two elements, we can represent it as $H = \{1, h\}$.

First, the condition that $g \in C_G(H)$ is $gxg^{-1} = x$ for all $x \in H = \{1, h\}$. Explicitly substituting in the elements of H for x, we have the following two conditions: $g1g^{-1} = 1$ and $ghg^{-1} = h$. The former is automatically satisfied for all $g \in G$ since $g1g^{-1} = gg^{-1} = 1$. The latter, $ghg^{-1} = h$, is a non-trivial condition. So, if $ghg^{-1} = h$ then $g \in C_G(H)$.

Second, the condition that an element $g \in G$ is also $g \in N_G(H)$ is $gHg^{-1} = H$. Again, explicitly substituting in the elements of H for x, we must have $g1g^{-1} = 1$, so we have the non-trivial condition that $ghg^{-1} = h$. So, if $ghg^{-1} = h$ then $g \in N_G(H)$.

Therefore, the condition for an element $g \in G$ to be in $C_G(H)$ and $N_G(H)$ are identical, i.e., $ghg^{-1} = h$, and we can conclude that $C_G(H) = N_G(H)$.

(b) *Claim:* If $N_G(H) = G$ then $H \leq Z(G)$.

Proof: If $N_G(H) = G$, then we can use the result from part (a) to conclude $C_G(H) = G$. Here, $C_G(H) = G$ means $gxg^{-1} = x$ for all $g \in G$ and for all $x \in H$. This implies that all elements of H commute with all elements of G. Therefore, $H \leq Z(G)$.

XII. CYCLIC GROUPS AND CYCLIC SUBGROUPS

D&F Exercise 2.3.2

If x is an element of the finite group G and $|x| = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show that this result need not be true if G is an infinite group.

Let x be an element of the finite group G and suppose $|x| = |G| = n$. We will show that $G = \langle x \rangle$. We can note the result from D&F Exercise 1.1.32, which states: *if x is an element of finite order n in a group G, then the elements $1, x, x^2, \cdots, x^{n-1}$ are all distinct.* So, we can use this result to say that the set $\langle x \rangle = \{1, x, x^2, \cdots, x^{n-1}\}$ contains distinct elements. In particular, there are n such distinct elements. But G only contains n elements. Therefore, $G = \langle x \rangle$.

This result holds when G is a finite group. However, if G is an infinite group, then it does not necessarily hold. To see why, consider $G = (\mathbb{Z}, +)$ and $2 \in G$. While $|G|$ and $|2|$ are both infinite, here $\langle 2 \rangle = \{\cdots, -4, -2, 0, 2, 4, \cdots\} \neq G$.

D&F Exercise 2.3.9

Let $Z_{36} = \langle x \rangle$. For which integers a does the map φ_a defined by $\varphi_a : \bar{1} \mapsto x^a$ extend to a well defined homomorphism from $\mathbb{Z}/48\mathbb{Z}$ into Z_{36}? Can ψ_a ever be a surjective homomorphism?

Let $Z_{36} = \langle x \rangle$, and let φ_a be the map $\varphi_a : \mathbb{Z}/48\mathbb{Z} \to Z_{36}$, defined by $\varphi_a(\bar{n}) = x^{na}$. We will derive for what integers a lead to φ_a being a well-defined homomorphism.

Before we begin, we will show the following results. In the following, let $a, m, n, x, y \in \mathbb{Z}$.

(i) *Claim*: If $m \equiv n \pmod{x}$ and $am \equiv an \pmod{y}$, then a is a multiple of $y/\gcd(x,y)$.

Proof: Let $d = \gcd(x,y)$, so $x = dx'$ and $y = dy'$, so $\gcd(x',y') = 1$. Since $m \equiv n \pmod{x}$ and $am \equiv an \pmod{y}$, there are integers k, ℓ such that $m - n = xk$ and $a(m-n) = y\ell$. This implies $axk = y\ell$, or equivalently, $\ell = (ax'/y')k$. The LHS of this equation is an integer, so the RHS must also be an integer. Now, the value of k is not uniquely determined. So in order to guarantee that ℓ is an integer, ax'/y' must be an integer, i.e., a must be a multiple of $y' = y/\gcd(x,y)$, as desired.

(ii) *Claim*: If $m \equiv n \pmod{x}$ and a is a multiple of $y/\gcd(x,y)$, then $am \equiv an \pmod{y}$.

Proof: Let $d = \gcd(x,y)$, where $y = y'd$. Assume a is a multiple of $y/d = y'$, so there is an integer ℓ such that $a = y'\ell$, and multiplying both sides by x yields $ax = xy'\ell$. Given that $m \equiv n \pmod{x}$, there is an integer k such that $m - n = xk$. Multiplying both sides by a, we have $a(m-n) = axk = (xy'\ell)k = (xy'k)\ell$. Since $xy'k$ is an integer, therefore $a(m-n) \equiv 0 \pmod{y}$, as desired.

Armed with these results, we will now solve the desired problem, where we will show that φ_a is well defined if and only if a is a multiple of 3. To begin, assume φ_a is well defined. Let $m, n \in \mathbb{Z}$, where $m \equiv n \pmod{48}$, then since φ_a is well defined, we have $\varphi_a(\overline{m}) = \varphi_a(\overline{n})$. This implies $x^{ma} = x^{na}$, which is equivalent to $x^{a(m-n)} = 1$. Since $|x| = 36$, we can conclude $a(m-n) \equiv 0 \pmod{36}$. Combining this result with $m - n \equiv 0 \pmod{48}$, we can use (i) to conclude that a is a multiple of $36/(36,48) = 36/12 = 3$.

Conversely, now we will show that if a is a multiple of 3, then φ_a is well-defined. To begin, assume a is a multiple of 3. Let $m, n \in \mathbb{Z}$, where $m \equiv n \pmod{48}$. Our aim is to show that $\varphi_a(\overline{m}) = \varphi_a(\overline{n})$. Since a is a multiple of $3 = 48/\gcd(36,48)$, we can use the result in (ii) to say $a(m-n) \equiv 0 \pmod{36}$. Since $|x| = 36$, then $1 = x^{a(m-n)}$, or equivalently, $x^{am} = x^{an}$, i.e., $\varphi_a(\overline{m}) = \varphi_a(\overline{n})$, and therefore φ_a is well defined.

We can note that φ_a satisfies the condition $\varphi_a(\overline{m})\varphi_a(\overline{n}) = x^{am}x^{an} = x^{a(m+n)} = \varphi_a(\overline{m+n}) = \varphi_a(\overline{m} + \overline{n})$ with no further constraint on the value of a. So, if a is a multiple of 3, then φ_a is a well-defined homomorphism.

Finally, we will show that φ_a cannot be a surjective homomorphism. To see why, we remind ourselves that $Z_{36} = \langle x \rangle$, and we consider the element $x \in Z_{36}$ in the co-domain of φ_a. Let a be a multiple of 3. We will show by way of contradiction that x is not in the image of φ_a. Assume x is in the image of φ_a, i.e., there is some $n \in \mathbb{Z}$ such that $\varphi_a(\bar{n}) = x$. But $\varphi_a(\bar{n}) = x^{na}$, so $na \equiv 1 \pmod{36}$. However, this is a contradiction, since according to D&F Exercise 0.3.12, if a and 36 are not relatively prime, then there is no integer n such that $na \equiv 1 \pmod{36}$. Therefore, φ_a cannot be a surjective homomorphism.

D&F Exercise 2.3.11

Find all cyclic subgroups of D_8. Find a proper subgroup of D_8 which is not cyclic.

These are the nontrivial cyclic subgroups of D_8:

- $\langle r \rangle = \{1, r, r^2, r^3\}$
- $\langle r^2 \rangle = \{1, r^2\}$
- $\langle s \rangle = \{1, s\}$
- $\langle sr \rangle = \{1, sr\}$
- $\langle sr^2 \rangle = \{1, sr^2\}$
- $\langle sr^3 \rangle = \{1, sr^3\}$

We can note the non-cyclic subgroup of D_8 from D&F Exercise 2.2.5(b): $\{1, s, r^2, sr^2\}$.

D&F Exercise 2.3.12

Prove that the following groups are not cyclic:

(a) $Z_2 \times Z_2$

(b) $Z_2 \times \mathbb{Z}$

(c) $\mathbb{Z} \times \mathbb{Z}$.

In order to solve these problems, we will show the following results:

(i) *Claim:* Let G_1 and G_2 be arbitrary nontrivial groups. If the product group $G = G_1 \times G_2$ is cyclic, then G is finite.

Proof: Let G_1 and G_2 be arbitrary groups and let G be the product group $G = G_1 \times G_2$. Suppose G is cyclic. We will show G is finite. To begin, because G is cyclic, this means that G can be generated by a single element $G = \langle (x, y) \rangle$, where $x \in G_1$ and $y \in G_2$. We can note that $(x, 1) \in G$ by definition, but since $G = \langle (x, y) \rangle$, then there exists some element $(x, y)^k \in \langle (x, y) \rangle$, where k is an integer, such that $(x, y)^k = (x, 1)$. Since $(x, y)^k = (x^k, y^k)$, this implies $x^{k-1} = 1$ and $y^k = 1$. So, x and y have finite order. Therefore, (x, y) also has finite order, and $\langle (x, y) \rangle = G$ is a finite group.

(ii) *Claim:* The product group $G = Z_m \times Z_n$ is cyclic if and only if $\gcd(m, n) = 1$.

Proof: Assume $G = Z_m \times Z_n$ is cyclic. Let $d = \gcd(m, n)$. We will show $d = 1$. Because G is cyclic, it can be generated by one of its elements, call it (x, y). Here, because x and y must generate all elements of Z_m and Z_n respectively, we must have $|x| = m$ and $|y| = n$. That is, $x^m = 1$ and $y^n = 1$. Next, we can note the following: $(1, 1) = \left((x^m)^{n/d}, (y^n)^{m/d}\right) = (x, y)^{mn/d}$. From this we can see that mn/d must be a multiple of the order of (x, y). Because (x, y) generates all elements of G, and $|G| = mn$, then $|(x, y)| = mn$, so d must be 1.

Conversely, assume $\gcd(m, n) = 1$. We will show G is cyclic. Because G_1 and G_2 are individually cyclic, let x and y be their generators, respectively, i.e., $G_1 = \langle x \rangle$ and $G_2 = \langle y \rangle$, where $|x| = m$ and $|y| = n$. Since G is finite, then there must be some integer k such that $(x, y)^k = (1, 1)$, and by definition the order of (x, y) is the smallest value of k where this condition is met. Since $(1, 1) = (x, y)^k = (x^k, y^k)$, we have $x^k = 1$ and $y^k = 1$, so k must be a common multiple of m and n. So, the order of (x, y) is the smallest common multiple of m and n, i.e., $mn/\gcd(m, n)$. We assumed $\gcd(m, n) = 1$, so the order of (x, y) is therefore mn, i.e., (x, y) generates mn distinct elements. Since there are mn elements in G, therefore (x, y) generates all of G, and thus G is cyclic.

Now back to the problems at hand:

(a) Using the contrapositive of the result in (ii), we can conclude that the group $Z_2 \times Z_2$ is not cyclic, since $\gcd(2, 2) = 2$.

(b) Using the contrapositive of the result in (i), we can conclude that because $Z_2 \times \mathbb{Z}$ is not finite, then it is not cyclic.

(c) Using the contrapositive of the result in (i), we can conclude that because $\mathbb{Z} \times \mathbb{Z}$ is not finite, then it is not cyclic.

D&F Exercise 2.3.15

Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

Using the contrapositive of the result (i) in D&F Exercise 2.3.12, we can conclude that because $\mathbb{Q} \times \mathbb{Q}$ is not finite, then it is not cyclic.

Alternatively, according to Theorem 2.3.7 in D&F, if a group is cyclic then every one of its subgroups is cyclic. The contrapositive of this statement is: if a subgroup is not cyclic then the group is not cyclic. Using this, we can conclude that because $\mathbb{Z} \times \mathbb{Z}$ is a subgroup of $\mathbb{Q} \times \mathbb{Q}$, and we showed that $\mathbb{Z} \times \mathbb{Z}$ is not cyclic in D&F Exercise 2.3.12(c), then $\mathbb{Q} \times \mathbb{Q}$ cannot be cyclic.

D&F Exercise 2.3.16

Assume $|x| = m$ and $|y| = n$. Suppose that x and y commute: $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true if x and y do not commute? Give an example of commuting elements x, y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.

Let G be a group where $x \in G$ has order m, $y \in G$ has order n, and $xy = yx$. We will show that $|xy|$ divides the least common multiple of m and n. To begin, let $d = \gcd(m, n)$. Because $|x| = m$ and $|y| = n$, then $x^m = 1$ and $y^n = 1$. So, because x and y commute, we have $1 = x^m y^n = (x^m)^{n/d}(y^n)^{m/d} = (xy)^{mn/d}$. This implies that that mn/d must be a multiple of $|xy|$. That is, $|xy|$ divides mn/d. Since the least common multiple of m and n is mn/d, therefore $|xy|$ divides the least common multiple of m and n.

On the other hand, this result is not necessarily true if x and y do not commute. For example, consider $x = (12)$ and $y = (23)$. Here, $|(12)| = 2$ and $|(23)| = 2$, so the least common multiple of 2 and 2 is 2. But $|xy| = |(12)(23)| = |(123)| = 3$, which does not divide 2.

Finally, we will show an example of commuting elements x, y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$. Consider the group $\langle r \rangle$, where $|r| = 3$, where all elements of G commute. Let $x = r$ and $y = r^2$, so $|x| = 3$ and $|y| = 3$. The least common multiple of $|x|$ and $|y|$ is 3, which is not equal to $|xy| = |r^3| = |1| = 1$.

D&F Exercise 2.3.19

Show that if H is any group and h is an element of H, then there is a unique homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$.

Let H be a group and let $h \in H$. Define the map $\varphi : \mathbb{Z} \to H$, defined as $\varphi(n) = h^n$.

First, φ is a homomorphism, since $\varphi(m + n) = h^{m+n} = h^m h^n = \varphi(m)\varphi(n)$.

Next, we will show φ is the unique homomorphism that satisfies $\varphi(1) = h$. To do this, suppose there is another homomorphism $\varphi' : \mathbb{Z} \to H$, where $\varphi'(1) = h$. Then we have $\varphi'(n) = \varphi'(1)^n = h^n = \varphi(n)$. Therefore, φ is the unique homomorphism that maps $\mathbb{Z} \to H$ such that $1 \mapsto h$.

D&F Exercise 2.3.21

Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1 + p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ but $(1 + p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. Deduce that $1 + p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Let p be an odd prime and let n be a positive integer. First, we aim to show $(1 + p)^{p^{n-1}} \equiv 1 \pmod{}$

p^n). Using the Binomial theorem, we have:

$$(1+p)^{p^{n-1}} = \sum_{k=0}^{p^{n-1}} \binom{p^{n-1}}{k} p^k \tag{77}$$

$$= \sum_{k=0}^{p^{n-1}} \frac{p^{n-1}!\; p^k}{k!\;(p^{n-1}-k)!} \tag{78}$$

$$= 1 + \sum_{k=1}^{p^{n-1}} \frac{(p^{n-1}-k+1)(p^{n-1}-k+2)\cdots(p^{n-1})p^k}{k!} \tag{79}$$

We can note that the summand in Eq. (79) is an integer, since the binomial coefficient is an integer. Now our aim will be show that the summand in Eq. (79) has at least n powers of p in the numerator. To keep notation simpler, we'll invent an indicator function, call it Φ_p, which is similar to a logarithm, but it only pays attention to the powers of p and nothing else. For example, $\Phi_p(cp^a p^{-b}) = a - b = \Phi_p(p^a) - \Phi_p(p^b)$, so

$$\Phi_p\left(\frac{(p^{n-1}-k+1)(p^{n-1}-k+2)\cdots(p^{n-1})p^k}{k!}\right) = \Phi_p\left((p^{n-1}-k+1)(p^{n-1}-k+2)\cdots(p^{n-1})\right) + \Phi_p(p^k) - \Phi_p(k!) \tag{80}$$

Now we can count the powers of p for the following terms:

- $\Phi_p((p^{n-1}-k+1)(p^{n-1}-k+2)\cdots(p^{n-1})) \geq n-1$.
- $\Phi_p(p^k) = k$
- $\Phi_p(k!) \leq (k-1)/(p-1)$ (cf D&F Exercise 0.2.8). Or, equivalently, $-\Phi_p(k!) \geq -(k-1)/(p-1)$.

and we have the following inequality:

$$\Phi_p\left(\frac{(p^{n-1}-k+1)(p^{n-1}-k+2)\cdots(p^{n-1})p^k}{k!}\right) \geq n+k-1-(k-1)/(p-1) \tag{81}$$

We can note that $k-1-(k-1)/(p-1) \geq 0$ when $k \geq 1$ and $p \geq 3$, so therefore

$$\Phi_p\left(\frac{(p^{n-1}-k+1)(p^{n-1}-k+2)\cdots(p^{n-1})p^k}{k!}\right) \geq n \tag{82}$$

To summarize, the summand in Eq. (79) is an integer and it has at least n powers of p. Therefore, all the terms in the sum (except the leading term, which is 1) in Eq. (79) are congruent to 0 (mod p^n). Therefore, $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$.

Now we will show that $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. Using the Binomial theorem, we have:

$$(1+p)^{p^{n-2}} = \sum_{k=0}^{p^{n-2}} \binom{p^{n-2}}{k} p^k \tag{83}$$

$$= \sum_{k=0}^{p^{n-2}} \frac{p^{n-2}!\; p^k}{k!\;(p^{n-2}-k)!} \tag{84}$$

$$= 1 + p^{n-1} + p^n \frac{(p^{n-2}-1)}{2} + \sum_{k=3}^{p^{n-2}} \frac{(p^{n-2}-k+1)(p^{n-2}-k+2)\cdots(p^{n-2})p^k}{k!} \tag{85}$$

The first term in Eq. (85) is 1, so it's congruent to 1 (mod p^n). The second term is not congruent to 1 (mod p^n). The third term is congruent to 0 (mod p^n), since p raised to any power is odd, so $p^{n-2}-1$ is even, so $(p^{n-2}-1)/2$ is an integer. What remains is to show the remaining terms under the summation sign are all congruent to 0 (mod p^n).

Following the same method as before,

$$\begin{aligned}\Phi_p\left(\frac{(p^{n-2}-k+1)(p^{n-2}-k+2)\cdots(p^{n-2})p^k}{k!}\right) &= \Phi_p\left((p^{n-2}-k+1)(p^{n-2}-k+2)\cdots(p^{n-2})\right) \\ &\quad + \Phi_p(p^k) - \Phi_p(k!) \end{aligned} \tag{86}$$

Now we can count the powers of p for the following terms:

- $\Phi_p((p^{n-2}-k+1)(p^{n-2}-k+2)\cdots(p^{n-2})) \geq n-2$.
- $\Phi_p(p^k) = k$
- $\Phi_p(k!) \leq (k-1)/(p-1)$ (cf D&F Exercise 0.2.8). Or, equivalently, $-\Phi_p(k!) \geq -(k-1)/(p-1)$.

and we have the following inequality:

$$\Phi_p\left(\frac{(p^{n-2}-k+1)(p^{n-2}-k+2)\cdots(p^{n-2})p^k}{k!}\right) \geq n+k-2-(k-1)/(p-1) \tag{87}$$

To simplify this further, we have the following inequality when $k \geq 3$ and $p \geq 3$:

$$\begin{aligned}(k-2)(p-2) &\geq 1 && (88)\\ kp-2k-2p+4 &\geq 1 && (89)\\ kp-k-2p+2 &\geq k-1 && (90)\\ (k-2)(p-1) &\geq k-1 && (91)\\ k-2 &\geq (k-1)/(p-1) && (92)\end{aligned}$$

Therefore,

$$\Phi_p\left(\frac{(p^{n-2}-k+1)(p^{n-2}-k+2)\cdots(p^{n-2})p^k}{k!}\right) \geq n \tag{93}$$

And, like before, the term under the summation sign of Eq. (85) are integers and have at least n factors of p, so they all congruent to 0 (mod p^n).

From these results, we aim to deduce that $1+p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Let a be the order of $1+p$, i.e., $a = |1+p|$. Since $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$, then p^{n-1} is a multiple of a, i.e., there is an integer ℓ such that $a\ell = p^{n-1}$. But since p^{n-1} only has factors of p, then a and ℓ must also only have factors of p. Put another way, we can represent a as $a = p^r$, where r is positive integer, so $(1+p)^{p^r} \equiv 1$, where $r \leq n-1$. We will now show $r = n-1$ by way of contradiction. Assume $r < n-1$. That is, there is some integer s such that $r+s = n-2$. Then we have $1 \equiv (1+p)^{p^r} \equiv \left((1+p)^{p^r}\right)^{p^s} \equiv (1+p)^{p^{r+s}} \equiv (1+p)^{p^{n-2}} \not\equiv 1$, a contradiction. Therefore, $r = n-1$, and $|1+p| = p^{n-1}$.

D&F Exercise 2.3.23

Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2.]

We will show that the group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. To do this, we will utilize Theorem 7 in D&F Section 2.3, which states that given a finite cyclic group of order n, for every a that divides n there is a unique subgroup of order a. So, if a group has more than one subgroup of the same order, then the group cannot be cyclic. So, our aim will be to identify more than one subgroups of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ that have the same order, when $n \geq 3$.

First, we can note that $(\mathbb{Z}/2^n\mathbb{Z})^\times = \{k \in \mathbb{Z} | (k, n) = 1\}$ will contains all odd integers less than 2^n since 2^n only has factors of 2 and odd integers must have at least one odd factor. That is, $(\mathbb{Z}/2^n\mathbb{Z})^\times = \{1, 3, 5, \cdots, 2^n - 1\}$. We identify two such odd integers in this set, i.e., $x_1 := 2^n - 1$ and $x_2 := 2^{n-1} - 1$. First, we can note that neither x_1 nor x_2 are congruent to 1 (mod 2^n) when $n \geq 3$. However, both of these elements square to 1 (mod 2^n):

$$\begin{aligned}
x_1^2 &= (2^n - 1)^2 && (94)\\
&= 2^{2n} - 2(2^n) + 1 && (95)\\
&= (2^n)(2^n - 2) + 1 && (96)\\
&\equiv 1 + 0 \ (\text{mod } 2^n) && (97)\\
&\equiv 1 \ (\text{mod } 2^n) && (98)\\
x_2^2 &= (2^{n-1} - 1)^2 && (99)\\
&= 2^{2(n-1)} - 2(2^{n-1}) + 1 && (100)\\
&= 2^n(2^{n-2} - 1) + 1 && (101)\\
&\equiv 0 + 1 \ (\text{mod } 2^n) && (102)\\
&\equiv 1 \ (\text{mod } 2^n). && (103)
\end{aligned}$$

Therefore, x_1 and x_2 both have order 2 when $n \geq 3$. So, we will always have more than one subgroup of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ of order 2 when $n \geq 3$. Therefore, we can use the contrapositive of Theorem 7 and conclude that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for $n \geq 3$.

D&F Exercise 2.3.25

Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's theorem to prove the same is true for any finite group of order n. (For such k each element has a k^{th} root in G. It follows from Cauchy's Theorem in Section 3.2 that if k is not relatively prime to the order of G then the map $x \mapsto x^k$ is not surjective.)

We will show the following results:

(i) *Claim:* Let $G = \langle x \rangle$, where $|x| = n$, and let k be an integer relatively prime to n. The map $\varphi : G \mapsto G$, defined as $\varphi(x) = x^k$, is surjective.

Proof: Because $(k, n) = 1$, then there exists integers a and b such that $ak + bn = 1$. Let $x^j \in G$. Because $x^n = 1$, we can note $\varphi(x^{aj}) = x^{ajk} = x^{j(1-bn)} = x^j(x^n)^{-jb} = x^j$. Therefore, φ is surjective.

(ii) *Claim:* Let G be a finite group of order n and let k be an integer that is relatively prime to n. The map $\varphi : G \mapsto G$, defined as $\varphi(g) = g^k$, is surjective.

Proof: Let $g \in G$. The group $\langle g \rangle$ is a subgroup of G. Let $m = |\langle g \rangle|$, so $g^m = 1$. According to Lagrange's theorem, $n = rm$ for some $r \in \mathbb{Z}$, so $g^n = g^{rm} = (g^m)^r = 1$. Now, since $(k, n) = 1$, then there exists integers a and b such that $ak + bn = 1$. So, we have $\varphi(g^a) = g^{ak} = g^{1-bn} = g(g^n)^{-b} = g$. Therefore, φ is surjective.

XIII. SUBGROUPS GENERATED BY SUBSETS OF A GROUP

D&F Exercise 2.4.2

Prove that if A is a subset of B then $\langle A\rangle \leq \langle B\rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A\rangle = \langle B\rangle$.

Let A be a subset of B. We will show $\langle A\rangle \leq \langle B\rangle$. Here, $\langle B\rangle$ is a group that contains B (cf p. 62 of D&F). Since all elements of A are contained B, then all elements of A are also contained in $\langle B\rangle$. So, by Proposition 2.8 (p. 62 of D&F), $\langle A\rangle$ is a subgroup of $\langle B\rangle$.

The following is an example where $A \subseteq B$ and $A \neq B$ but $\langle A\rangle = \langle B\rangle$. Let $A = \{(12), (123)\}$ and $B = \{(23), (123)\}$. Here, we have $A \subseteq B$ and $A \neq B$. But both $\langle A\rangle$ and $\langle B\rangle$ generate all of S_3. To verify this, we can confirm that A generates the rest of the elements in S_3:

$$(12)(12) = 1 \tag{104}$$
$$(12)(123) = (23) \tag{105}$$
$$(123)(123) = (132) \tag{106}$$
$$(123)(12) = (13) \tag{107}$$

and likewise B also generates the rest of the elements in S_3:

$$(23)(23) = 1 \tag{108}$$
$$(23)(123) = (13) \tag{109}$$
$$(123)(123) = (132) \tag{110}$$
$$(123)(23) = (12) \tag{111}$$

D&F Exercise 2.4.6

Prove that the subgroup of S_4 generated by (12) and $(12)(34)$ is a noncyclic group of order 4.

The subgroup of S_4 generated by (12) and $(12)(34)$ can be easily found since both (12) and $(12)(34)$ both have only order 2:

$$(12)(12) = 1 \tag{112}$$
$$(12)(34)(12)(34) = 1 \tag{113}$$
$$(12)(12)(34) = (34) \tag{114}$$
$$(12)(34)(12) = (34) \tag{115}$$

The set $A = \{1, (12), (12)(34), (34)\}$ is closed under multiplication and inverses, so indeed this is the subgroup generated by (12) and $(12)(34)$. We know A is not cyclic since it has more than one element of order 2 (cf Theorem 7 in D&F Section 2.3).

D&F Exercise 2.4.7

Prove that the subgroup of S_4 generated by (12) and $(13)(24)$ is isomorphic to the dihedral group of order 8.

We will show that the subgroup of S_4 generated by (12) and $(13)(24)$ is isomorphic to D_8. First, we

can note that s and rs generate of D_8, which can be easily verified:

$$\begin{aligned}(s)^2 &= 1 && (116)\\ (rs)(s) &= r && (117)\\ (rs)(s)(rs)(s) &= r^2 && (118)\\ (s)(rs) &= r^{-1} = r^3 && (119)\\ (rs)(s)(rs) &= r^2 s && (120)\\ (s)(rs)(s) &= sr = r^{-1}s = r^3 s && (121)\end{aligned}$$

So, we have $D_8 = \langle s, rs\rangle$. Now we can see what subgroup is generated by (12) and (13)(24):

$$\begin{aligned}(12)^2 &= 1 && (122)\\ (12)((13)(24)) &= (1324) && (123)\\ ((13)(24))(12) &= (1423) && (124)\\ (12)((13)(24))(12) &= (14)(23) && (125)\\ ((13)(24))(12)((13)(24)) &= (34) && (126)\\ ((13)(24))(12)((13)(24))(12) &= (12)(34) && (127)\end{aligned}$$

So, $\langle (12), (13)(24)\rangle$ is a subgroup of 8 elements.

Define the map $\varphi : D_8 \to \langle (12), (13)(24)\rangle$ defined as $s^i(rs)^j \mapsto (12)^i((13)(24))^j$. First, we can note that the generators are mapped to each other, i.e., $\varphi(s) = (12)$ and $\varphi(rs) = (13)(24)$. Then we can note that the relations of D_{2n}, i.e., $s^2 = 1$ and $(rs)^2 = 1$ also map to the identity, i.e., $\varphi(s^2) = 1$ and $\varphi((rs)^2) = 1$. Therefore, φ is a homomorphism. Furthermore, φ is an isomorphism, because there is a one-to-one correspondence between the element of D_8 and $\langle (12), (13)(24)\rangle$, which can be seen in the table below:

D_8	$\varphi(D_8)$
1	1
r	(1423)
r^2	(12)(34)
r^3	(1324)
rs	(13)(24)
r^2s	(34)
r^3s	(14)(23)

D&F Exercise 2.4.8

Prove that $S_4 = \langle (1234), (1243)\rangle$.

Let $A = \langle (1234), (1243)\rangle$. We will show that $A = S_4$. First we can note that $\{(1234), (1243)\} \in S_4$, $|S_4| = 24$, and $A \leq S_4$, so by Lagrange's Theorem, $|A|$ divides 24. We can note that $\langle (1234)\rangle$ is a subgroup of order 4. So, 4 divides $|A|$. Also, $(1234)(1243) = (142)$, and $\langle (142)\rangle$ is a subgroup of order 3. So, 3 divides $|A|$. Lastly, we can note $(1234)^2 = (13)(24)$ and $(1234)(1243)^3(1234) = (12)$, and we know from D&F Exercise 2.4.7 that (13)(24) and (12) generate a subgroup of order 8. So, 8 divides $|A|$. Therefore, $|A|$ must be equal to 24, i.e., all the elements of S_4, and thus $A = S_4$.

D&F Exercise 2.4.11

Show that $SL_2(\mathbb{F}_3)$ and S_4 are two non-isomorphic groups of order 24.

Stumped. Could it be possible to pass over this problem?

D&F Exercise 2.4.15

Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

We will show that there exists a subgroup of $\mathbb{Q}$ that is not cyclic. Consider the set $A = \{a/2^b | a \in \mathbb{Z}, b \in \mathbb{Z}_+\}$. Here, A is nonempty and $A \subseteq \mathbb{Q}$. To show that A is a subgroup under addition, let $a, b \in \mathbb{Z}$ and $c, d \in \mathbb{Z}_+$, and we can note $a/2^b + c/2^d = (2^d a + 2^b c)/(2^{b+d}) \in A$, since the numerator is an integer and the denominator is a power of 2, so the set is closed under addition. Also, given an element $a/2^b \in A$, its inverse is $-a/2^b \in A$, so the set is closed under inverses. Finally, the identity, i.e., 0, is in A. So, A is a subgroup of $\mathbb{Q}$. However, A is a proper subgroup of $\mathbb{Q}$, since, for example, $1/7 \notin A$ but $1/7 \in \mathbb{Q}$.

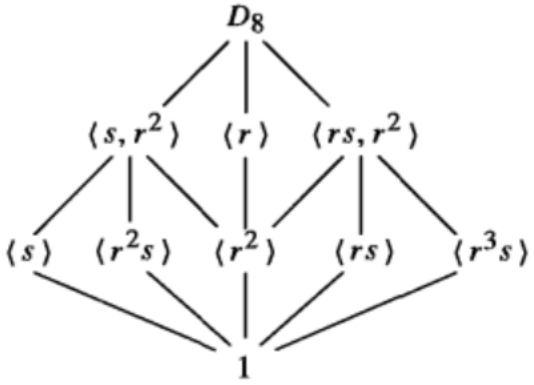
Finally, we will show that A is not cyclic by way of contradiction. Assume A is cyclic. Then it would be generated by one of its elements. Let the generator be $m/2^n$, where $m \in \mathbb{Z}$ and $n \in \mathbb{Z}_+$. Consider the element $m/2^{n+1} \in A$. Since $m/2^n$ generates A, then there is some integer k such that $km/2^n = m/2^{n+1}$. This implies $k = 1/2$, which is a contradiction, since k must be an integer. Therefore, A is a not cyclic.

XIV. THE LATTICE OF SUBGROUPS OF A GROUP

D&F Exercise 2.5.4

Use the given lattice to find all pairs of elements that generate D_8 (there are 12 pairs).

See below the lattice of D_8.



Our goal is to find all pairs of elements that generate D_8. As an example, the subgroups generated by r and s are not subgroups of each other, which can be seen from the lattice. Furthermore, the smallest subgroup of which $\langle s \rangle$ and $\langle r \rangle$ are both subgroups is D_8. Therefore, $\langle s, r \rangle$ generates D_8. The other 11 pairs that follow this same patters are [note: since $\langle r \rangle = \langle r^3 \rangle$, then for every time r is one of the generators of D_8, so will be r^3]: $\langle r, r^2 s \rangle$, $\langle r, rs \rangle$, $\langle r, r^3 s \rangle$, $\langle s, rs \rangle$, $\langle s, r^3 s \rangle$, $\langle r^2 s, rs \rangle$, $\langle r^2 s, r^3, s \rangle$, $\langle r^3, s \rangle$ $\langle r^3, r^2 s \rangle$, $\langle r^3, rs \rangle$, $\langle r^3, r^3 s \rangle$.

D&F Exercise 2.5.9

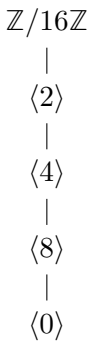
Draw the lattices of subgroups of the following groups:

(a) $\mathbb{Z}/16\mathbb{Z}$

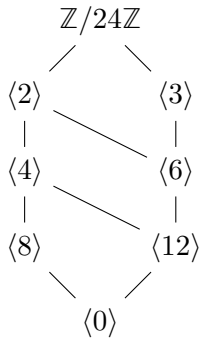
(b) $\mathbb{Z}/24\mathbb{Z}$

(c) $\mathbb{Z}/48\mathbb{Z}$ *[See Exercise 2.3.6]*

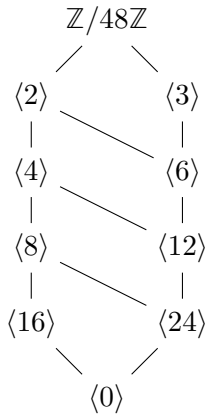
(a) Below is the lattice for $\mathbb{Z}/16\mathbb{Z}$:



(b) Below is the lattice for $\mathbb{Z}/24\mathbb{Z}$:



(c) Below is the lattice for $\mathbb{Z}/48\mathbb{Z}$:



D&F Exercise 2.5.10

Classify groups of order 4 by proving that if $|G| = 4$ then $G \cong Z_4$ or $G \cong V_4$. [See D&F Exercise 1.1.36.]

Let G be a group of order 4. We will show that when G is cyclic then $G \cong Z_4$, and when G is not cyclic then $G \cong V_4$.

To begin, first assume G is cyclic. This means G has an element of order 4 that generates 4 distinct elements, i.e., the entire group G. So, in this case, $G \cong Z_4$.

Now assume G is not cyclic. This means there is no element in G of order 4. To proceed, we can explicitly label the distinct group elements as $G = \{1, a, b, c\}$. What is the order of the subgroup $\langle a \rangle$? From Lagrange's theorem, $\langle a \rangle$ must divide 4, but it cannot be 1, since $a \neq 1$, and it cannot be 4, since we assumed G is not cyclic. So the order of $\langle a \rangle$ must be 2, and therefore a must have order 2. Using the same argument, b and c must also have order 2. Now, we will show that the rest of the multiplication rules of G are determined. For example, can $ab = a$? It cannot, since $b \neq 1$. Can $ab = b$? It cannot, since $a \neq 1$. Can $ab = 1$? It cannot, since $a^2 = 1$, and $a \neq b$. So, $ab = c$. The same argument can be followed to determine that $ba = c$, $ac = ca = b$ and $bc = cb = a$. This yields the multiplication rules for V_4, so $G \cong V_4$ (cf D&F Exercise 1.1.36).

XV. QUOTIENT GROUPS AND HOMOMORPHISMS: DEFINITIONS AND EXAMPLES

D&F Exercise 3.1.1

Let $\varphi : G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\varphi^{-1}(E) \leq G$ (i.e., the preimage or pullback of a subgroup under a homomorphism is a subgroup). If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker \varphi \trianglelefteq G$.

Let $\varphi : G \to H$ be a homomorphism, let E be a subgroup of H, and let $N = \varphi^{-1}(E)$.

First, we will show that $N \leq G$. We begin by noting that N is nonempty, since E is nonempty. Now, let $x, y \in N$. Here, $\varphi(x) = a$ and $\varphi(y) = b$, where $a, b \in E$, by definition. Because φ is a homomorphism and $ab^{-1} \in E$ since E is a subgroup, we have $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = ab^{-1} \in E$. So, $xy^{-1} \in N$, by definition. Since this follows for any choice for x and y, then $N \leq G$ according to the Subgroup Criterion.

Next, assume $E \trianglelefteq H$. We will show $N \trianglelefteq G$. To begin, let $g \in G$. Here, $\varphi(g) = a$, where $a \in H$. Now, since E is a normal subgroup, we have $\varphi(gNg^{-1}) = \varphi(g)\varphi(N)\varphi(g)^{-1} = aEa^{-1} = E$. So, $gNg^{-1} \in N$, by definition. This is the condition for normal subgroup, i.e., $N \trianglelefteq G$, as desired.

Finally, we can use the above result to deduce $\ker \varphi \trianglelefteq G$. So, if we let $E = \{1\}$, then $E \trianglelefteq H$ since the trivial subgroup is always normal. Furthermore in this case, $N = \varphi^{-1}(E = \{1\}) = \ker \varphi$. So, using the result in the previous paragraph, we have $\ker \varphi \trianglelefteq G$, as desired.

Alternatively, one can show that $\ker \varphi \trianglelefteq G$ in a straight-forward way. Let $g \in G$ and $x \in \ker \varphi$. Then we have $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)1\varphi(g)^{-1} = 1$. So $g \ker \varphi g^{-1} \subseteq \ker \varphi$ for any $g \in G$. Therefore, $\ker \varphi \trianglelefteq G$.

D&F Exercise 3.1.2

Let $\varphi : G \to H$ be a homomorphism of groups with kernel K and let $a, b \in \varphi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b, i.e., $X = \varphi^{-1}(a)$, $Y = \varphi^{-1}(b)$. Fix an element u of X (so $\varphi(u) = a$). Prove that if $XY = Z$ in the quotient group G/K and w is any member of Z, then there is some $v \in Y$ such that $uv = w$. [Show $u^{-1}w \in Y$.]

Let $\varphi : G \to H$ be a well-defined homomorphism with kernel K. Let $a, b \in \varphi(G)$, such that $X \in G/K$ is the fiber above a and $Y \in G/K$ is the fiber above b. Assume that $XY = Z$ in G/K, fix $u \in X$, and let $w \in Z$. We will show that there exists a $v \in Y$ where $uv = w$, i.e., that $u^{-1}w \in Y$.

To begin, since $XY = Z$ in G/K, we can note that because XY and Z are sets in G, and because φ is well-defined, that $\varphi(XY) = \varphi(Z)$. Because φ is a homomorphism, this implies $\varphi(X)\varphi(Y) = \varphi(Z)$, i.e., $ab = \varphi(Z)$. This means for any $z \in Z$, then $\varphi(z) = ab$. Now we can note: $\varphi(u^{-1}w) = \varphi(u)^{-1}\varphi(w) = a^{-1}(ab) = b$. Therefore, $u^{-1}w \in Y$, by definition.

D&F Exercise 3.1.3

Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

Let A be an abelian group and let B be a subgroup of A. To begin, we first prove a preliminary result [cf Example 2 in Section 3.1 of D&F]:

(i) *Claim:* Let H be a subgroup of G. If G is abelian, then H is a normal subgroup of G.

Proof: This follows from Theorem 6(3) in Section 3.1 in D&F, which states that if $N \leq G$, and $gN = Ng$ for all $g \in G$, then $N \trianglelefteq G$. In our case, since $H \leq G$ and $gH = Hg$ for all $g \in G$ since G is abelian, therefore $H \trianglelefteq G$, as desired.

Using (i), we can conclude that because A is abelian, then $B \trianglelefteq A$. So, A/B is a quotient group.

We will now show that A/B is also abelian. Let $\pi : A \to A/B$ be the natural projection homomorphism. Because π is surjective, this means that for every $X \in A/B$, there exists an $a \in A$ such that $\pi(a) = X$. Using this fact, let $X, Y \in A/B$ and $a_1, a_2 \in A$ such that $\pi(a_1) = X$ and $\pi(a_2) = Y$. So, because π is a homomorphism and all elements in A commute, we have $XY = \pi(a_1)\pi(a_2) = \pi(a_1a_2) = \pi(a_2a_1) = \pi(a_2)\pi(a_1) = YX$. Since the choices of X and Y were arbitrary, then we can conclude that A/B is abelian.

Now we will show an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian. Example 3 in Section 3.1 of D&F provides an example of this, where $G = D_8$ and $N = \{1, r^2\}$. The text shows that $G/N \cong V_4$, which is an abelian group.

D&F Exercise 3.1.5

Use [D&F Exercise 3.1.4, which proved that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$] to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$ (and gN has infinite order if no such positive integers exists). Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

Let G/N be a quotient group. If it exists, let n be the smallest positive integer such that $g^n \in N$. We will show that the order of gN is n. To begin, suppose $|gN| = \alpha$. This means α is the smallest positive integer such that $(gN)^\alpha = N$. Using D&F Exercise 3.1.4, this implies $g^\alpha N = N$. Since N is a subgroup, the relation $g^\alpha N = N$ implies $g^\alpha \in N$. Since α is the smallest positive integer where this holds, then $\alpha = n$, as desired.

On the other hand, suppose there is no positive integer n such that $g^n \in N$. We will show that there is no positive integer k such that $(gN)^k = 1$. We will proceed by contradiction. Assume there is a positive integer k such that $(gN)^k = N$. Then $(gN)^k = g^kN = N$, so $g^k \in N$. But this is a contradiction, since we assumed there is no such positive integer. Therefore, there is no positive integer k such that $(gN)^k = 1$.

In order to provide an example that the order of $gN \in G/N$ may be strictly smaller than the order of $g \in G$, consider when $G = D_8$, $N = \{1, r^2\}$, and $g = r$. Here, $|r| = 4$. But the element $gN = r\{1, r^2\}$ has order 2, since $r \neq 1$ and $r^2 = 1$, and by using the above result, then $|rN| = 2$.

D&F Exercise 3.1.10

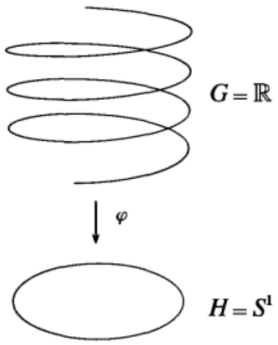
Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\bar{a}) = \bar{a}$. Show that this is a well defined, surjective homomorphism and describe its fibers and kernel explicitly (showing that φ is well defined involves the fact that $\bar{a}$ has a different meaning in the domain and range of φ).

Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\bar{a}) = \bar{a}$. First, we will show that φ is well defined. Let a and b be representatives of the same congruence class in $\mathbb{Z}/8\mathbb{Z}$, i.e., $\overline{a} = \overline{b}$. This implies $\overline{a} = \overline{b + 8k}$, where k is an integer. Then we have $\varphi(\overline{a}) = \varphi(\overline{b + 8k}) = \overline{b + 8k} = \overline{b + 4(2k)} = \overline{b} = \varphi(\overline{b})$. So, φ is well defined. Also, φ is a homomorphism, since $\varphi(\overline{a} + \overline{b}) = \varphi(\overline{a + b}) = \overline{a + b} = \overline{a} + \overline{b} = \varphi(\overline{a}) + \varphi(\overline{b})$. Finally, φ is surjective since any $\overline{a} \in \mathbb{Z}/4\mathbb{Z}$, we have $\varphi(\overline{a}) = \overline{a}$.

Here, we have $\ker\varphi = \{\overline{0}, \overline{4}\}$ and its fibers are $\varphi^{-1}(\overline{0}) = \{\overline{0}, \overline{4}\}$, $\varphi^{-1}(\overline{1}) = \{\overline{1}, \overline{5}\}$, $\varphi^{-1}(\overline{2}) = \{\overline{2}, \overline{6}\}$, and $\varphi^{-1}(\overline{3}) = \{\overline{3}, \overline{7}\}$.

D&F Exercise 3.1.12

Let G be the additive group of real numbers, let H be the multiplication group of complex numbers of absolute value 1 (the unit circle S^1 in the complex plane) and let $\varphi : G \to H$ be the homomorphism $\varphi : r \mapsto e^{2\pi i r}$. Draw the points on the real line which lie in the kernel of φ. Describe similarly the elements in the fibers of φ above the points -1, i, and $e^{4\pi i/3}$ of H. (Figure 1 of the text for this homomorphism φ is usually depicted using the following diagram.)



The points on the real line that correspond with the kernel of φ are those where $\varphi(r) = 1$, i.e., $\ker\varphi = \mathbb{Z}$. And we can also note the following fibers: $\varphi^{-1}(-1) = \varphi^{-1}(e^{2\pi i(1/2)}) = 1/2 + \mathbb{Z}$, $\varphi^{-1}(i) = \varphi^{-1}(e^{2\pi i(1/4)}) = 1/4 + \mathbb{Z}$, and $\varphi^{-1}(e^{4\pi i/3}) = \varphi^{-1}(e^{2\pi i(2/3)}) = 2/3 + \mathbb{Z}$.

D&F Exercise 3.1.21

Let $G = Z_4 \times Z_4$ be given in terms of the following generators and relations: $G = \langle x, y | x^4 = y^4 = 1, xy = yx\rangle$. Let $\overline{G} = G/\langle x^2y^2\rangle$ (note that every subgroup of the abelian group G is normal).

(a) Show that the order of $\overline{G}$ is 8.

(b) Exhibit each element of $\overline{G}$ in the form $\overline{x}^a\overline{y}^b$, for some integers a and b.

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

(d) Prove that $\overline{G} \cong Z_4 \times Z_2$.

Let $G = Z_4 \times Z_4$. First, a perhaps-too-detailed point: the groups $Z_4 \times Z_4$ and $\langle x, y | x^4 = y^4 = 1, xy = yx\rangle$ are not the same. In the former case, you have a product of two cyclic groups, where each are individually abelian, one generated by x and the other generated by y. In the latter case, you have a

non-product group, with two generators x and y, which commute with each other. But these groups are isomorphic, i.e., $Z_4 \times Z_4 = \{(x,y)|x^4 = 1, y^4 = 1\} \cong \langle x, y|x^4 = y^4 = 1, xy = yx\rangle$, which we state without proof. In this problem, we'll have G refer to the latter representation.

Let $\overline{G} = G/\langle x^2y^2\rangle$. First, we can note that since $x^4 = y^4 = 1$, that $\langle x^2y^2\rangle = \{1, x^2y^2\}$. In the answers to this exercise, we refer to the table below

$\overline{g} \in \overline{G}$	cosets of $N = \langle x^2y^2\rangle$ in G	order
$\overline{1}$	$N,\ x^2y^2N$	1
$\overline{x}$	$xN,\ x^3y^2N$	4
$\overline{x}^2$	$x^2N,\ y^2N$	2
$\overline{x}^3$	$x^3N,\ xy^2N$	4
$\overline{y}$	$yN,\ x^2y^3N$	4
$\overline{x}\ \overline{y}$	$xyN,\ x^3y^3N$	2
$\overline{x}^2\overline{y}$	$x^2yN,\ y^3N$	4
$\overline{x}^3\overline{y}$	$x^3yN,\ xy^3N$	4

(128)

We will show the following:

(a) The order of $\overline{G}$ is 8, as can be seen from the above table.

(b) The elements of $\overline{G}$ are exhibited in the form $\overline{x}^a\overline{y}^b$, for some integers a and b, the above table.

(c) The order of each element in (b) can be found in the table.

(d) *Claim*: $\overline{G} \cong Z_4 \times Z_2$.

Proof: From the above table, it can be verified that the multiplication rules on $\overline{G}$ are consistent with the following presentation: $\overline{G} = \langle \overline{x}, \overline{y}|\overline{x}^4 = (\overline{xy})^2 = 1, \bar{x}\bar{y} = \bar{y}\bar{x}\rangle$. It is straightforward to verify that $\overline{G} = \langle \overline{x}, \overline{xy}\rangle$. This presentation is isomorphic to $Z_4 \times Z_2 = \{(\overline{x}, \overline{xy})|\overline{x}^4 = 1, (\overline{xy})^2 = 1\}$.

D&F Exercise 3.1.22a

Prove that if H and K are normal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G.

Let G be a group with normal subgroups H and K. We will show that $H \cap K$ is also a normal subgroup of G. First, since H and K are subgroups, then $H \cap K$ is a subgroup (cf D&F Exercise 2.1.10a). Let $n \in H \cap K$, so $n \in H$ and $n \in K$. Let $g \in G$. Because H and K are both normal subgroups, we have $gng^{-1} \in H$ and $gng^{-1} \in K$, by definition. Therefore, $gng^{-1} \in H \cap K$. Since this holds for all $g \in G$, then $H \cap K$ is a normal subgroup of G (cf D&F Theorem 3.1.6(5)).

D&F Exercise 3.1.36

Prove that if $G/Z(G)$ is cyclic then G is abelian. [If $G/Z(G)$ is cyclic with generator $xZ(G)$, show that every element of G can be written in the form x^az for some integer $a \in \mathbb{Z}$ and some element $z \in Z(G)$.]

Let G be a group. Suppose $\overline{G} = G/Z(G)$ is cyclic. We will show that G is abelian. To begin, note that elements of $\overline{G}$ can be represented as $gZ(G)$, where $g \in G$ is some representative of each coset of $Z(G)$ in G. Assume $\overline{G}$ is cyclic, and let $xZ(G)$ be its generator, i.e., $\overline{G} = \langle xZ(G)\rangle$. So, all elements of $\overline{G}$ can be represented as $(xZ(G))^a = x^aZ(G)$ (cf D&F Exercise 3.1.4), where a is an integer.

Let $g_1, g_2 \in G$. Since all elements of G are in some coset of $Z(G)$ in G, then there exist $a_1, a_2 \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$ such that $g_1 = x^{a_1}z_1$ and $g_2 = x^{a_2}z_2$. So, since z_1 and z_2 commute with all elements in G,

we have $g_1g_2 = x^{a_1}z_1x^{a_2}z_2 = x^{a_2}z_2x^{a_1}z_1 = g_2g_1$. Since this holds for all pairs of elements in G, then G is abelian.

D&F Exercise 3.1.37

Let A and B be groups. Show that $\{(a,1)|a \in A\}$ is a normal subgroup of $A \times B$ and the quotient of $A \times B$ by this subgroup is isomorphic to B.

Let A and B be groups and $N = \{(a,1)|a \in A\}$. We will show the following:

(a) *Claim*: $N \trianglelefteq (A \times B)$.

Proof: Let $n = (a,1) \in N$, and let $g = (x,y) \in A \times B$. Note that $(x,y)^{-1} = (x^{-1},y^{-1})$. Then we have $gng^{-1} = (x,y)(a,1)(x^{-1},y^{-1}) = (xax^{-1},1)$. Since A is closed under multiplication, we have $xax^{-1} \in A$, so $gng^{-1} = (xax^{-1},1) \in N$. Since this holds for all $g \in A \times B$, then $N \trianglelefteq (A \times B)$.

(b) *Claim*: $(A \times B)/N \cong B$.

Proof: We begin by discussing the structure of the cosets of N in the group $(A \times B)$. Here, we can use the shorthand that $N = (A,1)$. Now, given an element $(a,b) \in A \times B$, we have the coset $(a,b)N = (A,b)$. This notation emphasizes the point that it is the element b that identifies the coset. Now we will proceed to show that there exists an isomorphism between $(A \times B)/N$ and B.

Let $\varphi : (A \times B)/N \to B$, where $\varphi((A,b)) = b$. First, we will show φ is well defined. Let (a_1,b) and (a_2,b) be elements of the same coset of N in $A \times B$. Then we can note that $\varphi((a_1,b)N) = \varphi((a_2,b)N)$ implies $\varphi((A,b)) = \varphi((A,b))$. Therefore, φ is well defined.

Next, we will show that φ is a homomorphism. Let $b_1, b_2 \in B$. We can note $\varphi((A,b_1))\varphi((A,b_1)) = b_1b_2 = \varphi((A,b_1b_2)) = \varphi((A,b_1)(A,b_2))$. Therefore, φ is a homomorphism.

Finally, we will show that φ is a bijection. First, we note that φ is injective since any two distinct elements in the domain, e.g., (A,b_1) and (A,b_2) where $b_1 \neq b_2$, will be mapped to different elements in the range, i.e., b_1 and b_2, respectively. Therefore, φ is injective. Furthermore, given any element $b \in B$, the preimage $\varphi^{-1}(b) = (A,b)$ is indeed a coset of N. Therefore, φ is surjective. Since φ is both injective and surjective, therefore it is bijective.

Since we have shown that φ is a well-defined bijective homomorphism, it is therefore an isomorphism. So, $(A \times B)/N \cong B$, as desired.

D&F Exercise 3.1.42

Assume both H and K are normal subgroups of G with $H \cap K = \{1\}$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$. [Show $x^{-1}y^{-1}xy \in H \cap K$.]

Let G be a group with normal subgroups H and K. Let $N = H \cap K$, $x \in H$, and $y \in K$. We will begin by showing the following result:

(i) *Claim*: $x^{-1}y^{-1}xy \in N$.

Proof: Because H is a normal subgroup, $y^{-1}xy \in H$. Since $x^{-1} \in H$, then also $x^{-1}(y^{-1}xy) \in H$. Because K is a normal subgroup, then $y^{-1} \in K$ and $x^{-1}y^{-1}x \in K$. Then also $(x^{-1}y^{-1}x)y \in K$. Since $x^{-1}y^{-1}xy \in H$ and $x^{-1}y^{-1}xy \in K$, then $x^{-1}y^{-1}xy \in H \cap K = N$, as desired.

Now, suppose $N = H \cap K = \{1\}$, then according to (i), we have $x^{-1}y^{-1}xy = 1$, i.e., $xy = yx$. This follows for all elements of H and K.

XVI. MORE ON COSETS AND LAGRANGE'S THEOREM

D&F Exercise 3.2.4

Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$.

Let G be a group, where $|G| = pq$ and p and q are primes. We will show that either G is abelian or $Z(G) = 1$. We will consider separately the cases when G is abelian or non-abelian.

First, if G is abelian, we are done.

On the other hand, if G is non-abelian, then we will show that $Z(G) = 1$. In this case, we can note that $Z(G)$ is a normal subgroup of G, so by Lagrange's theorem, $|Z(G)|$ divides $|G|$. This mean $|Z(G)|$ can either be pq, p, q, or 1. We will consider each of these cases:

- Suppose $|Z(G)| = pq$. Since there are only pq elements in G, this implies $Z(G) = G$. By the definition of the centralizer, this means G is abelian, which contradicts our assumption that G is non-abelian. Therefore $|Z(G)| \neq pq$.
- Suppose $|Z(G)| = p$. We have $|G/Z(G)| = |G|/|Z(G)|$ (cf D&F Sec. 3.2), so therefore $|G/Z(G)| = q$. But if $|G/Z(G)|$ is prime, then $G/Z(G)$ is cyclic (cf D&F Corollary 3.10), and if $G/Z(G)$ is cyclic, then G is a abelian (cf D&F Exercise 3.1.36), which contradicts our assumption that G is non-abelian. Therefore $|Z(G)| \neq p$.
- Suppose $|Z(G)| = q$. The same argument as above follows with the roles of p and q reversed, so we can conclude $Z(G) \neq q$.

The only option left is $Z(G) = 1$, as desired.

D&F Exercise 3.2.6

Let $H \leq G$ and let $g \in G$. Prove that if the right coset Hg equals some left coset of H in G then it equals the left coset gH and g must be in $N_G(H)$.

Let $H \leq G$ and let $g \in G$. We will show that if $Hg = g'H$, where $g' \in G$, then $Hg = gH$. To begin, suppose $Hg = g'H$ for some $g' \in G$. We can note that because $1 \in H$, then $g \in Hg$. Then $g \in Hg = g'H$, so there is some $h \in H$ such that $g = g'h$. This implies $g' = gh^{-1}$. But now $g'H = gh^{-1}H = gH$. Therefore $Hg = gH$, as desired. From this, we can deduce g commutes with all elements in H, so $g \in N_G(H)$, by definition.

D&F Exercise 3.2.8

Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = \{1\}$.

Let G be a group with subgroups H and K whose orders are relatively prime. We will show that $H \cap K = \{1\}$. To begin, we can note that both H and K are subgroups, so their intersection at least contains the identity, i.e., their intersection is not empty. Let $x \in H \cap K$. Here, $\langle x \rangle$ is a subgroup of both H and K. From Lagrange's theorem, this means $|x|$ divides both the order of H and the order of K. But since the orders of H and K are relatively prime, then $|x| = 1$, which means x can only be the identity. Therefore, $H \cap K = \{1\}$.

D&F Exercise 3.2.14

Prove that S_4 does not have a normal subgroup of order 8 or a normal subgroup of order 3.

We will show the following:

(a) *Claim*: S_4 does not have a normal subgroup of order 8.

Proof: We will proceed by contradiction. Assume S_4 has a normal subgroup N with $|N| = 8$. Interestingly, we can note from D&F Exercise 1.3.4 that S_4 has 9 elements of order 2. But N is of order 8, so N cannot contain all elements of order 2. Let σ be the element of order 2 not contained in N. Here, $\langle\sigma\rangle = \{1, \sigma\}$ is a subgroup of order 2 where $N \cap \langle\sigma\rangle = \{1\}$. Because N is normal, we have $N\langle\sigma\rangle \leq G$ (cf D&F Corollary 3.15), and since $N \cap \langle\sigma\rangle = \{1\}$ then $|N\langle\sigma\rangle| = |N||\langle\sigma\rangle|$ (cf D&F Proposition 3.13), i.e., $|N\langle\sigma\rangle| = 16$. According to Lagrange's theorem, 16 must divide 24. This is not true. Therefore, S_4 does not have a normal subgroup of order 8.

(b) *Claim*: S_4 does not have a normal subgroup of order 3.

Proof: We will proceed by contradiction. Assume S_4 has a normal subgroup N with $|N| = 3$. Since $N \leq 3$, and 3 is prime, then N is cyclic (cf D&F Corollary 3.10), i.e., it is generated by one element. From D&F Exercise 1.3.4, we can see there are 8 such elements of S_4 with order 3. So, N must be generated by one of these, call it x, and we can denote $N = \{1, x, x^2\}$. Now, there are enough elements of order 3 in S_4 such that we can always pick another, call it x', where $N \neq H = \{1, x', (x')^2\}$. Here, $|H| = 3$ and $N \cap H = \{1\}$. As an example, if $N = \langle(123)\rangle$, then we can pick $H = \langle(234)\rangle$. Since N is normal, we have $NH \leq G$ (cf D&F Corollary 3.15), and since $N \cap H = \{1\}$ then $|NH| = |N||H|$ (cf D&F Proposition 3.13), i.e., $|NH| = 9$. According to Lagrange's theorem, 9 must divide 24. This is not true. Therefore S_4 does not have a normal subgroup of order 3.

D&F Exercise 3.2.15

Let $G = S_n$ and for fixed $i \in \{1, 2, \cdots, n\}$ let G_i be the stabilizer of i. Prove that $G_i \cong S_{n-1}$.

Let $G = S_n$ and for fixed $i \in \{1, 2, \cdots, n\}$ let G_i be the stabilizer of i. We will show $G_i \cong S_{n-1}$. To begin, we can note that $G_i \leq S_n$ (cf D&F Exercise 1.7.4). Specifically, G_i contains all elements of S_n that leave the position of i fixed, i.e., it is the set of permutations on all the elements other than i. Therefore $|G_i| = n - 1$. Now, G_i has the same order as S_{n-1}, and both are permutations on $n - 1$ elements, so there is a natural bijection between them. Therefore $G_i \cong S_{n-1}$.

D&F Exercise 3.2.16

Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's Little Theorem: if p is a prime then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.

Let p be a prime and $a \in \mathbb{Z}$. We will show $a^p \equiv a \pmod{p}$. To begin, we remind ourselves that $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/p\mathbb{Z} \,|\, \gcd(a, p) = 1\}$. Here, p is prime, so $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$, and the order of $(\mathbb{Z}/p\mathbb{Z})^\times$ is $p - 1$. We denote $\overline{a} \equiv a \pmod{p}$, and we will consider the following two cases:

- $\overline{a} = \overline{0}$. When this is the case, then $\overline{a}^p = \overline{a^p} = \overline{a}$ is trivially satisfied, so $a^p \equiv a \pmod{p}$.
- $\overline{a} \neq \overline{0}$. Here, $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Let $|\overline{a}| = k$. This means $\overline{a}^k = \overline{1}$. Since $\langle\overline{a}\rangle$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$, then according to Lagrange's theorem there is some integer ℓ such that $k\ell = p - 1$. So we have $\overline{1} = \overline{a}^k = (\overline{a}^k)^\ell = \overline{a}^{k\ell} = \overline{a}^{p-1}$. So, $\overline{a}^{p-1} = \overline{1}$, and multiplying both sides by $\overline{a}$ yields $\overline{a}^p = \overline{a^p} = \overline{a}$. Therefore, $a^p \equiv a \pmod{p}$.

Therefore $a^p \equiv p \pmod{p}$.

XVII. MORE ON HOMOMORPHISMS AND ISOMORPHISMS

Exercise 1

Prove that if G is a simple abelian group then G is isomorphic to Z_p for some prime p.

Let G be a simple abelian group. We will show that $G \cong Z_p$ for some prime p. To do so, we will first show the following results:

(i) *Claim*: G has no nontrivial proper subgroups.

Proof: Since G is abelian, then all its subgroups are normal. Because G is simple, then by definition its only normal subgroups are 1 and G itself. From these facts, we can conclude that G only has two subgroups: 1 and G. Therefore, it has no nontrivial proper subgroups.

(ii) *Claim*: $G = \langle x \rangle$ for all $x \in G$ where $x \neq 1$.

Proof: From (i), we can conclude that G only has two subgroups: 1 and G. Let $x \in G$, where $x \neq 1$. Since $\langle x \rangle \leq G$, and $\langle x \rangle \neq 1$, then $\langle x \rangle = G$. Note that x was an arbitrary nonidentity element. So for all $x \in G$ where $x \neq 1$, we have $\langle x \rangle = G$.

(iii) *Claim*: G is finite.

Proof: Let $x \in G$ where $x \neq 1$. Since $x^2 \in G$, we can use (ii) to claim that $\langle x \rangle = G$ and $\langle x^2 \rangle = G$, so therefore $\langle x \rangle = \langle x^2 \rangle$.

Now we will use the contrapositive of Theorem 2.7(2) in D&F: *Let $G = \langle x \rangle$ be a cyclic group. If $\langle x^a \rangle = \langle x^b \rangle$ for distinct nonnegative integers a and b, then G is finite.*

From this, we can conclude that G is finite.

(iv) *Claim*: $|G|$ is prime.

Proof: From (iii), we can claim that G is finite. From (i), we know that there are no subgroups of G other than 1 and G itself.

We will now use the contrapositive of Theorem 2.7(3) in D&F: *Let G be a finite cyclic group. If there is not a subgroup of G of order a, then a does not divide $|G|$.*

Let a be an integer where $1 < a < |G|$. From the above theorem, we can conclude that because there are no subgroups of order a, then a does not divide $|G|$. Therefore, $|G|$ must be prime.

Using results from (ii), (iii), and (iv), we can say that G is a finite cyclic group of order p, where p is prime. We can note that Z_p is also a finite cyclic group of order p. So, using Theorem 2.4 in D&F, which states that any two cyclic groups of the same order are isomorphic, we can conclude that $G \cong Z_p$, where $p = |G|$.

Exercise 2

Write down some explicit surjective homomorphisms from $Z_6 \times Z_2$ onto the following groups. [You don't need to verify that these are surjective, or homomorphisms, but the idea is to get practice just writing down the maps.]

(a) Z_2

(b) Z_6

(c) Z_3

(d) $Z_2 \times Z_2$

The following are examples of well-defined surjective homomorphisms from $Z_6 \times Z_2$ onto the specified groups:

(a) $f : Z_6 \times Z_2 \to Z_2$ where $(\overline{a}, \overline{b}) \mapsto \overline{ma + nb}$ and m and n are integers that are not simultaneously even.

(b) $f : Z_6 \times Z_2 \to Z_6$ where $(\overline{a}, \overline{b}) \mapsto \overline{ma + 3b}$ and m is any integer.
$f : Z_6 \times Z_2 \to Z_6$ where $(\overline{a}, \overline{b}) \mapsto \overline{ma}$ and m an integer such that $\gcd(6, m) = 1$.

(c) $f : Z_6 \times Z_2 \to Z_3$ where $(\overline{a}, \overline{b}) \mapsto \overline{ma}$ and m is an integer such that $\gcd(3, m) = 1$.

(d) $f : Z_6 \times Z_2 \to Z_2 \times Z_2$ where $(\overline{a}, \overline{b}) \mapsto (\overline{3a}, \overline{b})$.

Note: there is also the trivial surjective homomorphism $f : Z_6 \times Z_2 \to 1$, where $(\overline{a}, \overline{b}) \mapsto 1$ for all $a, b \in Z$.

Exercise 3

Suppose that φ is a homomorphism from a finite group G onto $Z_6 \times Z_2$. [Onto means φ is surjective.] Suppose that the kernel of φ has order 5. Explain why G must have normal subgroups of orders 5, 10, 15, 20, 30, 60. Try to do this by finding some appropriate homomorphisms and look at their kernels.

Let $\varphi : G \to Z_6 \times Z_2$, where φ is surjective and $|\ker \varphi| = 5$. We will show that G must have normal subgroups of orders 5, 10, 15, 20, 30, and 60. Before we begin, we will show the following result:

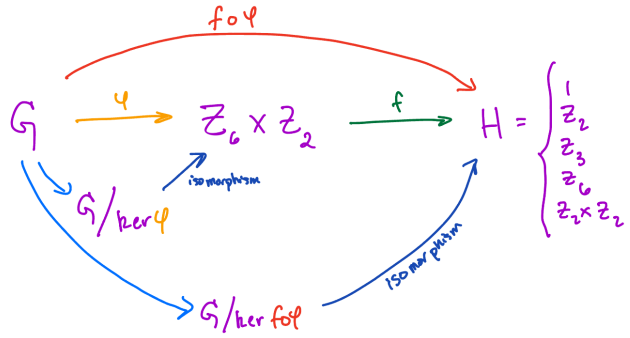
(i) *Claim*: Let $\varphi : G \to G'$ be a homomorphism. Then $|G| = |\ker \varphi||\varphi(G)|$.

Proof: Let $\varphi : G \to G'$ be a homomorphism. From the First Isomorphism Theorem, we know there is an isomorphism $G/\ker \varphi \cong \varphi(G)$, which implies $|G/\ker \varphi| = |\varphi(G)|$. By Lagrange's theorem, we also have $|G| = |G/\ker \varphi||\ker \varphi|$. Combining these two results, we have $|G| = |\ker \varphi||\varphi(G)|$, as desired.

(ii) *Claim*: Let $\varphi : G \to G'$ and $\psi : G' \to H$ both be homomorphisms. Then the functional combination $\psi \circ \varphi$ is a homomorphism.

Proof: Let $\varphi : G \to G'$ and $\psi : G' \to H$ be homomorphisms, and let $a, b \in G$. Then $(\psi \circ \varphi)(ab) = \psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b)) = \psi(\varphi(a))\psi(\varphi(b)) = (\psi \circ \varphi)(a)(\psi \circ \varphi)(b)$. Therefore $\psi \circ \varphi$ is a homomorphism.

Armed with this result, we are now ready to address the problem at hand. To illustrate the structure of this problem, we can refer to the figure below:



[Not all of this diagram is used in the solution to this problem, but it's nice to see how the result in (i) can be applied due to the First Isomorphism Theorem.] This diagram illustrates that we have a surjective

homomorphism φ from G onto $Z_6 \times Z_2$, a surjective homomorphism f from $Z_6 \times Z_2$ onto H, along with the functional combination of the two, $f \circ \varphi$, which, from (ii), is a surjective homomorphism that maps G onto H. Here, f should be recognized as representing one of the homomorphisms in the previous Exercise, where H can be the groups: 1, Z_2, Z_3, Z_6 or $Z_2 \times Z_2$. There are natural projections that map from G to $G/\ker\varphi$ and from G to $\ker(f \circ \varphi)$. From the First Isomorphism Theorem, there are isomorphisms from $G/\ker\varphi$ to $Z_6 \times Z_2$ as well as $G/\ker(f \circ \varphi)$ to H.

Off the bat, we can note that since the kernel of a homomorphism is a normal subgroup (cf D&F Exercise 3.1.1), i.e., $\ker\varphi \trianglelefteq G$, and since $|\ker\varphi| = 5$, then $\ker\varphi$ is one of the normal subgroups of G we're looking for. Furthermore, since φ is surjective, then $\varphi(G) = Z_6 \times Z_2$, so $|\varphi(G)| = |Z_6 \times Z_2| = 12$. Using the result from (i), we have $|G| = |\ker\varphi||\varphi(G)| = (5)(12) = 60$.

Using the result from (i), we have $|G| = |\ker(f\circ\varphi)||(f\circ\varphi)(G)|$. Because $f\circ\varphi$ is surjective, $(f\circ\varphi)(G) = H$, so then $|G| = |\ker(f\circ\varphi)||H|$. Since H can be the various groups studied in the previous Exercise, we can make the following table:

H	$\lvert H\rvert$	$\lvert\ker(\varphi\circ f)\rvert = \lvert G\rvert/\lvert H\rvert$
1	1	60
Z_2	2	30
Z_3	3	20
Z_6	6	10
$Z_2 \times Z_2$	4	15

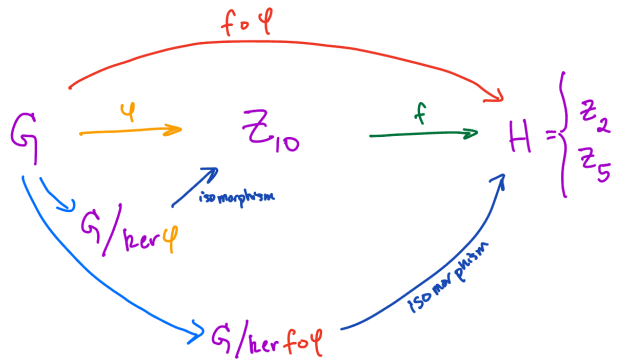
(129)

Since $\ker(f \circ \varphi) \trianglelefteq G$, we have found our remaining normal subgroups of G.

Exercise 4

Suppose there is a homomorphism from a finite group G onto Z_{10}. Prove that G has normal subgroups of indexes 2 and 5.

Let $\varphi : G \to Z_{10}$ be a surjective homomorphism. We will show that G has normal subgroups of indexes 2 and 5. We will use the same approach as the previous problem. To begin, we can note that the following well-defined surjective homomorphisms exist: $f : Z_{10} \to Z_2$ where $f(\overline{a}) = \overline{a}$, and $f : Z_{10} \to Z_5$ where $f(\overline{a}) = \overline{a}$. [This works because 10 is a multiple of both 2 and 5.]



Because φ and f are surjective homomorphisms, then from (ii) in the previous Exercise, $\varphi \circ f$ is a surjective homomorphism. Using (i) in the previous Exercise, we have $|G| = |\ker(f \circ \varphi)||(f \circ \varphi)(G)|$. Because $f \circ \varphi$ is surjective, then $(f \circ \varphi)(G) = H$, so $|G| = |\ker(f \circ \varphi)||H|$. Now, $\ker(f \circ \varphi) \trianglelefteq G$ (cf D&F Exercise 3.1.1), and the index of a normal subgroup of G is defined as $[G : \ker(f \circ \varphi)] = |G|/|\ker(f \circ \varphi)|$.

Combining these two equations, we have $[G : \ker(f \circ \varphi)] = |H|$. Since we showed $|H|$ can be 2 or 5, then $[G : \ker(f \circ \varphi)]$ is 2 or 5, as desired.

Exercise 5

If H is a normal subgroup of G and $|H| = 2$, prove that H is contained in the center of G. Use this to conclude that A_5 does not have a subgroup of order 2.

Let H be a normal subgroup of G and $|H| = 2$. We will first show that H is contained in the center of G. Let $g \in G$. Here, H is small enough were we can determine the act of conjugation on all elements of H. Denote $H = \{1, h\}$, where $|h| = 2$. Since H is a normal subgroup, then $gHg^{-1} \subseteq H$ (D&F Theorem 3.7). So, we can conjugate the element of H one by one. First, $g1g^{-1} = 1$. Second, ghg^{-1} can only be 1 or h, but it cannot be 1, since this would imply $gh = g$ and therefore $h = 1$, but this is a contradiction since $h \neq 1$. So, $ghg^{-1} = h$. Since the choice of $g \in G$ was arbitrary, these conjugation relations imply that all elements of H commute with all elements of G, so $H \subseteq Z(G)$.

Next, we will use this result to show that A_5 does not have a subgroup of order 2. Note that if it is the case that $Z(A_5) = 1$, then it is impossible that a subgroup of A_5 of order 2 can exist, since in the previous paragraph we proved that such a subgroup would be a subset of $Z(A_5)$. So, all we have to show is $Z(A_5) = 1$. To begin, we can note the fact brought up in D&F Section 3.5, which is A_n is a non-abelian simple group for all $n \geq 5$. [Do I need to prove this?] This means A_5 only has normal subgroups of 1 and A_5. Since the center of a group is automatically a normal subgroup, i.e., $Z(A_5) \trianglelefteq A_5$, and since A_5 is non-abelian, then the only possibility is $Z(A_5) = 1$. Therefore, A_5 cannot have a subgroup of order 2.

Exercise 6

Suppose that H is a normal subgroup of a finite group G. If G/H has an element of order n, show that G has an element of order n. Show, by example, that the assumption that G is finite is necessary.

[This is the converse of D&F Exercise 3.1.5.] Let H be a normal subgroup of a finite group G, and let $x \in G/H$. We can note that x can be represented as $x = gH$, where $g \in G$. Since G is finite, the order of the elements of G/H are finite, so let $|x| = n$. This implies that n is the smallest positive integer such that $x^n = (gH)^n = H$. We will show that G also has an element of order n.

To begin, we can note that G is finite, so let $|g| = \alpha$. Using $g^\alpha = 1$ and D&F Exercise 3.1.4, this implies $H = g^\alpha H = (gH)^\alpha$. Since n is the smallest positive integer such that $(gH)^n = H$, then α must be a multiple of n, i.e., there is a positive integer k such that $nk = \alpha$.

We will now show that $y = g^k$ is our desired element of G of order n. First, we can note that $y^n = (g^k)^n = g^\alpha = 1$. So, $|y| \leq n$. Suppose $|y| = m$, so $m \leq n$. To show $m = n$, we will proceed by contradiction. Assume $m < n$. Then $1 = y^m = (g^k)^m = g^{km}$. This means $\alpha | km$, i.e., $nk | km$, which implies $n | m$. This is a contradiction, since $m < n$. Therefore $m = n$, and we have $|y| = n$, as desired.

We can note that this result does not necessarily hold if G is infinite. As an example, consider when $G/N = \mathbb{Q}/\mathbb{Z}$, which has elements of finite order even though G does not. To see why, consider an element $x = p/q + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, where $p, q \in \mathbb{Z}$. Here, x has finite order because $qx = p + q\mathbb{Z} = 0 + \mathbb{Z}$, while $\mathbb{Q}$ has infinite order.

Exercise 7

Suppose $|G| = 30$ and $|Z(G)| = 5$. What is the structure of $G/Z(G)$? How does your answer change if $|Z(G)| = 3$? Generalize to the case that $|G| = 2pq$ where p and q are distinct odd primes. [Use the fact, to be proven later, that if p is an odd prime, then there are exactly two groups of order $2p$ (up to isomorphism): Z_{2p} and D_{2p}.]

Let G be a group where $|G| = 30$ and $|Z(G)| = 5$. We can note that by Lagrange's theorem $|G/Z(G)| = |G|/|Z(G)| = 30/5 = 6$. We can use the given fact that because $6 = 2 \cdot 3$, and 3 is an odd prime, then there are exactly two groups of order 6 to which $G/Z(G)$ could be isomorphic: Z_6 or D_6. However, if $G/Z(G)$ is isomorphic to Z_6, which is a cyclic group, then according to D&F Exercise 3.1.36, we can conclude that G is abelian. But if G is abelian, then $|Z(G)| = |G|$, which is contrary to our given fact that $|Z(G)| \neq |G|$. Therefore, $G/Z(G) \cong D_6$.

If instead $|Z(G)| = 3$, then $|G/Z(G)| = |G|/|Z(G)| = 30/3 = 10$. We can use the given fact that because $10 = 2 \cdot 5$, and 5 is an odd prime, then there are exactly two groups of order 10 to which $G/Z(G)$ could be isomorphic: Z_{10} or D_{10}. However, if $G/Z(G)$ is isomorphic to Z_{10}, which is a cyclic group, then according to D&F Exercise 3.1.36, we can conclude that G is abelian. But if G is abelian, then $|Z(G)| = |G|$, which is contrary to our given fact that $|Z(G)| \neq |G|$. Therefore, $G/Z(G) \cong D_{10}$.

More generally, suppose $|G| = 2pq$, where p and q are distinct odd primes. Before we proceed, we will prove the following result:

(i) *Claim*: Let G be a finite abelian group, where $|G| = pq$ and p and q are distinct primes. Then G is cyclic.

Proof: Let G be a finite abelian group, where $|G| = pq$ and p and q are distinct primes. Since G is finite and p and q are primes dividing $|G|$, then by Cauchy's Theorem (cf D&F Theorem 11) we can say that G has an element $x \in G$ where $|x| = p$ and $y \in G$ where $|y| = q$. Now consider the element $xy \in G$. Because G is abelian, and $\gcd(p, q) = 1$, then xy has order $\text{lcm}(p, q) = pq$. Therefore, $|\langle xy \rangle| = |G|$, so therefore G is cyclic.

Because $Z(G) \leq G$, then by Lagrange's theorem, $|Z(G)|$ can be 1, 2, q, p, $2q$, $2p$, or $2pq$. We can go through these cases one by one:

- Suppose $|Z(G)| = 1$. Then $|G/Z(G)| = 2pq$, and we cannot say anything more about the structure of G or $G/Z(G)$.

- Suppose $|Z(G)| = 2$. Then $|G/Z(G)| = |G|/|Z(G)| = pq$. We can also note that because p and q are prime, we can use D&F Exercise 3.2.4 to claim that $G/Z(G)$ is abelian. Furthermore, because p and q are distinct primes, we can use (i) to claim $G/Z(G)$ is cyclic. If $G/Z(G)$ is cyclic, then according to D&F Exercise 3.1.36, G is abelian. However, if G is abelian, then $Z(G) = G$, i.e., $|G/Z(G)| = |G|$, which is a contradiction. Therefore, there is no such group G with $Z(G) = 2$.

- If $|Z(G)| = p$, then we have $|G/Z(G)| = |G|/|Z(G)| = 2q$, and since q is an odd prime, then $G/Z(G)$ could be isomorphic to Z_{2q} or D_{2q}. Suppose $G/Z(G)$ were isomorphic to Z_{2q}, which is a cyclic group, then then according to D&F Exercise 3.1.36, we can conclude that G is abelian. But if G is abelian, then $Z(G) = G$, i.e., $|Z(G)| = |G|$. But we're given $|G| \neq |Z(G)|$, so we're dealt a contradiction. Therefore $G/Z(G) \cong D_{2q}$. [A similar argument can be followed when $|Z(G)| = q$, just with the roles of p and q swapped.]

- If $|Z(G)| = 2p$, then we have $|G/Z(G)| = |G|/|Z(G)| = q$. Because $|G/Z(G)|$ is prime, we can use D&F Corollary 3.10 to claim that $G/Z(G)$ is cyclic. Therefore, $G/Z(G) \cong Z_q$. If $G/Z(G)$ is cyclic, then according to D&F Exercise 3.1.36, G is abelian. However, if G is abelian, then $Z(G) = G$, i.e., $|G/Z(G)| = |G|$, which is a contradiction. Therefore, there is no such group G with $Z(G) = 2p$. [A similar argument can be followed when $|Z(G)| = 2q$, just with the roles of p and q swapped.]

- Suppose $|Z(G)| = 2pq$. We have $G/Z(G) = |G|/|Z(G)| = 1$.

XVIII. TRANSPOSITIONS AND THE ALTERNATING GROUP

Exercise 1

Write a given permutation as a product of transpositions. For instance, (12345)(678).

$$\begin{aligned}(12345)(678) &= (1345)(12)(68)(67) &(130)\\ &= (145)(13)(12)(68)(67) &(131)\\ &= (15)(14)(13)(12)(68)(67) &(132)\end{aligned}$$

Exercise 2

Let σ and $(a_1a_2\cdots a_k)$ be permutations in S_n. Prove that $\sigma(a_1a_2\cdots a_k)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$.

Let σ and $(a_1a_2\cdots a_k)$ be permutations in S_n. We will show that $\sigma(a_1a_2\cdots a_k)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$. In what follows, we will refer to the left-hand side of this equation as "LHS", and the right-hand side will be "RHS". To do this, it will suffice to show that LHS and RHS have the same effect when acting on any integer i where $1 \le i \le n$. Since permutations are bijections, we can let $i = \sigma(j)$, where j is some other integer $1 \le j \le n$. Now we will consider two cases: when j is one of the integers in $(a_1a_2\cdots a_n)$ and when it is not. First, when j is one of the integers in $(a_1a_2\cdots a_n)$, we can let $j = a_\ell$, where $1 \le \ell \le n$, so

$$\begin{aligned}\sigma(a_1a_2\cdots a_\ell\cdots a_k)\sigma^{-1}i &= \sigma(a_1a_2\cdots a_\ell\cdots a_n)\sigma^{-1}\sigma(j) &(133)\\ &= \sigma(a_1a_2\cdots a_\ell\cdots a_k)\sigma^{-1}\sigma(a_\ell) &(134)\\ &= \sigma(a_1a_2\cdots a_\ell\cdots a_k)a_\ell &(135)\\ &= \sigma(a_{\ell+1 \pmod k}) &(136)\\ (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_\ell)\cdots\sigma(a_k))i &= (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_\ell)\cdots\sigma(a_k))\sigma(j) &(137)\\ &= (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_\ell)\cdots\sigma(a_k))\sigma(a_\ell) &(138)\\ &= \sigma(a_{\ell+1 \pmod k}) &(139)\end{aligned}$$

In this case, we see indeed the LHS and RHS have the same effect on i. On the other hand, when j is not one of the integers in $(a_1a_2\cdots a_n)$, we have

$$\begin{aligned}\sigma(a_1a_2\cdots a_k)\sigma^{-1}i &= \sigma(a_1a_2\cdots a_n)\sigma^{-1}\sigma(j) &(140)\\ &= \sigma(a_1a_2\cdots a_k)j &(141)\\ &= \sigma(j) &(142)\\ (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))i &= (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))\sigma(j) &(143)\\ &= \sigma(j) &(144)\end{aligned}$$

The last equality follows from the fact that if $j \notin \{a_1, a_2, \cdots, a_k\}$, then $\sigma(j) \notin \{\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_k)\}$ since σ is a bijection. Therefore, the LHS and RHS have the same effect on an arbitrary integer i where $1 \le i \le n$. Therefore, we can conclude $\sigma(a_1a_2\cdots a_k)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$.

As a corollary, it also follows that even given a disjoint permutation, we have:

$$\begin{aligned}\sigma(a_1a_2\cdots a_k)(b_1b_2\cdots b_\ell)\sigma^{-1} &= \sigma(a_1a_2\cdots a_k)\sigma^{-1}\sigma(b_1b_2\cdots b_\ell)\sigma^{-1} &(145)\\ &= (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))(\sigma(b_1)\sigma(b_2)\cdots\sigma(b_\ell)) &(146)\end{aligned}$$

D&F Exercise 3.5.2

Prove that σ^2 is an even permutation for every permutation σ.

Every permutation σ is either even or odd. The act of squaring the permutation σ^2 has the effect of doubling the number of transpositions, always resulting in an even number of transpositions. Therefore, σ^2 is always an even permutation.

Alternatively, we can note that $\epsilon(\sigma)$ is a homomorphism $\epsilon : S_n \to \{\pm 1\}$ (cf D&F Proposition 23). Therefore, $\epsilon(\sigma^2) = \epsilon(\sigma)^2 = +1$, so σ^2 is even.

D&F Exercise 3.5.3

Prove that S_n is generated by $\{(i\ i+1)|1 \leq i \leq n-1\}$. [Consider conjugates, viz. (23)(12)(23)$^{-1}$.]

We will show that S_n is generated by $\mathcal{A}_n = \{(i\ i{+}1)|1 \leq i \leq n{-}1\}$. First, we can note that any element of S_n can be written as a product of transpositions, i.e., S_n is generated by the set of transpositions, i.e., $\mathcal{T}_n = \{(ij)|1 \leq i < j \leq n\}$. So, all we have to show is that any element of $\mathcal{T}$ can be generated by $\mathcal{A}_n$.

First, let's do a warm up. Say we pick element $(i\ i+1) \in \mathcal{A}_n$, and we conjugate it with another element $(i+1\ i+2) \in \mathcal{A}_n$:

$$(i+1\ i+2)(i\ i+1)(i+1\ i+2) = (i\ i+2) \tag{147}$$

Now we have produced an element in $\mathcal{T}_n$, but not in $\mathcal{A}_n$. Note that the first entry stayed the same, but the second entry increased by 1. Say we kept repeating this process of conjugation with elements from $\mathcal{A}_n$. Then we could produce any element $(ij) \in \mathcal{T}_n$. More formally, let $k = j - i$:

$$(ij) \ = \ (i+(k-1)\ i+k)\cdots(i+1\ i+2)(i\ i+1)(i+1\ i+2)\cdots(i+(k-1)\ i+k) \tag{148}$$

So, we have shown that an transposition can be generated by elements of $\mathcal{A}_n$, so therefore S_n is as well.

D&F Exercise 3.5.9

Prove that the (unique) subgroup of order 4 in A_4 is normal and is isomorphic to V_4.

We will show that the (unique) subgroup of order 4 in A_4 is normal and is isomorphic to V_4. Consider the set $H = \{1, (12)(34), (13)(24), (14)(23)\}$. Note that H contains the only elements of A_4 that are order 2, i.e., the three double-transpositions are their own inverses.

First, we will show that H is a normal subgroup. Since H also contains the identity and the set is closed under multiplication, then it is a subgroup. To prove normality, let $h \in H$, where $h \neq 1$. Let $g \in A_4$, and we can note that under conjugation ghg^{-1} is still an element of order 2 (cf D&F Exercise 1.1.22). Since H contains all the elements of order 2, then H is normal.

Next, we will show that $H \cong V_4$. We can note the result from D&F Exercise 2.5.10: *Any group G of order 4 is either isomorphic to Z_4 or V_4.* Since $|H| = 4$, then this result claims that either H is isomorphic to either Z_4 or V_4. Since Z_4 has an element of order 4, and since H has no element of order 4, then $H \cong V_4$.

XIX. GROUP ACTIONS AND PERMUTATION REPRESENTATIONS

D&F Exercise 4.1.4

Let S_3 act on the set Ω of ordered pairs: $\{(i,j)|1 \leq i,j \leq 3\}$ by $\sigma((i,j)) = (\sigma(i), \sigma(j))$.

(a) Find the orbits of S_3 on Ω.

(b) For each $\sigma \in S_3$ find the cycle decomposition of σ under this action (i.e., find its cycle decomposition when σ is considered as an element of S_9 – first fix a labeling of these nine ordered pairs.)

(c) For each orbit $\mathcal{O}$ of S_3 acting on these nine points pick some $a \in \mathcal{O}$ and find the stabilizer of a in S_3.

Let S_3 act on the set Ω of ordered pairs: $\{(i,j)|1 \leq i,j \leq 3\}$ by $\sigma((i,j)) = (\sigma(i), \sigma(j))$.

(a) There are two orbits of S_3 on Ω. To illustrate, consider the elements of S_3 acting on (11): $e \cdot (11) = (11)$, $(12) \cdot (11) = (22)$, $(23) \cdot (11) = (11)$, $(13) \cdot (11) = (33)$. So, the orbit of (11) is $\mathcal{O}_1 = \{(11), (22), (33)\}$. This is the same orbit as (22) and (33). Next, consider the elements of S_3 acting on (12) : $e \cdot (12) = (12)$, $(12) \cdot (12) = (21)$, $(13) \cdot (12) = (32)$, $(23) \cdot (12) = (13)$, $(123) \cdot (12) = (23)$, $(132) \cdot (12) = (31)$. So, the orbit of (12) is $\mathcal{O}_2 = \{(12), (21), (23), (32), (13), (31)\}$. This is the same orbit as (21), (13), (31), (23), and (32).

(b) If we use the following labeling: $\mathbf{1} = (12)$, $\mathbf{2} = (21)$, $\mathbf{3} = (23)$, $\mathbf{4} = (32)$, $\mathbf{5} = (13)$, $\mathbf{6} = (31)$, $\mathbf{7} = (11)$, $\mathbf{8} = (22)$, $\mathbf{9} = (33)$, we have the following cycle decomposition of $\sigma \in S_9$ under this action:

$g \in S_3$	$\sigma \in S_9$
e	e
(12)	$(\mathbf{12})(\mathbf{35})(\mathbf{46})(\mathbf{78})$
(23)	$(\mathbf{15})(\mathbf{26})(\mathbf{34})(\mathbf{89})$
(13)	$(\mathbf{14})(\mathbf{23})(\mathbf{56})(\mathbf{79})$
(123)	$(\mathbf{136})(\mathbf{245})(\mathbf{789})$
(132)	$(\mathbf{136})(\mathbf{245})(\mathbf{798})$

(149)

(c) First, we'll pick $\mathbf{7} \in \mathcal{O}_1$. Here, the stabilizer of (11) under this action is $\{e, (22), (33)\}$, since these are the elements of S_3 that act trivially on $\mathbf{7}$. Next, we'll pick $\mathbf{1} \in \mathcal{O}_2$ (note: this is not the identity, it is a label associated with an element in Ω), where its stabilizer is $\{e\}$.

XX. GROUP ACTING ON THEMSELVES BY LEFT MULTIPLICATION

D&F Exercise 4.2.10

Prove that every non-abelian group of order 6 has a non-normal subgroup of order 2. Use this to classify groups of order 6. [Produce an injective homomorphism into S_3.]

Let G be a group of order 6. We will show that either $G \cong Z_6$ or $G \cong D_6$.

First, suppose G is abelian. We will show $G \cong Z_6$. From (i) in D&F Exercise 7 above, we can use the result: *if G is a finite abelian group, where $G = pq$ and p and q are distinct primes, then G is cyclic.* From this, we can immediately claim that since $6 = 2 \cdot 3$, and 2 and 3 are distinct primes, then G is cyclic, i.e., $G \cong Z_6$.

Next, suppose G is non-abelian. We will show $G \cong D_6$. From D&F Theorem 3.12 (Sylow), we can note that G must have at least one subgroup of order 2, call it $H = \{1, x\}$. Next, consider the set of cosets of H, i.e., $A = \{H, g_1H, g_2H\}$, where $g_1, g_2 \in G$ are representatives of their respective coset. (Since cosets partition the group, we have now labeled all of our group elements, $G = \{1, x, g_1, g_1x, g_2, g_2x\}$.) Consider the group action $f : G \times A \to A$, where $g \cdot a \mapsto ga$. Since f is a group action, then there is a homomorphism $\varphi : G \to S_3$. Now we will determine what elements are contained in $\ker \varphi = \{g \in G | g \cdot a = a, a \in A\}$. Let $g \in \ker \varphi$. Then $gH = H$, so we can conclude that $g \in H = \{1, x\}$. We want to exclude the possibility that $g = x$. We will proceed by contradiction. Assume $g = x$. Because g is in the kernel, we must have

$gg_1H = g_1H = xg_1H$, so $xg_1 \in g_1H$, which implies $x \in g_1Hg^{-1}$, i.e., $x = 1$ (which is a contradiction) or $x = g_1xg_1^{-1}$, so x commutes with g_1. The same argument follows to conclude that x commutes with g_2. So, x commutes with all elements of G, and the center of the group $Z(G) \neq 1$. Since $|G| = 6 = 2 \cdot 3$, and 2 and 3 are primes, then either G is abelian or $Z(G) = 1$ (cf D&F Exercise 3.2.4). But G is non-abelian, and we showed that $Z(G) \neq 1$, so this is a contradiction. So, $g = 1$. Therefore, $\ker \varphi = 1$, and φ is therefore injective. Since there are 6 elements in G and there are 6 elements in S_3, then φ is an isomorphism. Therefore, $G \cong S_3$. And since $S_3 \cong D_6$, then $G \cong D_6$.

From this, we can deduce that every non-abelian group G of order 6 has a non-normal subgroup of order 2, since G is isomorphic to D_6, which itself has a non-normal subgroup of order 2, i.e., $\{1, s\}$.

XXI. SYLOW THEOREMS

JG Exercise 24.2

If a is a group element, prove that every element in $cl(a)$ has the same order as a.

Let G be a finite group and $a \in G$. Here, $cl(a) = \{gag^{-1} | g \in G\}$. An element and its conjugate have the same order, i.e., $|a| = |gag^{-1}|$ for all $g \in G$ (cf D&F Exercise 1.1.21). Therefore, all elements of $cl(a)$ have the same order as a.

[This also follows from the fact that conjugation by a fixed element is an isomorphism.]

JG Exercise 24.3

Let a be a group element of even order. Prove that a^2 is not in $cl(a)$.

Let G be a group with element a of even order. That is, $|a| = 2k$, where $k \in \mathbb{Z}^+$. We will show $a^2 \notin cl(a)$. First, we can note that $|a^2| = 2k/\gcd(2, 2k)$ (cf D&F Proposition 2.5). Since $\gcd(2, 2k) > 1$, then $|a^2| \neq 2k$, i.e., a and a^2 do not have the same order. Using JG Exercise 24.2, then we can conclude that a and a^2 cannot be in the same conjugacy class.

JG Exercise 24.7

Show that Z_2 is the only group that has exactly two conjugacy classes.

Suppose a group G has two conjugacy classes. We will show $|G| = 2$. To begin, we note that the identity is always in its own conjugacy class, so we can express the class equation for G as:

$$|G| = 1 + [G : C_G(a)] \tag{150}$$

where $a \in G$ is a representative of the conjugacy class to which a belongs. From Lagrange's theorem, we also have

$$|G| = |C_G(a)|[G : C_G(a)]. \tag{151}$$

For notational simplicity, let $x = |G|$ and $b = |C_G(a)|$, noting that x and b are positive integers. Solving for $[G : C_G(a)]$ in the second above equation and inserting it into the first equation yields $x = 1 + x/b$, i.e, $x = b/(b - 1)$. Since x must be an integer, this forces $b/(b - 1)$ to be an an integer, and the only integer where this is true is when $b = 2$. Therefore $x = 2$, and thus $|G| = 2$.

JG Exercise 24.8

What can you say about the number of elements of order 7 in a group of order $168 = 8 \cdot 3 \cdot 7$*?*

Consider a group of order $168 = 7 \cdot 24$. Since 7 does not divide 24, then by Sylow's Third Theorem, $n_7 \equiv 1 \pmod 7$ and $n_7 | 24$. The only values for n_7 that satisfy these conditions are $n_7 = 1$ or 8. Since these subgroups of order 7 are of prime order, then they are cyclic (cf D&F Corollary 3.10), and every non-identity element in these cyclic subgroup has order 7 (cf D&F Proposition 2.5). Therefore, when $n_7 = 1$, there are 6 elements with order 7. When $n_7 = 8$, we need to determine the intersection between these subgroups. Let P_1 and P_2 be any two of these cyclic Sylow 7-subgroups. We can note that the intersection $P_1 \cap P_2$ is itself a subgroup (cf D&F Exercise 2.1.10), so by Lagrange's theorem, it must have order 1 or 7. Since Sylow ensures that these are distinct subgroups, then only $P_1 \cap P_2 = \{1\}$. So, when $n_7 = 8$, we have $8 \cdot (7 - 1) = 48$ elements of order 7.

JG Exercise 24.12

Determine the class equation for non-abelian groups of orders 39 and 55.

Let G be a non-abelian group of order $39 = 3 \cdot 13$. We will determine its class equation. First, the class equation takes the form

$$|G| = |Z(G)| + \sum_a [G : C_G(a)] \tag{152}$$

where a is a representative of a conjugacy class outside the center. Since $Z(G)$ is a subgroup of G, by Lagrange's theorem, we have the following cases to consider:

- $|Z(G)| = 1$.
- $|Z(G)| = 3$. Here, $|G/Z(G)| = 13$, which is prime, so $G/Z(G)$ is cyclic, and therefore G is abelian. But this is a contradiction, so $|Z(G)| \neq 3$.
- $|Z(G)| = 13$. Here, $|G/Z(G)| = 3$, which is prime, so $G/Z(G)$ is cyclic, and therefore G is abelian. But this is a contradiction, so $|Z(G)| \neq 13$.
- $|Z(G)| = 39$. If $|Z(G)| = 39$, then the entire group is in the center, so the group is abelian, which is a contradiction.

So, $|Z(G)| = 1$. Next, by Lagrange's theorem, $[G : C_G(a)]$ must divide 39. We know $[G : C_G(a)] \neq 1$, otherwise a would be in the center of G, which was already counted. And $[G : C_G(a)] \neq 39$, since $[G : C_G(a)] = |G|/|C_G(a)|$, and $\langle a \rangle \leq C_G(a)$, so because $|a| > 1$, then $|C_G(a)| > 1$. So, $[G : C_G(a)]$ can either be 3 or 13, so we can write the class equation like: $39 = 1 + 13x + 3y$, where x and y are positive integers. It turns out there is only one solution: $x = 2$, $y = 4$. So the class equation for G is: $39 = 1 + 13 + 13 + 3 + 3 + 3 + 3$.

Let G be a non-abelian group of order $55 = 5 \cdot 11$. We will determine its class equation. The same arguments can be used to show that $Z(G) = 1$ and $[G : C_G(a)]$ is 5 or 11. We can write the class equation like: $55 = 1 + 11x + 5y$, where x and y are positive integers. There is only one solution: $x = 4$ and $y = 2$. So the class equation for G is: $55 = 1 + 11 + 11 + 11 + 11 + 5 + 5$.

JG Exercise 24.13

Determine which of the equations below could be the class equation given in the proof of [JG] Theorem 24.2. For each part, provide your reasoning.

(a) $9 = 3 + 3 + 3$

(b) $21 = 1 + 1 + 3 + 3 + 3 + 3 + 7$

(c) $10 = 1 + 2 + 2 + 5$

(d) $18 = 1 + 3 + 6 + 8$

JG Theorem 24.2 is: *Let G be a nontrivial finite group whose order is a power of a prime p. Then $Z(G)$ has more than one element.* The version of the class equation that appears in the proof for this theorem is $|G| = |Z(G)| + \sum_a |G : C_G(a)|$, so I believe this means that the first term on the right-hand side of this version of the class equation is the value of $|Z(G)|$.

(a) $9 = 3 + 3 + 3$. Here, the order of the group is the square of a prime, so the group is abelian (cf JG Corollary of Theorem 24.4). But if the group is abelian, then every element of the group is in the center, so the class equation must be $9 = 1 + 1 + \cdots + 1$. So, $9 = 3 + 3 + 3$ is not a feasible class equation.

(b) $21 = 1 + 1 + 3 + 3 + 3 + 3 + 7$. Here, 21 is not a power of a prime, so JC Theorem 24.2 does not apply. Furthermore, for $p-$groups, the sizes of the non-central classes have to be powers of the same p, and this example mixes different primes.

(c) $10 = 1 + 2 + 2 + 5$. Here, 10 is not a power of a prime, so JC Theorem 24.2 does not apply.

(d) $18 = 1 + 3 + 6 + 8$. Here, 18 is not a power of a prime, so JC Theorem 24.2 does not apply.

JG Exercise 24.14

Exhibit a Sylow 2-subgroup of S_4. Describe an isomorphism from this group to D_8.

Here $|S_4| = 4! = 24 = 2^3 \cdot 3$, so by the First Sylow Theorem, S_4 must have a Sylow 2-subgroup of order 8. An explicit representation of such a Sylow 2-subgroup is $P = \langle (1234), (13) \rangle$. One can explicitly check by hand that these two elements generates a subgroup of order 8: 1, $r = (1234)$, $r^2 = (13)(24)$, $r^3 = (1432)$, $s = (13)$, $sr = (12)(34)$, $sr^2 = (24)$, $sr^3 = (14)(23)$.

As the notation above suggests, there is an isomorphism between D_8 and P. Recall $D_8 = \langle r, s | r^4 = 1, s^2 = 1, (sr)^2 = 1 \rangle$. Define the map $\varphi : D_8 \to P$, where $r \mapsto (1234)$ and $s \mapsto (13)$. First, we can check the relations: $r^4 = (1234)^4 = 1$, $s^2 = (13)^2 = 1$, and $(sr)^2 = ((13)(1234))^2 = 1$. Since the relations match, φ is a homomorphism. The image of φ contains (1234) and (13), which generate P, so φ is surjective. Since $|D_8| = |P| = 8$, then φ is a isomorphism.

JG Exercise 24.15

Suppose that G is a group of order 48. Show that the intersection of any two distinct Sylow 2-subgroups of G has order 8.

Let G be a group of order $48 = 2^4 \cdot 3$. By the Third Sylow Theorem, $n_2 \equiv 1 \pmod 2$ and $n_2 | 3$. This restricts $n_2 = 1, 3$. We will show that the intersection of any two Sylow 2-subgroups of G will have an intersection of order 8.

If $n_2 = 1$, then the statement is trivially true, so we will proceed by assuming $n_2 = 3$. Take any two distinct Sylow 2-subgroups of order 16, $P_1, P_2 \in Syl_2(G)$. By D&F Proposition 3.13, we have $|P_1 P_2| = |P_1||P_2|/|P_1 \cap P_2| = 16^2/|P_1 \cap P_2|$. But $P_1 P_2 \subseteq G$. So, $|P_1 P_2| = 16^2/|P_1 \cap P_2| \leq 48$, and therefore $|P_1 \cap P_2| \geq 16^2/48 = 16/3$. Also, $P_1 \cap P_2 \leq P_1$, and $|P_1| = 16 = 2^4$, so by Lagrange's theorem $|P_1 \cap P_2| = 2^a$, where $1 \leq a \leq 4$. So, we have the constraints $|P_1 \cap P_2| \geq 16/3$ and $|P_1 \cap P_2| = 2^a$, where $1 \leq a \leq 4$. The only possibilities are $|P_1 \cap P_2| = 8$ or 16. But if $|P_1 \cap P_2| = 16$, then P_1 and P_2 are not distinct subgroups, since they both have order 16. Therefore, $|P_1 \cap P_2| = 8$.

JG Exercise 24.16

Find all the Sylow 3-subgroups of S_4.

All groups of order 3 are isomorphic to Z_3. So, the subgroups of S_4 of order 3 are just cyclic permutations on 3 elements. So, here are all these order-3 subgroups of S_4: $\{1, (123), (132)\}$, $\{1, (134), (143)\}$, $\{1, (234), (243)\}$, and $\{1, (124), (142)\}$.

JG Exercise 24.21

Suppose that G is a group of order 168. If G has more than one Sylow 7-subgroup, exactly how many does it have?

Let G be a group of order $168 = 2^3 \cdot 3 \cdot 7$. By the Third Sylow Theorem, $n_7 \equiv 1 \pmod 7$ and $n_7 | 24$, so this means $n_7 = 1$ or 8. So, if $n_7 \neq 1$, then $n_7 = 8$.

JG Exercise 24.22

Show that every group of order 56 has a proper nontrivial normal subgroup.

Let G be a group of order $56 = 2^3 \cdot 7$. By the Third Sylow Theorem, then $n_7 \equiv 1 \pmod 7$ and $n_7 | 8$. The only possibility is $n_7 = 1, 8$. If $n_7 = 1$, then this subgroup is a proper normal subgroup (JG Corollary p. 393), and we are done.

Now we will consider the case when $n_7 = 8$. Note by the First Sylow Theorem, G must have a Sylow 2-subgroup of order 8, call it P_2, and its nontrivial elements must have a order that divides 8. If instead $n_7 = 8$, then we can note the Sylow 7-subgroups have trivial overlap among themselves (because any intersection is a subgroup of order dividing 7), so there are $8(7-1) = 8$ elements of order 7 in G, and one of these is the identity. These 8 leftover elements must make up P_2, since it's guaranteed to exist. Therefore, when $n_7 = 8$, there is a single Sylow 2-subgroup, so therefore it is normal.

JG Exercise 24.27

How many Sylow 3-subgroups of S_5 are there? Exhibit five.

Just as in a previous exercise [JG Exercise 24.16], all groups of order 3 will be isomorphic to Z_3, so we just have to count the number of subsets of 3 elements on which we can do cyclic permutations. For a set of 5 elements, there are $\binom{5}{3} = 5!/(3!2!) = 10$ such subsets. Here are 5 of them: $\{1, (123), (132)\}$, $\{1, (134), (143)\}$, $\{1, (234), (243)\}$, $\{1, (124), (142)\}$, and $\{1, (125), (152)\}$.

JG Exercise 24.30

Prove that a group of order 175 is Abelian.

Let G be a group of order $175 = 5^2 \cdot 7$. We will show that G is abelian. By the Third Sylow Theorem, $n_5 \equiv 1 \pmod 5$ and $n_5 | 7$, so $n_5 = 1$, and call this subgroup H. Likewise, $n_7 \equiv 1 \pmod 7$ and $n_7 | 25$, so $n_7 = 1$, and call this subgroup K. Let's collect some facts:

(i) *Claim*: H and K are both normal subgroups.

Proof: H is the only Sylow 5-subgroup, so $H \trianglelefteq G$. Also, K is the only Sylow 7-subgroup, so $K \trianglelefteq G$ (cf JG Corollary p. 393).

(ii) *Claim*: H and K are abelian.

Proof: Since $|H| = 25 = 5^2$, and 5 is prime, then H is abelian (cf JG Corollary p. 389). Since $|K| = 7$, and 7 is prime, then K is cyclic (cf D&F Corollary 3.10), and so K is abelian.

(iii) *Claim*: $H \cap K = 1$.

Proof: Since $\gcd(|H|, |K|) = \gcd(25, 7) = 1$, then $H \cap K = 1$ (cf D&F Exercise 3.2.8).

(iv) *Claim*: $HK = G$.

Proof: We have $|HK| = |H||K|/|H \cap K|$ (cf D&F Proposition 3.13). From (iii), $H \cap K = 1$, so $|HK| = |H||K|$. But $|H||K| = 175 = |G|$ and because $HK \subseteq G$, therefore $HK = G$.

(v) *Claim*: $hk = kh$ for all $h \in H$ and $k \in K$.

Proof: From (i) both H and K are normal subgroups of G, and from (iii) $H \cap K = 1$, then $hk = kh$ for all $h \in H$ and $k \in K$ (cf D&F Exercise 3.1.42).

Because $G = HK$ from (iv), $hk = kh$ for all $h \in H$ and $k \in K$ from (v), and H and K are both abelian from (ii), we can conclude that G is abelian, i.e., a group of order 175 is abelian.

JG Exercise 24.39

Show that the center of a group of order 60 cannot have order 4.

Let G be a group of order 60. We will show that $|Z(G)| \neq 4$. We will proceed by contradiction. Assume $Z(G) = 4$. Then $|G/Z(G)| = 15$. From the Third Sylow Theorem, the number of Sylow p-subgroups of $G/Z(G)$ are $n_5 = 1$ (call it H, which has order 5) and $n_3 = 1$ (call it K, which has order 3). Let's collect some facts:

(i) *Claim:* H and K are both normal subgroups of $G/Z(G)$.

Proof: H and K are both normal subgroups of $G/Z(G)$ because they are the unique Sylow p-subgroups of order 5 and 3, respectively (cf JG Corollary p. 393).

(ii) *Claim*: H and K are cyclic, i.e., $H \cong Z_5$ and $K \cong Z_3$.

Proof: Since $|H| = 5$, and 5 is prime, then H is cyclic (cf D&F Corollary 3.10), i.e., $H \cong Z_5$. Since $|K| = 3$, and 3 is prime, then K is cyclic (cf D&F Corollary 3.10), i.e., $K \cong Z_3$.

(iii) *Claim*: $H \cap K = 1$.

Proof: Since $\gcd(|H|, |K|) = \gcd(5, 3) = 1$, then $H \cap K = 1$ (cf D&F Exercise 3.2.8).

(iv) *Claim*: $G/Z(G) = HK$.

Proof: Since H and K are subgroups, $|HK| = |H||K|/|H \cap K|$ (cf D&F Proposition 3.13). From (iii), then $|HK| = |H||K| = 15 = |G/Z(G)|$, so therefore $G/Z(G) = HK$.

(v) *Claim*: For normal subgroups H and K with $H \cap K = 1$, HK is a subgroup and $HK \cong H \times K$.

Proof: This is D&F Proposition 5.8.

(vi) *Claim*: $G/Z(G) \cong Z_3 \times Z_5$.

Proof: From (iv) we have $G/Z(G) = HK$. From (i) and (iii), we can use (v) to say $HK \cong H \times K$. Therefore, $G/Z(G) \cong H \times K$. From (ii), we therefore have $G/Z(G) \cong Z_3 \times Z_5$.

(vii) *Claim*: $G/Z(G)$ is cyclic.

Proof: From (vii), $G/Z(G) \cong Z_3 \times Z_5$. Since $\gcd(3,5) = 1$, then $Z_3 \times Z_5 \cong Z_{15}$, so $G/Z(G)$ is cyclic.

From (viii), $G/Z(G)$ is cyclic, so G is abelian (cf D&F Exercise 3.1.36). However, if G is an abelian group of order 60, then $|Z(G)| = 60$, which is a contradiction. Therefore, $|Z(G)| \neq 4$.

XXII. FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS

JG Exercise 11.1

What is the smallest positive integer n such that there are two non isomorphic groups of order n? Name the two groups.

We'll step through groups of increasing order, starting with 1, and analyze each in turn. Groups of size one are just the trivial group, and there is only one of these. There is one group of order two, i.e., Z_2. There is only one group of order 3, i.e., Z_3. There are two abelian groups of order 4, which we know from the Fundamental Theorem of Finite Abelian Groups, i.e., Z_4 and $Z_2 \times Z_2$, which are not isomorphic.

JG Exercise 11.4

Calculate the number of elements of order 2 in each of Z_{16}, $Z_8 \times Z_2$, $Z_4 \times Z_4$, and $Z_4 \times Z_2 \times Z_2$. Do the same for elements of order 4.

In the following, I'll use the $\mathbb{Z}/n\mathbb{Z}$ notation for Z_n (since these groups are isomorphic). So, $\overline{0}$ is the identity and $\overline{1}$ is the generator.

For Z_{16}, the only element of order 2 is $\overline{8}$. The elements of order 4 are $\overline{4}$ and $\overline{4}$.

For $Z_8 \times Z_2$, the elements of order 2 are $(\overline{0},\overline{1})$, $(\overline{4},\overline{0})$, and $(\overline{4},\overline{1})$. The elements of order 4 are $(\overline{2},\overline{0})$, $(\overline{2},\overline{1})$, $(\overline{6},\overline{0})$, and $(\overline{6},\overline{1})$.

For $Z_4 \times Z_4$, the elements of order 2 are $(\overline{2},\overline{0})$, $(\overline{0},\overline{2})$, and $(\overline{2},\overline{2})$. The elements of order 4 are any element that contains a $\overline{1}$ or $\overline{3}$ in either slot; there are 16 of these.

For $Z_4 \times Z_2 \times Z_2$, the elements of order 2 are $(\overline{2},\overline{0},\overline{0})$, $(\overline{0},\overline{1},\overline{0})$, $(\overline{0},\overline{0},\overline{1})$, $(\overline{0},\overline{1},\overline{1})$, $(\overline{2},\overline{1},\overline{0})$, $(\overline{2},\overline{0},\overline{1})$, and $(\overline{2},\overline{1},\overline{1})$. The elements of order 4 are $(\overline{1},\overline{0},\overline{0})$, $(\overline{1},\overline{1},\overline{0})$, $(\overline{1},\overline{0},\overline{1})$, $(\overline{1},\overline{1},\overline{1})$, $(\overline{3},\overline{0},\overline{0})$, $(\overline{3},\overline{1},\overline{0})$, $(\overline{3},\overline{0},\overline{1})$, and $(\overline{3},\overline{1},\overline{1})$.

JG Exercise 11.5

Prove that any abelian group of order 45 has en element of order 15. Does every abelian group of order 45 have an element of order 9?

Given an abelian group G or order 45, it can isomorphic to $Z_9 \times Z_5$ or $Z_3 \times Z_3 \times Z_5$. If the former group, an element of order 15 is $(\overline{3},\overline{1})$, and an element of order 9 is $(\overline{1},\overline{0})$. If the latter group, an element of order 15 is $(\overline{1},0,\overline{1})$, and there is no element of order 9. Therefore, all abelian groups of order 45 have an element of order 15, but not all have an element of order 9.

JG Exercise 11.10

Find all abelian groups (up to isomorphism) of order 360.

Using the Fundamental Theorem of Finite Abelian Groups as articulated in JG, the list of non-isomorphic abelian groups of order 360 are:

1. $Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_5$,
2. $Z_4 \times Z_2 \times Z_3 \times Z_3 \times Z_5$,
3. $Z_8 \times Z_3 \times Z_3 \times Z_5$,
4. $Z_2 \times Z_2 \times Z_2 \times Z_9 \times Z_5$,
5. $Z_4 \times Z_2 \times Z_9 \times Z_5$,
6. $Z_8 \times Z_9 \times Z_5$.

JG Exercise 11.11

Prove that every finite abelian group can be expressed as the direct product of cyclic groups of orders $n_1, n_2, \cdots n_t$, where n_{i+1} divides n_i for $i = 1, 2, \cdots, t-1$.

A quick example: consider a cyclic group of order 45. This group can be isomorphic to $Z_9 \times Z_5$ or $Z_3 \times Z_3 \times Z_5$. Recall the combination rule: $Z_n \times Z_m \cong Z_{mn}$ if and only if $\gcd(m, n) = 1$. So $Z_9 \times Z_5 \cong Z_{45}$ and $Z_3 \times Z_3 \times Z_5 \cong Z_{15} \times Z_3$. I think this satisfies the desired result, as long as we consider $Z_{45} \cong Z_{45} \times Z_1$.

The idea of the proof is to use the combination rule to combine products of cyclic groups of relatively prime orders into a single group. I'm not going to prove this now, but it's a nice result to know.

JG Exercise 11.15

How many abelian groups (up to isomorphism) are there of order 6? Of order 15? Of order 42? Or order pq, where p and q are distinct primes? Of order prq, where p, q, and r are distinct primes? Is there a way to generalize this?

Recall the combination rule: $Z_a \times Z_b \cong Z_{ab}$ if and only if $\gcd(a, b) = 1$.

The only possible abelian group of order 6 is $Z_2 \times Z_3 \cong Z_6$.

The only possible abelian groups of order 15 is $Z_3 \times Z_5 \cong Z_{15}$.

The only possible abelian groups of order 42 is $Z_2 \times Z_3 \times Z_7 \cong Z_{42}$.

The only possible abelian groups of order pq, where p and q are distinct primes is $Z_p \times Z_q \cong Z_{pq}$.

The only possible abelian groups of order pqr, where p, q, r are distinct primes is $Z_p \times Z_q \times Z_r \cong Z_{pqr}$.

One possible generalization is that for a abelian group with order that has a prime factorization where the power of each prime is at most 1, then there is only one abelian group of that order. Furthermore, for a group of this type, if m divides the order of the group, there is a subgroup of that order.

JG Exercise 11.20

Verify the corollary to the Fundamental Theorem of Finite Abelian Groups in the case that the group has order 1080 and the divisor is 180.

The corollary is (JG p. 217): if m divides the order of a finite Abelian group G, then G has a subgroup of order m.

Here, 180 divides 1080, so according to this corollary, an abelian group of order 1080 has a subgroup of order 180. We can verify this via the Fundamental Theorem of Finite Abelian Groups, which states that an abelian group of order 1080 must be isomorphic to one of the following groups (note that $1080 = 2^3 \cdot 3^3 \cdot 5$ and $180 = 2^2 \cdot 3^2 \cdot 5$):

- $Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_5$. This has a subgroup of order 180: $Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_5$.

- $Z_4 \times Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_5$. This has a subgroup of order 180: $Z_4 \times Z_3 \times Z_3 \times Z_5$.
- $Z_8 \times Z_3 \times Z_3 \times Z_3 \times Z_5$. Let $\langle 2 \rangle$ denote the subgroup of order 4 of Z_8. Then this group has a subgroup of order 180: $\langle 2 \rangle \times Z_3 \times Z_3 \times Z_5$.
- $Z_2 \times Z_2 \times Z_2 \times Z_9 \times Z_3 \times Z_5$. This has a subgroup of order 180: $Z_2 \times Z_2 \times Z_9 \times Z_5$.
- $Z_4 \times Z_2 \times Z_9 \times Z_3 \times Z_5$. This has a subgroup of order 180: $Z_4 \times Z_9 \times Z_5$.
- $Z_8 \times Z_9 \times Z_3 \times Z_5$. Let $\langle 2 \rangle$ denote the subgroup of order 4 of Z_8. This has a subgroup of order 180: $\langle 2 \rangle \times Z_9 \times Z_5$.
- $Z_2 \times Z_2 \times Z_2 \times Z_{27} \times Z_5$. Let $\langle 3 \rangle$ denote the subgroup of order 9 of Z_{27}. Then this group has a subgroup of order 180: $Z_2 \times Z_2 \times \langle 3 \rangle \times Z_5$.
- $Z_4 \times Z_2 \times Z_{27} \times Z_5$. Let $\langle 3 \rangle$ denote the subgroup of order 9 of Z_{27}. Then this group has a subgroup of order 180: $Z_4 \times \langle 3 \rangle \times Z_5$.
- $Z_8 \times Z_{27} \times Z_5$. Let $\langle 2 \rangle$ denote the subgroup of order 4 of Z_8. Let $\langle 3 \rangle$ denote the subgroup of order 9 of Z_{27}. Then this group has a subgroup of order 180: $\langle 2 \rangle \times \langle 3 \rangle \times Z_5$.

JG Exercise 11.26

The set $G = \{1, 7, 17, 23, 49, 55, 65, 71\}$ is a group under multiplication modulo 96. Write G as an external and an internal direct product of cyclic groups.

Below is a table of the orders of each element:

$g \in G$	$\lvert g \rvert$
1	1
7	4
17	2
23	4
49	2
55	4
65	2
71	4

(153)

So, there are only elements of order 1, 2, and 4. An abelian group of order 8 must be isomorphic to one of these three groups:

- $Z_2 \times Z_2 \times Z_2$. This group has no elements of order 4.
- $Z_4 \times Z_2$. This has elements of order 1, 2, and 4, e.g., (0,0), (2,1), and (1,0), respectively.
- Z_8. This group has an element of order 8, i.e., (1,0).

So $G \cong Z_4 \times Z_2$.

JG Exercise 11.30

Suppose that G is an abelian group of order 16, and in computing the orders of its elements, you come across an element of order 8 and two elements of order 2. Explain why no further computations are needed to determine the isomorphism class of G.

Let G be a finite abelian group of order 16, which has an element of order 8 and two elements of order 2. There are only four groups it could be isomorphic to:

- $Z_2 \times Z_2 \times Z_2 \times Z_2$. This group has no elements of order 8.
- $Z_4 \times Z_2 \times Z_2$. This group has no elements order 8.
- $Z_8 \times Z_2$. This group has an element of order 8, i.e., (1,0), and two elements of order 2, i.e., (0,1) and (4,0).
- Z_{16}. This group has an element of order 8, i.e., (2), but only one element of order 2, i.e., (8).

Therefore, G must be isomorphic to $Z_8 \times Z_2$.

JG Exercise 11.33

Without using Lagrange's theorem, show that an abelian group of odd order cannot have an element of even order.

Let G be a finite abelian group of odd order. We will show that G cannot have an element of even order. First, let's prove the following useful result:

(i) *Claim*: Let $g \in Z_{p^n}$, where p is prime. Then $|g|$ divides p^n.

Proof: Let $g \in Z_{p^n}$, where p is prime. Let $\langle x \rangle = Z_{p^n}$, so $g = x^a$. Then we have $|g| = |x^a| = p^n / \gcd(p^n, a)$ (cf D&F Proposition 2.5). We can note that for any value of a, $\gcd(p^n, a)$ must be equal to a power of p, i.e., $\gcd(p^n, a) = p^k$, where $0 \leq k \leq n$. So, $|x^a| = p^{n-k}$. Then $|g| = p^{n-k}$, and therefore $|g|$ divides p^n.

Now back to the problem at hand. According to the Fundamental Theorem of Finite Abelian groups, G is isomorphic to a group of the form:

$$G \cong Z_{p_1^{n_1}} \times \cdots \times Z_{p_k^{n_k}} \tag{154}$$

where p_i's are not necessarily distinct primes, but since $|G|$ is odd, then the p_i's must be odd primes. Pick an arbitrary element $a = (g_1, ..., g_k) \in G$. Since each g_i is an element of a group of order a prime power, then according to (i), $|g_i|$ must divide $p_i^{n_i}$. So, since $p_i^{n_i}$ is odd, therefore $|g_i|$ must also be odd. Now, $|a| = \text{lcm}(|g_1|, ..., |g_k|)$, and the least common multiple of a set of odd numbers must itself be odd. Since a was an arbitrary elements of G, we can therefore conclude that all elements of G have odd order.

XXIII. SEMIDIRECT PRODUCTS

D&F Exercise 5.5.1

Let H and K be groups, let φ be a homomorphism from K into $Aut(H)$, and identify H and K as subgroups of $G = H \rtimes_\varphi K$. Prove that $C_K(H) = \ker \varphi$.

Let $G = H \rtimes_\varphi K$, where $\varphi : K \to \text{Aut}(H)$. We will show that $C_K(H) = \ker \varphi$. To do this, we will show that the definition of $C_K(H)$, after a bit of massaging, matching the definition of $\ker \varphi$.

We use the definitions $\widetilde{H} = \{(h,1) \in G | h \in H\} \cong H$ and $\widetilde{K} = \{(1,k) \in G | k \in K\} \cong K$. The desired centralizer is $C_K(H) = \{(1,k) \in \widetilde{K} | (1,k)(h,1)(1,k)^{-1} = (h,1), \forall (h,1) \in \widetilde{H}\}$. Here we can note $(1,k)(h,1)(1,k)^{-1} = (\varphi(k)(h),k)(1,k^{-1}) = (\varphi(k)(h),1)$, so

$$C_K(H) = \{(1,k) \in \widetilde{K} | (\varphi(k)(h),1) = (h,1), \forall (h,1) \in \widetilde{H}\} \tag{155}$$

This is the same as the definition of $\ker \varphi = \{(1,k) \in \widetilde{K} | (\varphi(k)(h),1) = (h,1), \forall (h,1) \in \widetilde{H}\}$. So, $C_K(H) = \ker \varphi$.

D&F Exercise 5.5.2

Let H and K be groups, let φ be a homomorphism from K into $Aut(H)$, and identify H and K as subgroups of $G = H \rtimes_\varphi K$. Prove that $C_H(K) = N_H(K)$.

Let $G = H \rtimes_\varphi K$, where $\varphi : K \to \mathrm{Aut}(H)$. We will show that $C_H(K) = N_H(K)$ by showing that, after some massaging, their definitions are equivalent. We use the definitions $\widetilde{H} = \{(h,1) \in G | h \in H\} \cong H$ and $\widetilde{K} = \{(1,k) \in G | k \in K\} \cong K$. To begin, note that $C_H(K) = \{(h,1) \in G | (h,1)(1,k)(h,1)^{-1} = (1,k), \forall (1,k) \in \widetilde{K}\}$, and we can simplify $(h,1)(1,k)(h,1)^{-1} = (h,k)(h^{-1},1) = (h\varphi(k)(h^{-1}),k)$. So, this means that $(h,1) \in C_H(K)$ if and only if $h\varphi(k)(h^{-1}) = 1$ for all $k \in K$. Likewise, we have $N_H(K) = \{(h,1) \in G | (h,1)(1,k)(h,1)^{-1} \in \widetilde{K}, \forall (1,k) \in \widetilde{K}\}$. Noting the simplification $(h,1)(1,k)(h,1)^{-1} = (h\varphi(k)(h^{-1}),k)$, the only way this can be an element of $\widetilde{K}$ is if $h\varphi(k)(h^{-1}) = 1$ for all $k \in K$. Therefore, the requirements for an element of G to be in $C_H(K)$ and $N_H(K)$ are the same, so $C_H(K) = N_H(K)$.