Dummit & Foote: Exercises

blanket

Fall 2025

Contents

0   Preliminaries

0.1   Basics

For Exercises 1 to 4, let

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and $\mathscr{B} = \{X \in \mathscr{A} : MX = XM\}$, where $\mathscr{A}$ denotes the set of 2×2 matrices with real entries.

(1) Determine which of the following elements of $\mathscr{A}$ lie in $\mathscr{B}$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Solution. Note that the 1st matrix is M itself so that it belongs to $\mathscr{B}$, since $MX = XM = M^2$. Further note that the 3rd, 5th, and 6th matrices are the zero, identity, and exchange matrices respectively. Then the 3rd and 5th belong to $\mathscr{B}$ while the 6th does not. Then only the remaining matrices to check are the 2nd and 4th matrices. For the 2nd matrix:

$$MX = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 1 \cdot 1 & 1 \cdot 1 + 1 \cdot 1 \\ 0 \cdot 1 + 1 \cdot 1 & 0 \cdot 1 + 1 \cdot 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$$

$$XM = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 1 \cdot 0 & 1 \cdot 1 + 1 \cdot 1 \\ 1 \cdot 1 + 1 \cdot 0 & 1 \cdot 1 + 1 \cdot 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}$$

Then $MX \neq XM$ and the 2nd matrix does not belong to $\mathscr{B}$. For the 4th matrix:

$$MX = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 1 \cdot 1 & 1 \cdot 1 + 1 \cdot 0 \\ 0 \cdot 1 + 1 \cdot 1 & 0 \cdot 1 + 1 \cdot 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

$$XM = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 1 \cdot 0 & 1 \cdot 1 + 1 \cdot 1 \\ 1 \cdot 1 + 0 \cdot 0 & 1 \cdot 1 + 0 \cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

So that $MX \neq XM$. □

(2) Prove that if $P, Q \in \mathscr{B}$, then $P + Q \in \mathscr{B}$ where + denotes the usual sum of two matrices.

Solution. For Exercises 2 and 3, let

$$P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad Q = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, \quad P + Q = \begin{pmatrix} a + e & b + f \\ c + g & d + h \end{pmatrix}, \quad P \cdot Q = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$

where $PM = MP$ and $QM = MQ$. Then

$$\begin{aligned}
M(P + Q) &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a + e & b + f \\ c + g & d + h \end{pmatrix} \\
&= \begin{pmatrix} a + e + c + g & b + f + d + h \\ c + g & d + h \end{pmatrix} \\
&= \begin{pmatrix} a + c & b + d \\ c & d \end{pmatrix} + \begin{pmatrix} e + g & f + h \\ g & h \end{pmatrix} \\
&= MP + MQ \\
&= PM + QM \\
&= \begin{pmatrix} a & a + b \\ c & c + d \end{pmatrix} + \begin{pmatrix} e & e + f \\ g & g + h \end{pmatrix} \\
&= \begin{pmatrix} a + e & a + e + b + f \\ c + g & c + g + d + h \end{pmatrix} \\
&= \begin{pmatrix} a + e & b + f \\ c + g & d + h \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
&= (P + Q)M \qquad\qquad\qquad\qquad\qquad □
\end{aligned}$$

(3) Prove that if $P, Q \in \mathscr{B}$, then $P \cdot Q \in \mathscr{B}$ where $\cdot$ denotes the usual product of two matrices.

Solution. Using PQ, proceed as we did above with $M(PQ)$. Rewriting the entries will result in $(MP)Q$. Since $P \in \mathscr{B}$, then we have $(PM)Q$. We rewrite entries again to result in $P(MQ)$. Because $Q \in \mathscr{B}$, we have $P(QM)$, and a final rewrite results in $(PQ)M$. $\qquad\square$

(4) Find conditions on p, q, r, s which determine precisely when $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathscr{B}$.

Solution. Let X be the matrix described above. Note that

$$MX = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix}$$
$$XM = \begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix}$$

Because $X \in \mathscr{B}$, then we may compare entries to obtain the following:

$$\begin{cases} p+r=p \\ q+s=p+q \\ r=r \\ s=r+s \end{cases}$$

The first and fourth equations force $r = 0$, and the second equation forces $p = s$. Then $\mathscr{B}$ is classified as

$$\mathscr{B} = \left\{ \begin{pmatrix} p & p+q \\ 0 & p \end{pmatrix} \middle| \; p, q \in \mathbb{R} \right\} \qquad\square$$

(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 $f(a/b) = a^2/b^2$.

Solution.
  (a) No, because $1/2 = 2/4$, but $f(1/2) = 1$ and $f(2/4) = 2$.
  (b) Yes; suppose $a/b = c/d$. Then $ad = bc$, or that $a^2 d^2 = b^2 c^2$. Then $a^2/b^2 = c^2/d^2$, or $f(a/b) = f(c/d)$. $\qquad\square$

(6) Determine whether the function $f : R^+ \to \mathbb{Z}$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well defined.

Solution. No. Note that $1 = 1.000\ldots = 0.999\ldots$, but $f(1.000\ldots) = 1$ and $f(0.999\ldots) = 9$. $\qquad\square$

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

$$a \sim b \iff f(a) = f(b)$$

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

Solution. The relation above is an equivalence relation, since $=$ is already an equivalence relation on B.
  Consider now some $b \in B$. Since f is surjective, there exists $a \in A$ such that $f(a) = b$. The equivalence class of a is the set $\{x \in A \mid x \sim a\}$. By definition of $\sim$, this is equal to the set $\{x \in A \mid f(x) = f(a) = b\}$, which is precisely the fiber of f over b. $\qquad\square$

0.2   Properties of the Integers

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 $ax + by$ 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) $a = 507885, b = 60808$

Solution.

(a) Note: for this exercise, we will only do (e) as that has the most steps in calculating both the g.c.d and the Euclidean Algorithm. The l.c.m is obtained by dividing the product ab by (a, b).

$$(20, 13) = 1, \text{lcm}(20, 13) = 260, 1 = 2(20) - 3(13)$$

(b) $(69, 372) = 3, \text{lcm}(69, 372) = 8556, 27(69) - 5(372)$

(c) $(792, 275) = 11, \text{lcm}(792, 275) = 19800, 8(792) - 23(275)$

(d) $(11391, 5673) = 3, \text{lcm}(11391, 5673) = 21540381, 3 = 253(5673) - 126(11391)$

(e) Applying the Euclidean Algorithm to $a = 1761$ and $b = 1567$, we get:

$$1761 = (1)1567 + 194$$
$$1567 = (8)194 + 15$$
$$194 = (12)15 + 14$$
$$15 = (1)14 + 1$$

Then $(1761, 1567) = 1$ so that $\text{lcm}(1761, 1567) = 2759487$. Reversing the Euclidean Algorithm steps to solve for 1, we get:

$$1 = 15 - 14$$
$$= 15 - (194 - 12(15)) = 13(15) - 194$$
$$= 13(1567 - 8(194)) - 194 = 13(1567) - 105(194)$$
$$= 13(1567) - 105(1761 - 1567) = -105(1761) + 118(1567)$$

(f) $(507885, 60808) = 691, \text{lcm}(507885, 60808) = 44693880, 691 = 142(60808) - 17(507885)$ □

2. Prove that if the integer k divides the integers a and b then k divides $as + bt$ for every pair of integers s and t.

Solution. Since $k \mid a$ and $k \mid b$, there exists $x, y \in \mathbb{Z}$ such that $a = kx$ and $b = ky$. Then for any $s, t \in \mathbb{Z}$, we have $as + bt = kxs + kyt = k(xs + yt)$ which is divisible by k. □

3. Prove that if n is composite then there are integers a and b such that n divides ab but n does not divide either a or b.

Solution. By the Fundamental Theorem of Arithmetic, n has at least two prime factors a, b such that $1 < a, b < n$. Putting $n = ab$, then $n \mid ab$ but $n \nmid a$ and $n \nmid b$. □

4. Let a, b and N be fixed integers with a and b nonzero and let $d = (a, b)$ be the greatest common divisor of a and b. Suppose x_0 and y_0 are particular solutions to $ax + by = N$ (i.e., $ax_0 + by_0 = N$). Prove for any integer t that the integers

$$x = x_0 + \frac{b}{d}t \text{ and } y = y_0 - \frac{a}{d}t$$

are also solutions to $ax + by = N$ (this is in fact the general solution).

Solution. We have

$$ax + by = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right)$$
$$= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t$$
$$= ax_0 + by_0 = N$$

□

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

   Solution.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

n	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\varphi(n)$	8	16	6	18	8	12	10	22	8	20	12	18	12	28	8

   $\square$

6. Prove the Well Ordering Property of $\mathbb{Z}$ by induction and prove the minimal element is unique.

   Solution. Let $A \subseteq \mathbb{N}$ be nonempty. If $0 \in A$, then it has a minimal element. Suppose now that $0 \notin A$. Moreover, suppose that $1, 2, \ldots, k \notin A$ for some k. By strong induction, it follows that $k + 1 \notin A$. However, this results in there being no positive integer in A, contradicting that it is nonempty, thus it must have a minimal element. Moreover, if it had two minimal elements a, b, then it follows that $a \leq b$ and $b \leq a$ by definition of minimal element. Hence, $a = b$, and the minimal element of A is unique. $\square$

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).

   Solution. Suppose $\sqrt{p}$ is a rational number. Then there exists $a, b \in \mathbb{Z}$ such that $a^2 = b^2 p$, and $(a, b) = 1$. If $(a, b) = d \neq 1$, then take $a' = a/d$ and $b' = b/d$ instead. Then $p \mid a^2 = a \cdot a$, and $p \mid a$. We then have $a = kp$ for some $k \in \mathbb{Z}$. Then $b^2 = k^2 p$ so that $p \mid b$, and $b = mp$ for $m \in \mathbb{Z}$. This contradicts that $(a, b) = 1$, hence $\sqrt{p}$ cannot be a rational number. $\square$

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

   Solution. Note that in $n!$, there are $\lfloor n/p \rfloor$ integers that are divisible by p, where the greatest integer function is necessary since n may not be a perfect multiple of p (consider $n = 36$ and $p = 7$. Then there are the multiples $7, 14, 21, 28$, and 35 which is $\lfloor 36/7 \rfloor = 5$). However, this alone does not account for the factors of p in $n!$, so we move onto p^2. In this case, there are $\lfloor n/p^2 \rfloor$ integers divisible by p^2. We continue this process until a certain integer $a \in \mathbb{N}$ such that $p^a \leq n$. (We must bound p^a above by n, up to equality, since n may be a power of p, and any power a such that $p^a > n$ would result in $\lfloor n/p^a \rfloor = 0$). It then follows that $a \leq \log_p(n)$, or that the maximum power of p (and any of its multiples) that divide $n!$ is given by $a = \lfloor \log_p(n) \rfloor$. Thus, the largest power of p that divides $n!$ is given by

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

   $\square$

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.

Require: Integers a, b (not both zero)
Ensure: Integers g, x, y such that $g = (a, b)$ and $ax + by = g$

```
 1:  x₁ ← 1, y₁ ← 0
 2:  x₂ ← 0, y₂ ← 1
 3:  while b ≠ 0 do
 4:      q ← 0
 5:      r ← a
 6:      while (r ≥ b) or (r ≤ −b) do
 7:          r ← r − b
 8:          q ← q + 1
 9:      end while
10:      a ← b
11:      b ← r
```

```
12:      (x₁, x₂) ← (x₂, x₁ − q × x₂)
13:      (y₁, y₂) ← (y₂, y₁ − q × y₂)
14: end while
15: g ← a
16: return (g, x₁, y₁)
```

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

Solution. Let $N \in \mathbb{N}$ be fixed, and let $n \in \mathbb{N}$ such that $\varphi(n) = N$. We can break apart n into its primes p_i (where $p_1 < p_2 < \dots$) with associated exponents α_i:

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} \implies \varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = N$$

In particular, each of the terms $p_i - 1$ divides N so that $p_i - 1 \le N$, or $p_i \le N + 1$. It follows that any prime q of some n must be such a prime where $q - 1 \le N$. Moreover, for some $p_i^{\alpha_i}$ that is a part of n's prime factorization, it follows that $p_i^{\alpha_i - 1}$ divides N. Since $\alpha_i - 1$ is finite, this limits the exponents for any particular p_i. With a finite list of primes and finitely many exponents, it follows that the amount of n such that $\varphi(n) = N$ is finite.

For some $N_0 \in \mathbb{N}$, there are finitely many n such that $\varphi(n) = N_0$. Then there are infinitely many $m > n$ such that $\varphi(m) > N_0$, or that $\varphi(n)$ tends towards infinity. $\qquad\square$

11. Prove that if d divides n then $\varphi(d)$ divides $\varphi(n)$ where φ denotes Euler's φ-function.

Solution. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ with $d \mid n$. Then d is a composition of some p_i present in n, so some α_i may go to 0 or are less. In particular, we have that $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, where $\beta_i \le \alpha_i$ for all i. To see if $\varphi(d) \mid \varphi(n)$, it follows to check if $p_i^{\beta_i - 1}(p_i - 1)$ divides $p_i^{\alpha_i - 1}(p_i - 1)$, which further simplifies to checking if $p_i^{\beta_i}$ divides $p_i^{\alpha_i}$ for each i. Clearly, $p_i^{\alpha_i} = p_i^{\beta_i} \cdot p_i^{\alpha i - \beta_i}$, hence $\varphi(d) \mid \varphi(n)$. $\qquad\square$

0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

1. Write down explicitly all the elements in the residue classes of $\mathbb{Z}/18\mathbb{Z}$.

Solution.

$$\bar{0} = \{0 + 18k : k \in \mathbb{Z}\} = \{0, 18, -18, 36, -36, \dots\}$$
$$\bar{1} = \{1 + 18k : k \in \mathbb{Z}\} = \{1, 19, -17, 37, -35, \dots\}$$
$$\bar{2} = \{2 + 18k : k \in \mathbb{Z}\} = \{2, 20, -16, 38, -34, \dots\}$$
$$\bar{3} = \{3 + 18k : k \in \mathbb{Z}\} = \{3, 21, -15, 39, -33, \dots\}$$
$$\bar{4} = \{4 + 18k : k \in \mathbb{Z}\} = \{4, 22, -14, 40, -32, \dots\}$$
$$\bar{5} = \{5 + 18k : k \in \mathbb{Z}\} = \{5, 23, -13, 41, -31, \dots\}$$
$$\bar{6} = \{6 + 18k : k \in \mathbb{Z}\} = \{6, 24, -12, 42, -30, \dots\}$$
$$\bar{7} = \{7 + 18k : k \in \mathbb{Z}\} = \{7, 25, -11, 43, -29, \dots\}$$
$$\bar{8} = \{8 + 18k : k \in \mathbb{Z}\} = \{8, 26, -10, 44, -28, \dots\}$$
$$\bar{9} = \{9 + 18k : k \in \mathbb{Z}\} = \{9, 27, -9, 45, -27, \dots\}$$
$$\overline{10} = \{10 + 18k : k \in \mathbb{Z}\} = \{10, 28, -8, 46, -26, \dots\}$$
$$\overline{11} = \{11 + 18k : k \in \mathbb{Z}\} = \{11, 29, -7, 47, -25, \dots\}$$
$$\overline{12} = \{12 + 18k : k \in \mathbb{Z}\} = \{12, 30, -6, 48, -24, \dots\}$$
$$\overline{13} = \{13 + 18k : k \in \mathbb{Z}\} = \{13, 31, -5, 49, -23, \dots\}$$
$$\overline{14} = \{14 + 18k : k \in \mathbb{Z}\} = \{14, 32, -4, 50, -22, \dots\}$$
$$\overline{15} = \{15 + 18k : k \in \mathbb{Z}\} = \{15, 33, -3, 51, -21, \dots\}$$
$$\overline{16} = \{16 + 18k : k \in \mathbb{Z}\} = \{16, 34, -2, 52, -20, \dots\}$$
$$\overline{17} = \{17 + 18k : k \in \mathbb{Z}\} = \{17, 35, -1, 53, -19, \dots\}$$

$\square$

2. Prove that the distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are precisely $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$ (use the Division Algorithm).

   Solution. Clearly, $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \in \mathbb{Z}/n\mathbb{Z}$. Let $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. By the Division Algorithm, there exists $q \in \mathbb{Z}$ and $0 \leq r < n$ such that $a = nq + r$. Then $a \equiv r \bmod n$, so that $\bar{a} = \bar{r}$, where r is any one of the aforementioned equivalence classes. Moreover, if $\bar{a} = \bar{b}$ where $0 \leq a, b < n$, it follows that $n \mid (a-b)$ so that $a - b = 0$, or $a = b$. Hence, the equivalence classes of $\mathbb{Z}/n\mathbb{Z}$ are precisely the set above. $\square$

3. Prove that if $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$ is any positive integer then $a \equiv (a_n + a_{n-1} + \cdots + a_1 + a_0) \bmod 9$ (note that this is the usual arithmetic rule that the remainder after division by 9 is the same as the sum of the decimal digits mod 9—in particular an integer is divisible by 9 if and only if the sum of its digits is divisible by 9) [note that $10 \equiv 1 \bmod 9$].

   Solution. Using the note, then

   $$\begin{aligned} a &\equiv (a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0) \bmod 9 \\ &\equiv (a_n 1^n + a_{n-1} 1^{n-1} + \cdots + a_1 1 + a_0) \bmod 9 \\ &= (a_n + a_{n-1} + \cdots + a_1 + a_0) \bmod 9 \end{aligned}$$

   $\square$

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

   Solution. Note the following:

   $$\begin{aligned} 37^2 &\equiv 6 \bmod 29 \\ 37^4 &\equiv 6^2 \bmod 29 \equiv 7 \bmod 29 \\ 37^8 &\equiv 7^2 \bmod 29 \equiv 20 \bmod 29 \\ 37^{16} &\equiv 20^2 \bmod 29 \equiv 23 \bmod 29 \equiv -6 \bmod 29 \\ 37^{32} &\equiv (-6)^2 \bmod 29 \equiv 7 \bmod 29 \\ 37^{64} &\equiv 20 \bmod 29 \end{aligned}$$

   Then we have
   $$37^{64} 37^{32} 37^4 \equiv 20 \cdot 7 \cdot 7 \bmod 29 \equiv 20^2 \bmod 29 \equiv 23 \bmod 29$$

   Hence the remainder when dividing 37^{100} by 29 is 23. $\square$

5. Compute the last two digits of 9^{1500}.

   Solution. Note that $9^3 \equiv 29 \bmod 100$ so that $29^3 \equiv 89 \bmod 100$. Then $89 \cdot 9 \equiv 1 \bmod 100$, or $9^{10} \equiv 1 \bmod 100$. Since 1500 is a multiple of 10, then $9^{1500} = (9^{10})^{150} \equiv 1^{150} \bmod 100 \equiv 1 \bmod 100$. Then the last two digits is 01. $\square$

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

   Solution.

   $$\begin{aligned} 0^2 &= 0 \equiv 0 \bmod 4 \\ 1^2 &= 1 \equiv 1 \bmod 4 \\ 2^2 &= 4 \equiv 0 \bmod 4 \\ 3^2 &= 9 \equiv 1 \bmod 4 \end{aligned}$$

   $\square$

7. Prove that 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).

Solution. Since a^2 and b^2 is either $0 \bmod 4$ or $1 \bmod 4$, then we have 4 potential sums:

$$0 + 0 \equiv 0 \bmod 4$$
$$0 + 1 \equiv 1 \bmod 4$$
$$1 + 0 \equiv 1 \bmod 4$$
$$1 + 1 \equiv 2 \bmod 4$$

In any of the sums, there is no remainder of 3 when dividing by 4. □

8. Prove that the equation $a^2 + b^2 = 3c^2$ has no solutions in nonzero integers a, b and c. [Consider the equation $\bmod 4$ as in the previous two exercises and show that a, b and c would all have to be divisible by 2. Then each of 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.]

Solution. As hinted, consider the equation in $\bmod 4$. The left side must be 0 or 1, while the right side must be 0 or 3, hence both sides must be equivalent to $0 \bmod 4$. Then $3c^2 \equiv 0 \bmod 4$ implies c is even. If a is even, then b is even. If a is odd, then b must be odd. However, putting $a = 2x + 1$ and $b = 2y + 1$ for $x, y \in \mathbb{Z}$ results in $a^2 + b^2 = (2x+1)^2 + (2y+1)^2 \equiv 2 \bmod 4$, contradicting that $a^2 + b^2 \equiv 0 \bmod 4$. It must be that a and b are even. We may then divide the original equation by 4 to get a new equation $r^2 + s^2 = 3t^2$, where $r < a, s < b, t < c$. But then we may use the same reasoning to conclude that the new r, s, t must also be even, resulting in a new equation with smaller integer solutions. This process cannot be iterated indefinitely as we cannot halve any integer indefinitely and remain an integer. Hence, the original equation does not have integer solutions. □

9. Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.

Solution. Take $a = 2k + 1, k \in \mathbb{Z}$. Then $a^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$. Note that $k(k+1)$ is even, so that $4k(k+1)$ is divisible by 8. Then $a^2 \equiv 1 \bmod 8$. □

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

Solution. Recall that $\varphi(n)$ produces the number of integers that are relatively prime to n. It suffices to prove that the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ are the equivalence classes of $\mathbb{Z}/n\mathbb{Z}$ whose representatives are relatively prime to n.

Let $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then there exists $\overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\overline{a} \cdot \overline{b} = \overline{1}$. In particular, $\overline{a} \cdot \overline{b} - \overline{1} = \overline{0}$, or $n \mid (ab - 1)$. Then $nx + ab = 1$ for $x \in \mathbb{Z}$, which shows that $(a, n) = 1$. Conversely, if $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $(a, n) = 1$, then there exists $b, x \in \mathbb{Z}$ such that $ab + xn = 1$, or $ab = 1 \bmod n$. It follows that $\overline{b}$ is the inverse of $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

11. Prove that if $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Solution. It follows that there exist $\overline{x}, \overline{y} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\overline{a} \cdot \overline{x} = \overline{b} \cdot \overline{y} = \overline{1}$. In particular:

$$\overline{1} = \overline{1} \cdot \overline{1} = (\overline{a} \cdot \overline{x}) \cdot (\overline{b} \cdot \overline{y}) = (\overline{a} \cdot \overline{b}) \cdot (\overline{x} \cdot \overline{y})$$

So that the multiplicative inverse of $\overline{a} \cdot \overline{b}$ is $\overline{x} \cdot \overline{y}$. □

12. Let $n \in \mathbb{Z}, n > 1$ and let $a \in \mathbb{Z}$ 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 $ab \equiv 0 \bmod n$ and deduce that there cannot be an integer c such that $ac \equiv 1 \bmod n$.

Solution. Since a and n are not relatively prime, then $(a, n) = d$ where $1 < d \leq a$. Then $n/d, a/d \in \mathbb{Z}$, and $a(n/d) = n(a/d) \equiv 0 \bmod n$ so that $b = n/d$. Moreover, if there was such a c such that $ac \equiv 1 \bmod n$, then $abc \equiv b \bmod n$, which is false since $ab \equiv 0 \bmod n$. Hence, no such b may exist. □

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

Solution. Since $(a, n) = 1$, there exists $c, x \in \mathbb{Z}$ such that $ac + nx = 1$. Then $ac \equiv 1 \bmod n$. □

14. Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\overline{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 4. Verify this directly in the case $n = 12$.

Solution. The previous two exercises show that a and n are relatively prime if and only if there exists b such that $ab \equiv 1 \bmod n$, which is exactly the proposition. For $n = 12$, the elements $1, 5, 7, 11$ are relatively prime to 12, so that $(\mathbb{Z}/11\mathbb{Z})^{\times} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ whose inverses are $\overline{1}, \overline{7}, \overline{5}, \overline{11}$ respectively. $\square$

15. For each of the following pairs of integers a and n, show that a is relatively prime to n and determine the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$.

    (a) $a = 13, n = 20$
    (b) $a = 69, n = 89$
    (c) $a = 1891, n = 3797$
    (d) $a = 6003722857, n = 77695236973$

    Solution.

    (a) Refer to the previous set of exercises on how to do the Euclidean Algorithm and how to calculate such an x such that $ax + by = 1$, or $ax \equiv 1 \bmod n$. For this exercise, we obtain $-3 \equiv 17 \bmod 20$, so the inverse is $\overline{17}$.
    (b) $40(69) - 31(89) = 1 \implies 40 \cdot 89 \equiv 1 \bmod 89$, so the inverse is $\overline{40}$.
    (c) $253(1891) - 126(3797) = 1 \implies 253 \cdot 1891 \equiv 1 \bmod 3797$, so the inverse is $\overline{253}$.
    (d) $17n - 220a = 1 \implies -220a \equiv 1 \bmod n \implies 77695237193a \equiv 1 \bmod n$, so the inverse is $\overline{77695237193}$. $\square$

16. Write a computer program to add and multiply mod n, for any n given as input. The output of these operations should be the least residues of the sums and products of two integers. Also include the feature that if $(a, n) = 1$, an integer c between 1 and $n-1$ such that $\overline{a} \cdot \overline{c} = \overline{1}$ may be printed on request. (Your program should not, of course, simply quote "mod" functions already built into many systems).

1 Introduction to Groups

1.1 Basic Axioms and Examples

Let G be a group.

(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 $a \star b = \dfrac{a}{b}$

   Solution.

   (a) Not associative: $(2-0)-2 \neq 2-(0-2)$.

   (b) Associative:

$$\begin{aligned}
(a \star b) \star c &= (a + b + ab) \star c \\
&= (a + b + ab) + c + (a + b + ab)c \\
&= a + b + ab + c + ac + bc + abc \\
&= a + b + c + bc + ab + ac + abc \\
&= a + (b + c + bc) + a(b + c + bc) \\
&= a \star (b + c + bc) \\
&= a \star (b \star c)
\end{aligned}$$

   (c) Not associative: $(1 \star 0) \star 2 = 11/25, 1 \star (0 \star 2) = 7/25$.

   (d) Associative:

$$\begin{aligned}
[(a,b) \star (c,d)] \star (e,f) &= (ad + bc, bd) \star (e,f) \\
&= ((ad + bc)f + bde, bdf) \\
&= (adf + bcf + bde, bdf) \\
&= (adf + b(cf + de), bdf) \\
&= (a,b) \star (cf + de, df) \\
&= (a,b) \star [(c,d) \star (e,f)]
\end{aligned}$$

   (e) Not associative: $(1 \star 2) \star 3 = 1/6, 1 \star (2 \star 3) = 3/2$. $\qquad\square$

(2) Decide which of the binary operations in the preceding exercise are commutative.

   Solution.

   (a) Not commutative: $1 - 0 \neq 0 - 1$.

   (b) Commutative: $a \star b = a + b + ab = b + a + ba = b \star a$.

   (c) Commutative: $a \star b = (a + b)/5 = (b + a)/5 = b \star a$.

   (d) Commutative: $(a,b) \star (c,d) = (ad + bc, bd) = (cb + da, db) = (c,d) \star (a,b)$.

   (e) Not commutative: $1/2 \neq 2/1$. $\qquad\square$

(3) Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

   Solution. Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$. Then $(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{(a+b)+c} = \overline{a + (b+c)} = \overline{a} + \overline{b+c} = \overline{a} + (\overline{b} + \overline{c})$. $\qquad\square$

(4) Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).

Solution. Uses similar reasoning as the previous exercise (where $\cdot$ is associative over $\mathbb{Z}$). $\qquad\square$

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

Solution. Note that in any $\mathbb{Z}/n\mathbb{Z}$, $\bar{1}$ is a multiplicative identity. Moreover, there is no $x \in \mathbb{Z}$ such that $0x = 1$ so that $\bar{0} \in \mathbb{Z}/n\mathbb{Z}$ has no multiplicative inverse. $\qquad\square$

(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

Solution. Let S denote the set in each part.

  (a) Clearly, $0 \in S$ and for any $r \in S$, then $-r \in S$ is the additive inverse. To prove closure, let $a/b, c/d \in S$, and consider its sum $(ad + bc)/bd$. Since b, d are odd, then bd is also odd. Since having an even factor results in an even number, then any divisor of bd must also be odd. Then $(ad + bc, bd)$ must also be odd, and if we divide both the numerator and the denominator by this quantity, then we still result in odd numbers. Hence, A is closed under addition and is a group.

  (b) S is not a group, since $1/2 \in S$, but $1/2 + 1/2 = 2/2 = 1/1 \notin S$.

  (c) Same as previous.

  (d) S is not a group, since $3/2, 1 \in S$, but $3/2 - 1 = 1/2 \notin S$.

  (e) Using the Division Algorithm, any $p \in S$ may be split into the form $a + b/2$, where a is even and b is either 0 (if the numerator p is even) or 1 (if the numerator of p is odd). Then if we have $a_1 + b_1/2, a_2 + b_2/2 \in S$ and we consider their sum, then either both b_i is 0 or 1, in which case we remain an integer with denominator 1, or just one of the b_i is 1 in which case we end with a rational with denominator 2 (WLOG, suppose $b_1 = 1$ and $b_2 = 0$. Then we get the rational $(2a_1 + 2a_2 + 1)/2$). Hence, S is closed under addition, and it also has identity 0 and additive inverse $-p$ so that S is a group.

  (f) S is not a group, since $1/2, 1/3 \in S$, but $1/2 + 1/3 = 5/6 \notin S$. $\qquad\square$

(7) Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ 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*).

Solution. Let $x, y \in G$. Then we have two cases:
- $0 \leq x + y < 1$: Then $[x + y] = 0$, and $x \star y = x + y \in G$,
- $1 \leq x + y < 2$: Then $[x + y] = 1$, and $x \star y = x + y - 1 \in G$.

so that $\star$ is well defined on G. To show associativity, let $z \in G$. Then there are three cases:
- If $0 \leq x + y, y + z < 1$, then $[x + y] = [y + z] = 0$:

$$
\begin{aligned}
(x \star y) \star z &= (x + y - [x + y]) \star z \\
&= x + y + z - [x + y + z] \\
&= x \star (y + z - [y + z]) \\
&= x \star (y \star z)
\end{aligned}
$$

- If $1 \leq x + y, y + z < 2$, then $[x + y] = [y + z] = 1$:

$$
\begin{aligned}
(x \star y) \star z &= (x + y - [x + y]) \star z \\
&= (x + y - 1) + z - [x + y - 1 + z] \\
&= x + (y + z - 1) - [x + y + z - 1] \\
&= x \star (y + z - 1) - [x + (y + z - 1)] \\
&= x \star (y + z - [y + z]) \\
&= x \star (y \star z)
\end{aligned}
$$

- If $1 \leq x + y < 2$ and $0 \leq y + z < 1$, then $[x+y] = 1$ and $[y+z] = 0$. The case of $0 \leq x + y < 1$ and $1 \leq y + z < 2$ is similar:

$$
\begin{aligned}
(x \star y) \star z &= (x + y - [x+y]) \star z \\
&= (x + y - 1) + z - [x + y - 1 + z] \\
&= x + y - 1 + z - ([x + y + z] - 1) \\
&= x + y + z - 1 - [x + y + z] + 1 \\
&= x + y + z - [x + y + z] \\
&= x \star (y + z - [y + z]) \\
&= x \star (y \star z)
\end{aligned}
$$

Then $\star$ is associative. Moreover, commutativity of regular addition implies commutativity of G. For the identity element, note that $0 \in G$ and $0 \star x = x + 0 - [x] = x$. To determine the inverse of some $x \in G$, suppose $w \in G$ such that $x \star w = 0$. Then $x + w - [x + w] = 0$. Note that $0 \leq x + w < 2$, so $[x + w] = 0$ or 1. If $[x+w] = 0$, then $w = -x$. Since $w, x \in G$, then this is when $x = w = 0$. If $[x + w] = 1$, then $w = 1 - x$ for $0 < x < 1$. Hence, G is closed under inverses and is a group. $\qquad\square$

(8) Let $G = \{z \in \mathbb{C} : z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

   (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.

   Solution.

   (a) Note that $1 \in G$, so G has an identity. Moreover, if $z z^{-1} = 1$ for some $z \in G$, then $z^{-1} = 1/z \in G$ because $(1/z)^n = 1/z^n = 1$. Lastly, let $z, w \in G$, where $z^n = 1$ and $w^m = 1$ for $n, m \in \mathbb{Z}^+$. Then

   $$ (zw)^{mn} = (z^n)^m (w^m)^n = 1 $$

   so that $zw \in G$. Moreover, multiplication is associative in G since $G \subseteq \mathbb{C}$.
   (b) Note that $1, -1 \in G$, but $1 + (-1) = 0 \notin G$, since there is no n such that $0^n = 1$. $\qquad\square$

(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 multiplicative inverses.]

   Solution.

   (a) Since $0 + 0\sqrt{2} = 0 \in G$, then G has an identity. Moreover, for any $a + b\sqrt{2} \in G$, it has inverse $-a - b\sqrt{2} \in G$. Associativity in G follows from associativity in $\mathbb{R}$, and for $a + b\sqrt{2}, c + d\sqrt{2} \in G$, we have $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$, where $a + b, c + d \in q$ so that it is closed under addition. Hence, G is a group.
   (b) Since $1 + 0\sqrt{2} = 1 \in G$, then G has identity. Moreover, for $a + b\sqrt{2}$, we take:

   $$ \frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} $$

   where $a^2 - 2b^2 \neq 0$ (otherwise, then $a/b = \pm\sqrt{2}$, which is impossible). Then G is closed under inverses. Associativity in G follows from associativity of multiplication in $\mathbb{R}$, and for $a + b\sqrt{2}, c + d\sqrt{2} \in G$, we have $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$ where $ac + 2bd, ad + bc \in \mathbb{Q}$ so that G is closed under multiplication. Then G is a group. $\qquad\square$

(10) Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

   Solution. Let G be a finite group with elements $g_1, g_2, \ldots, g_n$ for finite n and $g_1 = 1$. Then G is abelian if and only if $g_i g_j = g_j g_i$ for any i, j if and only if the group table is a symmetric matrix. $\qquad\square$

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

Solution. For each $\overline{x} \in \mathbb{Z}/12\mathbb{Z}$, add it to itself until we arrive at $\overline{0}$. $|\overline{0}| = 1$, and $\overline{1} = 12$ since $12 \cdot \overline{1} = \overline{12} = \overline{0}$. In particular, we have:

$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$|\overline{x}|$	1	12	6	4	3	12	2	12	3	4	6	12

$\square$

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

Solution.

$\overline{x}$	$\overline{1}$	$\overline{-1}$	$\overline{5}$	$\overline{7}$	$\overline{-7}$	$\overline{13}$
$|\overline{x}|$	1	2	2	2	2	1

$\square$

(13) Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: $\overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.

Solution.

$\overline{x}$	$\overline{1}$	$\overline{2}$	$\overline{6}$	$\overline{9}$	$\overline{10}$	$\overline{12}$	$\overline{-1}$	$\overline{-10}$	$\overline{-18}$
$|\overline{x}|$	36	18	6	4	18	3	36	18	2

$\square$

(14) Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{13}, \overline{-13}, \overline{17}$.

Solution.

$\overline{x}$	$\overline{1}$	$\overline{-1}$	$\overline{5}$	$\overline{13}$	$\overline{-13}$	$\overline{17}$
$|\overline{x}|$	1	2	6	3	6	2

$\square$

(15) Prove that $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1}$ for all $a_1, a_2, \ldots, a_n \in G$.

Solution. For $n = 1$, the result follows. Suppose it holds for $n = k \in \mathbb{Z}^+$. For $n = k + 1$, we have:

$$(a_1 a_2 \ldots a_k a_{k+1})^{-1}(a_{k+1}^{-1} a_k^{-1} \ldots a_2^{-1} a_1^{-1}) = (a_1 a_2 \ldots a_k)(a_{k+1} a_{k+1}^{-1})(a_k^{-1} \ldots a_2^{-1} a_1^{-1})$$
$$= (a_1 a_2 \ldots a_k)^{-1}(a_k^{-1} \ldots a_2^{-1} a_1^{-1})$$
$$= 1$$

The result follows by induction. $\square$

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

Solution. If $x^2 = 1$, then $|x| \le 2$. Then $|x| = 1$ or 2. If $|x| = 1$, then $x = 1$, and $x^2 = 1^2 = 1$. If $|x| = 2$, then $x^2 = 1$. $\square$

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

Solution. Note that $x^n = x^{n-1} x = 1$. Then $x^{n-1} = x^{-1}$. $\square$

(18) Let x, y be elements of G. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

Solution.

$$xy = yx$$
$$y^{-1}xy = y^{-1}yx$$
$$y^{-1}xy = x$$
$$x^{-1}y^{-1}xy = x^{-1}x$$
$$x^{-1}y^{-1}xy = 1$$

$\square$

(19) Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.

    (a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.

    (b) Prove that $(x^a)^{-1} = x^{-a}$.

    (c) Establish part (a) for arbitrary integers a and b (positive, negative, or zero).

    Solution.

    (a) Since x^a has a amount of x and x^b has b amount of x, and x^{a+b} has $a + b$ amount of x, the result follows. Similarly, b amount of x^a means there are ab amount of x, or x^{ab}.

    (b) Note that $x^{-a} = (x^{-1})^a$. For $a = 1$, this follows. Suppose $(x^a)^{-1} = (x^{-1})^a$ for $a = n \in \mathbb{Z}^+$. Then for $a = n+1$, we have $(x^{-1})^{n+1}(x^{n+1}) = (x^{-1})^n x^{-1} x x^n = 1$, which is true by the inductive hypothesis.

    (c) The case where both a and b are positive is done. If $a \in \mathbb{Z}$ and $b = 0$, then $x^{a+0} = x^a x^0 = x^a$. Moreover, we have $(x^a)^0 = 1$ by definition, so $x^{a \cdot 0} = x^0 = 1$. If $a > 0$ and $b < 0$, we have two cases for the first part of (a):

       • If $a + b > 0$, then $x^a = x^{a+b-b} = x^{a+b} x^{-b}$. Then $x^a x^b = x^{a+b}$.

       • If $a + b < 0$, then $x^b = (x^{-b})^{-1} = (x^{-(a+b)+a})^{-1} = (x^{-(a+b)} x^a)^{-1} = (x^a)^{-1}(x^{-(a+b)})^{-1} = x^{-a} x^{a+b}$. Then $x^a x^b = x^{a+b}$.

    For the second part of (a), we have $(x^a)^b = ((x^a)^{-b})^{-1} = (x^{-ab})^{-1} = x^{ab}$. Next, the case of $a < 0$ and $b > 0$ is similar. Lastly, if $a < 0$ and $b < 0$, then $x^{a+b} = (x^{-b-a})^{-1} = (x^{-b} x^{-a})^{-1} = (x^{-a})^{-1}(x^{-b})^{-1} = x^a x^b$. Additionally, $(x^a)^b = ((x^a)^{-b})^{-1} = (x^{-ab})^{-1} = ((x^{ab})^{-1})^{-1} = x^{ab}$. $\qquad\square$

(20) For x an element in G, show that x and x^{-1} have the same order.

    Solution. Let $|x| = n \in \mathbb{Z}^+$. Then $(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$, so $|x^{-1}| \leq |x|$. If $|x^{-1}| = m \in \mathbb{Z}^+$, then $x^m = (x^{-1})^{-m} = ((x^{-1})^m)^{-1} = 1^{-1} = 1$, ,so $|x| \leq |x^{-1}|$. Hence, $n = m$. This establishes that the orders are the same if it is finite; otherwise, both $|x|$ and $|x^{-1}|$ must be of infinite order. $\qquad\square$

(21) Let G be a finite group and let x be an element of order n. Prove that if n is odd, then $x = (x^2)^k$ for some $k \geq 1$.

    Solution. Put $n = 2k - 1$ for $k \geq 1$. Then $1 = x^n = x^{2k-1} = (x^2)^k x^{-1}$. The result follows. $\qquad\square$

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

    Solution. We first prove that $(g^{-1} x g)^n = g^{-1} x^n g$ by induction. For $n = 1$, the result is clear. Supposing it is true for some $n = k$, then for $n = k + 1$, we have $(g^{-1} x g)^{k+1} = (g^{-1} x g)^k (g^{-1} x g) = (g^{-1} x^k g)(g^{-1} x g) = g^{-1} x^{k+1} g$.

    Put $|x| = n \in \mathbb{Z}^+$. Then $(g^{-1} x g)^n = g^{-1} x^n g = g^{-1} 1 g = 1$ so that $|g^{-1} x g| \leq n$. Similarly, put $|g^{-1} x g| = m$. Then $1 = (g^{-1} x g)^m = g^{-1} x^m g$. Then $1 = x^m$ so that $|x| \leq m$, hence $|x| = |g^{-1} x g|$. Similar to the previous exercise, then both must be of finite or infinite order. Finally, for $a, b \in G$, we have $|ab| = |b(ab)b^{-1}| = |ba|$. $\qquad\square$

(23) Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s and t, prove that $|x^s| = t$.

    Solution. Let $|x^s| = r$. Since $1 = x^n = x^{st} = (x^s)^t$, then $|x^s| \leq t$. Moreover, we have $(x^s)^r = x^{sr} = 1$ so that $|x| = st \leq sr$. Then $t \leq |x^s|$. $\qquad\square$

(24) If a and b are commuting elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. [Do this by induction for positive n first.]

    Solution. The case for $n = 1$ is clear. Supposing the result holds for $n = k$, then for $n = k + 1$, we have $(ab)^{k+1} = (ab)^k(ab) = a^k b^k ab = a^{k+1} b^{k+1}$. The result for $n = 0$ is trivial, and for $n < 0$, we have $(ab)^n = (ba)^n = ((ba)^{-n})^{-1} = (b^{-n} a^{-n})^{-1} = a^n b^n$. $\qquad\square$

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

    Solution. Note that $x^2 = 1$ implies $x = x^{-1}$ for any $x \in G$. Then for $a, b \in G$, we have that $ab = (ab)^{-1} = b^{-1} a^{-1} = ba$. $\qquad\square$

(26) Assume H is a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all $h, k \in H$, hk, $h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H (such a subset H is called a *subgroup* of G).

Solution. Since $hk, h^{-1} \in H$, then H has existence of inverse and closure. Moreover, $\star$ is associative in H due to associativity in G. Lastly, there exists $h \in H$ since it is nonempty. Then $h^{-1} \in H$ so that $hh^{-1} = 1 \in H$. Hence, $(H, \star)$ is a group. $\qquad\square$

(27) Prove that if x is an element of the group G, then $\{x^n : n \in \mathbb{Z}\}$ is a subgroup. (cf. the preceding exercise) of G (called the *cyclic subgroup* of G generated by x).

Solution. Let $x^m, x^n \in G$. Then $x^m x^n = x^{m+n} \in G$ since $m + n \in \mathbb{Z}$. Moreover, $x^{-n} \in G$ since $-n \in \mathbb{Z}$ so that the set has an inverse. Additionally, $x^0 = 1$ is in the set. Then the set is a subgroup of G. $\qquad\square$

(28) Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product (as defined in Example 6). Verify all the group axioms for $A \times B$:

  (a) Prove that the associative law holds:

$$\text{for all } (a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B, [(a_1, b_1)(a_2, b_2)](a_3, b_3) = (a_1, b_1)[(a_2, b_2)(a_3, b_3)]$$

  (a) Prove that $(1, 1)$ is the identity of $A \times B$, and

  (b) Prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

Solution.

  (a) Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B$. Then

$$
\begin{aligned}
[(a_1, b_1)(a_2, b_2)](a_3, b_3) &= (a_1 a_2, b_1 b_2)(a_3, b_3) \\
&= ((a_1 a_2)a_3, (b_1 b_2)b_3) \\
&= (a_1(a_2 a_3), b_1(b_2 b_3)) \\
&= (a_1, b_1)(a_2 a_3, b_2 b_3) \\
&= (a_1, b_1)[(a_2, b_2)(a_3, b_3)]
\end{aligned}
$$

  (b) For $a \in A, b \in B$, we have $(a, b)(1, 1) = (a \star 1, b \diamond 1) = a, b)$.

  (c) We have $(a, b)(a^{-1}, b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (1, 1)$. $\qquad\square$

(29) Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

Solution. Let $a, a' \in A$ and $b, b' \in B$. Suppose $A \times B$ is abelian. Then

$$(aa', bb') = (a, b)(a', b') = (a', b')(a, b) = (a'a, b'b)$$

so that A and B are abelian. If A and B are both abelian, then

$$(a, b)(a', b) = (aa', bb') = (a'a, b'b) = (a', b')(a, b)$$

hence $A \times B$ is abelian. $\qquad\square$

(30) Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

Solution. We have $(a, 1)(1, b) = (a1, 1b) = (1a, b1) = (1, b)(a, 1)$. Let $\ell = \operatorname{lcm}(|a|, |b|)$ so that $\ell = m|a| = n|b|$ for $m, n \in \mathbb{Z}$. Put $|(a, b)| = k$. Since $(a, b)^k = (a^k, b^k) = (1, 1)$, then $|a|$ and $|b|$ must divide k so that $\ell \le k$. Moreover, we have $(a, b)^\ell = (a^\ell, b^\ell) = (a^{m|a|}, b^{n|b|}) = (1^m, 1^n) = (1, 1)$ so that $k \le \ell$. The result follows. $\qquad\square$

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

Solution. Note that if $g \in G$, then $g^{-1} \in G$ so that the elements of $t(G)$ come in pairs. Then $|t(G)|$ is even, and $|G - t(G)|$ is also even. Moreover, $1 \notin t(G)$ since $1^{-1} = 1$. Then $1 \in G - t(G)$ so that it is nonempty, and there must exist $h \in G - t(G)$ such that $h = h^{-1}$ and $h \neq 1$ (because $|G - t(G)| \le 2$). Then $h^2 = 1$. $\qquad\square$

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

Solution. Suppose x^a, x^b are not distinct for $1 \le a < b < n$. Then $x^{b-a} = 1$. But then $b - a < n$, contradicting that $|x| = n$. It follows that $|x| \le |G|$. □

(33) Let x be an element of finite order in G.
  (a) Prove that if n is odd then $x^i \ne x^{-i}$ for all $i = 1, 2, \ldots, n - 1$.
  (b) Prove that if $n = 2k$ and $1 \le i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

  Solution.
  (a) Let $i \le n$. Then $x^i x^{n-i} = 1$ and $x^{-i} = x^{n-1}$. By Exercise (32), then $x^i \ne x^{n-i}$ when $i \ne n - i$. Then $x^i \ne x^{-i}$. For odd n, certainly $i \ne i$ so the result follows.
  (b) For $1 \le i < n$ where $i \ne k$, then $i \ne n - i$ so that $x^i \ne x^{n-i}$ by the previous part. Moreover, if $i = k$, then $x^i x^i = 1$ and $x^i = x^{-i}$. □

(34) If x is an element of infinite order in G, prove that the elements x^n, $n \in \mathbb{Z}$ are all distinct.

  Solution. Suppose $x^m = x^n$ for $m \ne n$. Then $x^{m-n} = 1$, which is a contradiction. □

(35) If x is an element of finite order in G, use the Division Algorithm to show that any integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup (cf. Exercise 27 above) of G generated by x).

  Solution. Let $x^k \in G$ and $|x| = n$. Then $k = nq + r$ for $0 \le r < n$ and $q \in \mathbb{Z}$. Then $x^k = x^{nq+r} = x^{nq} x^r = 1 x^r = x^r$. □

(36) Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4 (so by Exercise 32, every element has order ≤ 3). Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.

  Solution. Since no element has order 4, then each of the elements must have order 2. Now consider ab (without loss of generality; we may use bc or ac). If $ab = 1$, then $a = b^{-1}$, which cannot be true since $b = b^{-1}$ because $b^2 = 1$. Moreover, $ab \ne a$ since $b \ne 1$. Similarly, $ab \ne b$. It must be that $ab = c$. Moreover, $a^2 b = ac$ so that $ba^{-1} = aca^{-1} = a(ab)a = ba$. Using similar reasoning, we deduce that $bc = cb = a$ and $ac = ca = b$. Then we have the group table:

·	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

  □

1.2   Dihedral Groups

In these exercises, D_{2n} has the usual presentation $D_{2n} = \langle r, s \mid r^n = s^2 = 1, \ rs = sr^{-1} \rangle$.

(1) Compute the order of each of the elements in the following groups:
  (a) D_6
  (b) D_8
  (c) D_{10}

  Solution. Note that for any sr^k for $1 \le k \le n - 1$, we have $(sr^k)(sr^k) = s(r^k s)r^k = s(sr^{-k})r^k = s^2 = 1$ so that $|sr^k| = 2$. All that's left for the rest of the exercises is to calculate the order of the rotations:
  (a) $D_6 = \{1, r, r^2, s, sr, sr^2\}$. Then $|1| = 1$ and $|r| = |r^2| = 2$.
  (b) $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Then $|1| = 1, |r^2| = 2$ and $|r| = |r^3| = 4$.
  (c) $D_{10} = \{1, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}$. Then $|1| = 1$ and $|r| = |r^2| = |r^3| = |r^4| = 5$. □

(2) Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.

Solution. If $x \neq r^k$, then $x = sr^k$. Then $r(sr^k) = (sr^{-1})r^k = sr^k r^{-1}$. $\square$

(3) Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2. [cf. Exercise 33 of Section 1.]

Solution. See Exercise (1) from this section for the solution to the first part. For any $r^i \in D_{2n}$, then $(s(sr))^i = r^i$, and for any $sr^i \in D_{2n}$, then $s(s(sr))^i = sr^i$ so that D_{2n} is generated by $\{s, sr\}$. $\square$

(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}. [cf. Exercise 33 of Section 1.]

Solution. Clearly $r^k \neq 1$, and $(r^k)^2 = r^n = 1$ so that $|r^k| = 2$. Noting that $r^k = r^{-k}$ since $r^{2k} = 1$, then for any $s^i r^j$ where $i \in \{0,1\}$ and $1 \leq j \leq n-1$, then $(s^i r^j)r^k = (s^i r^k)r^j = (r^{-k}s^i)r^j = r^k(s^i r^j)$ so that r^k commutes with any element.
  Suppose now that there existed a nonidentity element $w \in D_{2n}$ that commutes with every element of D_{2n}. In particular, w must commute with s, i.e., $sw = ws$. There are two cases to discuss:
  - If $w = r^t$ for some $t \in \mathbb{Z}$, then $sw = sr^t$ and $ws = r^t s$. Then $sr^t = r^t s$, or $sr^t = sr^{-t}$, implying that $t = k$ by [Section 1, Exercise (33)].
  - If $w = sr^t$, then $sw = r^t$ and $ws = r^{-t}$, implying that $t = 0$ or $t = k$. Then $w = s$ or $w = sr^k$. Since s does not commute with r, then that cannot be. If $w = sr^k$, then $sr^{k+1} = rsr^k = sr^{k-1}$, or that $k = 2$, contradicting that $n \geq 4$. Hence, it follows that w cannot be a reflection.
  Then $w = r^k = z$, making it unique. $\square$

(5) If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}. [cf. Exercise 33 of Section 1.]

Solution. Use the odd case in [Section 1, Exercise (33)]. $\square$

(6) Let x and y be elements of order 2 in any group G. Prove that if $t = xy$, then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, y satisfy the same relations in G as s, r do in D_{2n}).

Solution. Note that $|x| = |y| = 2$, so $x = x^{-1}$ and $y = y^{-1}$. Then $tx = xyx = xy^{-1}x^{-1} = xt^{-1}$. $\square$

(7) Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle$ gives a presentation for D_{2n} in terms of the two generators a and b of order 2 computed in Exercise 3 above. [Show that the relations for r and s follow from the relations for a and b and conversely, the relations for a and b follow from those for r and s.]

Solution. Suppose $a^2 = b^2 = (ab)^n = 1$. The first natural choice is to let $a = s$ so that $s^2 = 1$. The next one is that $ab = r$ so that $r^n = 1$. Since $sb = r$, then $b = s^{-1}r = sr$. Moreover, $sr = b = b^{-1} = r^{-1}s^{-1} = r^{-1}s$ so that we have the regular presentation of D_{2n}.
  Using the regular representation, then $a^2 = s^2 = 1$ and $b^2 = srsr = ssr^{-1}r = 1$. Moreover, we have $(ab)^n = (s(sr))^n = r^n = 1$, and we have the resulting presentation. $\square$

(8) Find the order of the cyclic subgroup of D_{2n} generated by r (cf. Exercise 27 of Section I).

Solution. Let $G = \langle r \rangle$ be the cyclic subgroup of D_{2n} generated by r. Clearly $\{1, r, r^2, \ldots, r^{n-1}\} \subseteq G$ so that $|G| \geq n$. Moreover, for $r^k \in G$, we may use the division algorithm to write $k = nq + x$ for $0 \leq r < n$, and $r^k = r^{nq+x}$ so that $r^k = r^x$, where r^x is any one of the elements in G by definition. Then $G \subseteq \{1, r, r^2, \ldots, r^{n-1}\}$ so that $|G| = n$. $\square$

In each of Exercises 9 to 13 you can find the order of the group of rigid motions in $\mathbb{R}^3$ (also called the group of rotations) of the given Platonic solid by following the proof for the order of D_{2n}: find the number of positions to which an adjacent pair of vertices can be sent. Alternatively, you can find the number of places to which a given face may be sent and, once a face is fixed, the number of positions to which a vertex on that face may be sent.

(9) Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

Solution. Label the vertices of a tetrahedron 1 through 4 so that vertex 1 has 4 choices. Then vertex 2 has 3 remaining choices, and vertex 3 and 4 are determined after. It follows that $4(3) = 12$ symmetries.   □

(10) Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.

Solution. 8 choices for vertex 1 and 3 adjacent vertices for vertex 2; $8(3) = 24$ symmetries.   □

(11) Let G be the group of rigid motions in $\mathbb{R}^3$ of an octahedron. Show that $|G| = 24$.

Solution. 6 choices for vertex 1 and 4 adjacent vertices for vertex 2; $6(4) = 24$ symmetries.   □

(12) Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.

Solution. 20 choices for vertex 1 and 3 adjacent vertices for vertex 2; $20(3) = 60$ symmetries.   □

(13) Let G be the group of rigid motions in $\mathbb{R}^3$ of an icosahedron. Show that $|G| = 60$.

Solution. 12 choices for vertex 1 and 5 adjacent vertices for vertex 2; $12(5) = 60$ symmetries.   □

(14) Find a set of generators for $\mathbb{Z}$.

Solution. Any integer is of the form $n1$, so $\mathbb{Z} = \langle 1 \rangle$.   □

(15) Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.

Solution. Each element of $\mathbb{Z}/n\mathbb{Z}$ is of the form $k\bar{1}$ for $0 \le k < n$. Then $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \mid n\bar{1} = \bar{0} \rangle$.   □

(16) Show that the group $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \rangle$ is the dihedral group D_4 (where x_1 may be replaced by the letter r and y_1 by s). (Show that the last relation is the same as $x_1 y_1 = y_1 x_1^{-1}$.)

Solution. Note that $D_4 = \langle r, s \mid r^2 = s^2 = 1, rs = sr^{-1} \rangle$. Note that $r = r^{-1}$ so that $rs = sr$. Put $x_1 = r$ and $y_1 = s$. If $rs = sr$, then $(x_1 y_1)^2 = rsrs = r^2 s^2 = 1$. Moreover, if $(x_1 y)^2 = 1$, then $rsrs = 1$ so that $rs = sr$.   □

(17) Let X_{2n} be the group whose presentation is displayed in (1.2).
  (a) Show that if $n = 3k$, then X_{2n} has order 6, and it has the same generators and relations as D_6 when x is replaced by r and y by s.
  (b) Show that if $(3, n) = 1$, then x satisfies the additional relation: $x = 1$. In this case deduce that X_{2n} has order 2. [use the facts that $x^n = 1$ and $x^3 = 1$.]

Solution.
  (a) Applying $n = 3k$, we have $X_{2n} = X_{6k} = \langle x, y \mid x^{3k} = y^2 = 1, xy = yx^2 \rangle$. Now suppose the given relations, and recall the text showing $x^3 = 1$. Set $x = r$ and $y = s$. Then $r^3 = 1$ and $s^2 = 1$. From $xy = yx^2$, we have $rs = sr^2 = sr^{-1}$.
      Suppose now that $r^3 = s^2 = 1$ and $rs = sr^{-1}$. Then $x^{3k} = (x^3)^k = 1$. Moreover, $s^2 = y^2 = 1$, and $xy = rs = sr^{-1} = sr^2 = yx^2$. Then the two representations are equal.
  (b) Note that $(3, n) = 1$ implies that $3a + nb = 1$ for some $a, b \in \mathbb{Z}$. Then $x = x^{3a+nb} = x^{3a} x^{nb} = (x^3)^a (x^n)^b = 1$. Then $X_{2n} = \{1, y\}$, and $|X_{2n}| = 2$.   □

(18) Let Y be the group whose presentation is displayed in (1.3).
  (a) Show that $v^2 = v^{-1}$. [Use the relation $v^3 = 1$.]
  (b) Show that v commutes with u^3. [Show that $v^2 u^3 v = u^3$ by writing the left-hand side as $(v^2 u^2)(uv)$ 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 $u^4 v^3 = 1$.]

Solution.

(a) $v^3 = 1 \implies v^2 = v^{-1}$.

(b) From $uv = v^2 u^2$, we have $vuv = u^2$ so that $vu = u^2 v^{-1} = u^2 v^2$. It follows that $v^2 u^3 v = (v^2 u^2)(uv) = (uv)(uv) = u(vu)v = u(u^2 v^2)v = u^3$.

(c) It follows that $u^9 = (u^4)^2 u = u$. Then $uv = (u^3)^3 v = v(u^3)^3 = vu$.

(d) $uv = v^2 u^2 = u^2 v^2$. Then $1 = uv$.

(e) $u^4 v^3 = u(uv)^3 = u 1^3 = 1$. Then $1v = 1$, and $u = v = 1$, so $Y = 1$. $\square$

1.3 Symmetric Groups

(1) Let σ be the permutation
$$1 \mapsto 3, \quad 2 \mapsto 4, \quad 3 \mapsto 5, \quad 4 \mapsto 2, \quad 5 \mapsto 1$$
and let τ be the permutation
$$1 \mapsto 5, \quad 2 \mapsto 3, \quad 3 \mapsto 2, \quad 4 \mapsto 4, \quad 5 \mapsto 1.$$

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

Solution.

$$\sigma = (1\ 3\ 5)(2\ 4)$$
$$\tau = (1\ 5)(2\ 3)$$
$$\sigma^2 = (1\ 5\ 3)$$
$$\sigma\tau = (2\ 5\ 3\ 4)$$
$$\tau\sigma = (1\ 2\ 4\ 3)$$
$$\tau^2\sigma = (1\ 3\ 5)(2\ 4)$$

$\square$

(2) Let σ be the permutation

$1 \mapsto 13$	$2 \mapsto 2$	$3 \mapsto 15$	$4 \mapsto 14$	$5 \mapsto 10$
$6 \mapsto 7$	$7 \mapsto 12$	$8 \mapsto 9$	$9 \mapsto 3$	$10 \mapsto 1$
$11 \mapsto 7$	$12 \mapsto 9$	$13 \mapsto 5$	$14 \mapsto 11$	$15 \mapsto 8$

and let τ be the permutation

$1 \mapsto 14$	$2 \mapsto 9$	$3 \mapsto 10$	$4 \mapsto 2$	$5 \mapsto 12$
$6 \mapsto 6$	$7 \mapsto 5$	$8 \mapsto 11$	$9 \mapsto 15$	$10 \mapsto 3$
$11 \mapsto 8$	$12 \mapsto 7$	$13 \mapsto 4$	$14 \mapsto 1$	$15 \mapsto 13$

Find the cycle decompositions of the following permutations: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma$, and $\tau^2\sigma$.

Solution.

$$\sigma = (1\ 13\ 5\ 1)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)$$
$$\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)$$
$$\sigma^2 = (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)(10\ 13)$$
$$\sigma\tau = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(8\ 10\ 14)$$
$$\tau\sigma = (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14)$$
$$\tau^2\sigma = (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)$$

$\square$

(3) For each of the permutations whose cycle decompositions were computed in the preceding two exercises, compute its order.

Solution. Note that the order of a cycle decomposition is the lcm of the orders of each of the cycles, and that the order of an m-cycle is m. Then the orders are the following (the first number will be for Exercise 1, and the second for Exercise 2):

$$|\sigma| = 6, 12$$
$$|\tau| = 2, 30$$
$$|\sigma^2| = 3, 6$$
$$|\sigma\tau| = 4, 6$$
$$|\tau\sigma| = 4, 6$$
$$|\tau^2\sigma| = 6, 13$$

$\square$

(4) Compute the order of each of the elements in the following groups:

  (a) S_3

  (b) S_4

Solution.

  (a)

Permutation	Order
1	1
(12)	2
(13)	2
(23)	2
(123)	3
(132)	3

  (b)

Permutation	Order	Permutation	Order	Permutation	Order	Permutation	Order
1	1	(34)	2	(143)	3	(1342)	4
(12)	2	(123)	3	(234)	3	(1423)	4
(13)	2	(124)	3	(243)	3	(1432)	4
(14)	2	(132)	3	(1234)	4	(12)(34)	2
(23)	2	(134)	3	(1243)	4	(13)(24)	2
(24)	2	(142)	3	(1324)	4	(14)(23)	2

$\square$

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

Solution. $\text{lcm}(5, 2, 3) = 30$. $\square$

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

Solution. See Exercise 4. $\square$

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

Solution. See Exercise 4. $\square$

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

Solution. Consider the permutation $\sigma_n = (2n-1 \ 2n)$. Note that $\sigma_i \neq \sigma_j$ for any $i, j \in \mathbb{Z}^+$ so that the set $A = \{\sigma_n \mid n \in \mathbb{Z}^+\}$ are all distinct. Moreover, A is an infinite subset of S_Ω so that $|S_\Omega| = \infty$. $\square$

(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). For which positive integers i is ω^i also a 14-cycle?

Solution.

(a) We will compute the explicit powers for the first problem, notice a pattern with the integers that produce a 12-cycle, and apply that pattern to the other problems.

For each integer between 1 and 11, we compute the cycle:

$$\sigma^1 = \sigma$$
$$\sigma^2 = (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12)$$
$$\sigma^3 = (1\ 4\ 7\ 10)(2\ 5\ 8\ 11)(3\ 6\ 9\ 12)$$
$$\sigma^4 = (1\ 5\ 9)(2\ 6\ 10)(3\ 7\ 11)(4\ 8\ 12)$$
$$\sigma^5 = \sigma$$
$$\sigma^6 = (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12)$$
$$\sigma^7 = \sigma$$
$$\sigma^8 = \sigma^4$$
$$\sigma^9 = \sigma^3$$
$$\sigma^{10} = \sigma^2$$
$$\sigma^{11} = \sigma$$

From direct calculations, it seems that the integers i such that $(12, i) = 1$ produce a 12-cycle, while i such that $(12, i) = k$ produces k $12/k$-cycles. In this particular case, the set of integers that produce a 12-cycle is the set $\{x + 12k \mid x \in \{1, 5, 7, 11\}, k \in \mathbb{Z}\}$.

(b) $\{x + 8k \mid x \in \{1, 3, 5, 7\}, k \in \mathbb{Z}\}$.

(c) $\{x + 14k \mid x \in \{1, 3, 5, 9, 11, 13\}, k \in \mathbb{Z}\}$.   □

(10) Prove that if σ is the m-cycle $(a_1\ a_2\ \ldots\ a_m)$, then for all $i \in \{1, 2, \ldots, m\}$, $\sigma^i(a_k) = a_{k+i}$, where $k + i$ is replaced by its least residue mod m when $k + i > m$. Deduce that $|\sigma| = m$.

Solution. We prove the first part by induction. Clearly for $i = 1$, this holds true by definition of cycles. Suppose it holds true for some $i \in \mathbb{Z}^+$. Then $\sigma^{i+1}(a_k) = \sigma(\sigma^i(a_k)) = \sigma(a_{k+i}) = a_{k+i+1}$.

Now suppose $1 \le i < m$. Then $\sigma^i(a_1) = a_{1+i} \ne a_1$. But then $\sigma^m(a_1) = a_{1+m} = a_1$ since $(1 + m) \mod m = 1$. Then $|\sigma| = m$.   □

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

Solution. Suppose σ^i is an m-cycle, and put $(m, i) = d$. Then there exists $a, b \in \mathbb{Z}^+$ such that $ad = i$ and $bd = m$. Noting that $|\sigma^i| = m$ because it is an m-cycle, then $(\sigma^i)^b = (\sigma^{ad})^b = (\sigma^{bd})^a = (\sigma^m)^a = 1^a = 1$. Then $|\sigma^i| \le b$, or $m = b$. It follows that $d = 1$.

Suppose that $(m, i) = 1$, and denote $x' \equiv x \mod m$. Note that the integers $(1+i)', (1+2i)', \ldots, (1+(m-1)i)'$ are all distinct, since for any $0 \le x, y \le m-1$ such that $x \ne y$, then $xi \equiv yi \mod m$ implies $x = y$ (This is seen as follows: $i(x - y) \equiv 0 \mod m$ implies that $m \mid (x - y)$, since $(m, i) = 1$. Since $1 - m \le x - y \le m - 1$, then the only choice for $x - y$ is 0, or that $x = y$). Then we have m integers so that

$$\sigma^i = (1\ (1+i)'\ (1+2i)'\ldots(1+(m-1)i)'),$$

and σ^i is an m-cycle.   □

(12) (a) If $\tau = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$, determine whether there is an n-cycle ($n \ge 10$) with $\tau = \sigma^k$ for some integer k.

(b) If $\tau = (1\ 2)(3\ 4\ 5)$, determine whether there is an n-cycle ($n \ge 5$) with $\tau = \sigma^k$ for some integer k.

Solution.

(a) $\sigma = (1\ 3\ 5\ 7\ 9\ 2\ 4\ 6\ 8\ 10), \sigma^5 = \tau$.

(b) We first prove that $(ac, bc) = c(a, b)$. Let $d = (a, b)$ and $d' = (ac, bc)$. Then there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$. Then $acx + bcy = dc$. Since d' is the smallest integer that is written of the form $acx' + bcy'$ for $x', y' \in \mathbb{Z}$ (if there were any greater, then $d' \neq (ac, bc)$), then $d' \leq dc$. Moreover, $d \mid a$ and $d \mid b$ implies $cd \mid ac$ and $cd \mid bc$. Then $cd \mid d'$, or $cd \leq d'$. Then $dc = d'$, or $c(a, b) = (ac, dc)$.

Suppose there existed some n-cycle σ and k such that $\sigma^k = \tau$. Then $\sigma^{2k}(1) = 1$, or $2k \equiv 0 \bmod n$. Moreover, $\sigma^{3k}(3) = 3$, or that $3k \equiv 0 \bmod n$. Then $n \mid 2k$ and $n \mid 3k$ so that $n \mid (2k, 3k)$. By the above, then $(2k, 3k) = k(2, 3) = k$, and $n \mid k$. But then $\sigma^k = (\sigma^n)^q = 1$, contradicting that $\sigma^k = \tau$. $\qquad\square$

(13) Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

Solution. Suppose $\sigma \in S_n$ such that $|\sigma| = 2$. Perform cycle decomposition on σ so that it becomes a product of commuting, disjoint cycles. Pick one of the cycles $(a_1\ a_2 \dots a_m)$. Since $\sigma \neq 1$, then $\sigma(a_1) = a_2$ and $\sigma^2(a_1) = a_3$. However, $\sigma^2 = 1$, so $\sigma^2(a_1) = a_1$ so that $a_1 = a_3$. Then $m \leq 2$, and the cycle is $(a_1\ a_2)$ so that any cycle in the cycle decomposition of σ is of length 2.

Suppose $\sigma = (a_1\ b_1)(a_2\ b_2) \dots (a_k\ b_k)$. Since $(a_1\ b_1)^2 = 1$, and the 2-cycles commute, then $\sigma^2 = 1$. Moreover, because $\sigma \neq 1$, then $|\sigma| = 2$. $\qquad\square$

(14) Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

Solution. Suppose $\sigma \in S_n$ such that $|\sigma| = p$ that is prime. Put

$$\sigma = \pi_1 \pi_2 \dots \pi_k$$

as the cycle decomposition of σ so that π_i commutes with π_j for any $i \neq j$. Clearly, $\sigma^p = \pi_1^p \pi_2^p \dots \pi_k^p$. Since $\sigma^p = 1$, then each $\pi_i^p = 1$. Then π_i must be a p-cycle or $\pi_i = 1$. But no $\pi_i = 1$, since $\sigma \neq 1$. Then π_i must be a p-cycle.

Suppose σ's cycle decomposition is a product of commuting p-cycles π_i. Then for any $t < p$, we have

$$\sigma^t = \pi_1^t \pi_2^t \dots \pi_k^t \neq 1$$

since π_i is a p-cycle. If $t = p$, then $\sigma^t = 1$. Then $|\sigma| = p$. $\qquad\square$

(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.

Solution. Let $\sigma \in S_n$ have the cycle decomposition $\sigma = \pi_1 \pi_2 \dots \pi_k$, and let π_i have length p_i so that $|\pi_i| = p_i$. Suppose $|\sigma| = m$. Then $\pi_i^m = 1$ so that $p_i \mid m$. In particular, every p_i must divide m so that m is a common multiple of all p_i. Moreover, if there was another t such that $\sigma^t = 1$, then t must be a common multiple of all p_i and $m \leq t$ so that m is the least common multiple of all p_i. $\qquad\square$

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

$$\frac{n(n-1)(n-2)\dots(n-m+1)}{m}.$$

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

Solution. Note that in an m-cycle, there are m integers to write. The first integer has n choices, the second $n-1$ choices. Continuing on, then the m-th integer has $n-m+1$ choices. However, each choice of m integers has m equivalent representations (such as (1 2 3 4) being equivalent to (2 3 4 1) by shifting each integer to the left one place). Then take the product $n(n-1)(n-2)\dots(n-m+1)$ and divide by m. $\qquad\square$

(17) Show that if $n \geq 4$ then the number of permutations in S_n which are the product of two disjoint 2-cycles is $n(n-1)(n-2)(n-3)/8$.

Solution. The first 2-cycle has $n(n-1)/2$ choices, and the second 2-cycle has $(n-2)(n-3)/2$ choices. Moreover, there are 2 representations for the same set of 2-cycles, so multiply the above quantities and divide by 2 to obtain $n(n-1)(n-2)(n-3)/8$. $\qquad\square$

(18) Find all numbers n such that S_5 contains an element of order n.

Solution. S_5 contains elements of order 1 through 5. Moreover, we can have a 2 and 3-cycle together whose lcm is 6. Then $n = 1, 2, 3, 4, 5, 6$. □

(19) Find all numbers n such that S_7 contains a number an element of order n.

Solution. We have n from 1 to 7. We can have 2 and 5-cycles and 3 and 4-cycles. Then $n = 10$ and 12. □

(20) Find a set of generators and relations for S_3.

Solution. Recall that $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. Moreover, no element in S_3 has order 6 so that no element generates S_3. It must be that there are at least 2 generators. Put $\alpha = (1\ 2)$ and $\beta = (1\ 3)$. Then $\alpha^2 = \beta^2 = 1$. Then $|\alpha| = |\beta| = 2$, and $\alpha\beta = (1\ 3\ 2), \beta\alpha = (1\ 2\ 3)$, and $\alpha\beta\alpha = (2\ 3)$. Since $\alpha^2 = \beta^2 = 1$ is not enough to determine the order of $\alpha\beta$ (because $\alpha\beta \neq \beta\alpha$), then we must add $(\alpha\beta)^2 = 1$. Then we have the presentation $S_3 = \langle \alpha, \beta \mid \alpha^2 = \beta^2 = (\alpha\beta)^3 = 1 \rangle$. □

1.4   Matrix Groups

Let F be a field and let $n \in \mathbb{Z}^+$.

(1) Prove that $|\mathrm{GL}_2(\mathbb{F}_2)| = 6$.

Solution. Note that $\mathbb{F}_2 = \{0, 1\}$. Moreover, consider

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$$

The determinant is $ad - bc$, which is never 0 whenever a, d are nonzero or when b, c are nonzero, but not both. Then

$$\mathrm{GL}_2(\mathbb{F}_2) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

□

(2) Write out all the elements of $\mathrm{GL}_2(\mathbb{F}_2)$ and compute the order of each element.

Solution. By direct calcuation, we obtain the following:

A	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$
$|A|$	1	2	2	2	3	3

□

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

Solution.

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

□

(4) Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Solution. Since n is not prime, there exists $a, b \in \mathbb{Z}^+$ such that $n = ab$. Since $(a, n) \neq 1$, then Section 0, Proposition 4 says that a has no multiplicative inverse. □

(5) Show that $\mathrm{GL}_n(F)$ is a finite group if and only if F has a finite number of elements.

Solution. Suppose F is infinite. Note that the set $\{\alpha I \mid \alpha \in F^\times\} \subseteq \mathrm{GL}_n(F)$. Then $\mathrm{GL}_n(F)$ is infinite.

Suppose $|F| = m < \infty$. Then there are m^{n^2} potential $n \times n$ matrices, and less whose determinants are nonzero. Then $|\mathrm{GL}_n(F)|$ is finite. □

(6) If $|F| = q$ is finite prove that $|\text{GL}_n(F)| < q^{n^2}$.

Solution. See previous solution. □

(7) Let p be a prime. Prove that the order of $\text{GL}_2(\mathbb{F}_p)$ 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.]

Solution. Note that the number of 2×2 matrices with entries from $\mathbb{F}_p$ is p^4. Using the given fact, let r_1 denote the first row and r_2 the second row of the matrices. Then if $r_1 = k r_2$ for some $k \in \mathbb{F}_p$, then the matrix is linearly independent. We then cover the cases:

1. Suppose $r_1 = 0$. Then r_2 is automatically a multiple of r_1, and there are p^2 choices for r_2 since there are 2 entries.
2. Suppose $r_1 \neq 0$. Then we have $p^2 - 1$ choices for r_1. Since there are p scalars, then we have p choices for r_2 (take $k r_1$ for $k \in \{0, 1, \dots, p-1\}$). Then there are $(p^2 - 1)p = p^3 - p$ matrices that are not invertible.

The total of matrices that are not invertible is then $p^3 + p^2 - p$. The result follows. □

(8) Show that $\text{GL}_n(F)$ is non-abelian for any $n \geq 2$ and any F.

Solution. Note that every F has elements 0 and 1 as additive and mutliplicative identities respectively, so we may safely assume $\mathbb{F}_2$ to be our field.

Proceeding by induction, the case of $n = 2$ was proven in Exercise 3. Now suppose $\text{GL}_{n-1}(\mathbb{F}_2)$ is non-abelian for $n \geq 3$. Let $A, B \in \text{GL}_{n-1}(\mathbb{F}_2)$ be noncommuting matrices. Using a block matrix, then

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} BA & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$$

□

(9) Prove that the binary operation of matrix multiplication of 2×2 matrices with real number entries is associative.

Solution.

$$\begin{aligned}
\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right]\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} &= \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} \\
&= \begin{pmatrix} (aa' + bc')a'' + (ab' + bd')c'' & (aa' + bc')b'' + (ab' + bd')d'' \\ (ca' + dc')a'' + (cb' + dd')c'' & (ca' + dc')b'' + (cb' + dd')d'' \end{pmatrix} \\
&= \begin{pmatrix} aa'a'' + bca'' + ab'c'' + bd'c'' & aa'b'' + bc'b'' + ab'd'' + bd'd'' \\ ca'a'' + dc'a'' + cb'c' + dd'c' & ca'b'' + dc'b'' + cb'd'' + dd'd'' \end{pmatrix} \\
&= \begin{pmatrix} a(a'a'' + b'c'') + b(c'a'' + d'c'') & a(a'b'' + b'd'') + b(c'b'' + d'd'') \\ c(a'a'' + b'c'') + d(c'a'' + d'c'') & c(a'b'' + b'd'') + d(c'b'' + d'd'') \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a'a'' + b'c'' & a'b'' + b'd'' \\ c'a'' + d'c'' & c'b'' + d'd'' \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\left[\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}\right]
\end{aligned}$$

□

(10) Let

$$G = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{R}, a \neq 0, c \neq 0\right\}$$

(a) Compute the product of $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ to show that G is closed under matrix multiplication.

(b) Find the matrix inverse of $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and deduce that G is closed under inverses.

(c) Deduce that G is a subgroup of $GL_2(\mathbb{R})$ (cf. Exercise 26, Section 1).

(d) Prove that the set of elements of G whose two diagonal entries are equal (i.e., $a = c$) is also a subgroup of $GL_2(\mathbb{R})$.

Solution.

(a)
$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix}$$

Since $a_i \neq 0$ and $c_i \neq 0$, then $a_1 a_2 \neq 0$ and $c_1 c_2 \neq 0$ so that G is closed under matrix multiplication.

(b) The determinant is ac. We then have the inverse
$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \frac{1}{ac}\begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1/a & -b/ac \\ 0 & 1/c \end{pmatrix}$$

(c) Since G is closed under inverses and matrix multiplication, the result follows.

(d) Let $H = \{A \in G \mid a = c\}$. Then
$$\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 a_2 \\ 0 & a_1 a_2 \end{pmatrix} \in H$$

and
$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \frac{1}{a^2}\begin{pmatrix} a & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1/a & -b/a^2 \\ 0 & 1/a \end{pmatrix} \in H$$

Then H is closed under inverses and matrix multiplication, hence it is a subgroup of $GL_2(\mathbb{R})$. □

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

called the *Heisenberg group* over F. Let
$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \text{ and } Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

be elements of $H(F)$.

(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 of the group $H(\mathbb{R})$ has infinite order.

Solution.

(a) The product is calculated:
$$XY = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \in H(F)$$

Moreover, we have that

$$
\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\neq\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
$$

(b) To calculate the inverse, one can use Gaussian elimination:

$$
\left(\begin{array}{ccc|ccc} 1 & a & b & 1 & 0 & 0 \\ 0 & 1 & c & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)\implies\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -a & ac-b \\ 0 & 1 & 0 & 0 & 1 & -c \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)
$$

The right 3×3 matrix, call it Z, is the inverse of X and can be shown as such through direct calculation, i.e., $XZ=ZX=I$ so that $X^{-1}=Z$.

(c)

$$
\begin{aligned}
\left[\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\right]&\begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & a+d & af+b+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}\\
&=\begin{pmatrix} 1 & a+d+g & h+i(a+d)+af+b+e \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix}\\
&=\begin{pmatrix} 1 & a+d+g & ai+ad+af+b+e+h \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix}\\
&=\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d+g & di+e+h \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix}\\
&=\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\left[\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}\right]
\end{aligned}
$$

Moreover, there are 3 choices to vary in each matrix in $H(F)$, such as a,b,c in X. Then there are $|F|^3$ elements in $H(F)$.

(d) To save time, denote a matrix in $H(\mathbb{Z}/2\mathbb{Z})$ as the 3-tuple (a,b,c), where regular matrix multiplication is $(a,b,c)(d,e,f)=(a+d,af+b+e,c+f)$. Note that $(a,b,c)^2=(2a,ac+2b,2c)$. Since $a,b,c\in\mathbb{Z}/2\mathbb{Z}$, this degrades to $(0,ac,0)$. We then have two cases to consider:

  1. Suppose $ac=0$. Then at least one of a and c is 0, while b can be 0 or 1. Then the matrices are $(0,0,0),(1,0,0),(0,0,1),(0,1,0),(1,1,0),(0,1,1)$. Except for $(0,0,0)$ which is the identity matrix and thus has order 2, squaring the other matrices results in $(0,0,0)$ so that each have order 2.

  2. Suppose $ac=1$. Then this occurs when both $a=c=1$ and b is either 0 or 1. These are the matrices $(1,1,0)$ and $(1,1,1)$. Since squaring these matrices results in $(0,0,1)$ which has order 2. then the aforementioned matrices have order 4.

(e) Utilizing the same formulation as in part (d), let $A=(a,b,c)\in H(\mathbb{R})$. We prove that

$$
(a,b,c)^n=(na,n(n-1)ac/2+nb,nc)
$$

To that end, it is clear that $n=1$ holds true. Suppose it holds for some n. Then for $n+1$, we have

$$
\begin{aligned}
(a,b,c)^{n+1}&=(a,b,c)^n(a,b,c)\\
&=(na,n(n-1)ac/2+nb,nc)(a,b,c)\\
&=(na+a,(na)c+n(n-1)ac/2+nb+b,nc+c)\\
&=((n+1)a,n(n+1)ac/2+(n+1)b,(n+1)c)
\end{aligned}
$$

so that the relationship is true by induction. Since $A \neq I$, then at least one of a, b, c must be nonzero. Then for any $n \in \mathbb{Z}^+$, none of the integers $na, n(n-1)ac/2 + nb$, or nc are 0. Then no power of (a, b, c) results in $(0,0,0)$, hence no nonidentity element of $H(\mathbb{R})$ has any finite order. Therefore, every nonidentity element of $H(\mathbb{R})$ has infinite order.   □

1.5   The Quaternion Group

(1) Compute the order of each of the elements in Q_8.

Solution.

a	1	-1	i	$-i$	j	$-j$	k	$-k$
$|a|$	1	2	4	4	4	4	4	4

□

(2) Write out the group tables for S_3, D_8, and Q_8.

Solution. S_3:

$\circ$	1	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
1	1	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	1	(1 2 3)	(1 3 2)	(1 3)	(2 3)
(1 3)	(1 3)	(1 3 2)	1	(1 2 3)	(2 3)	(1 2)
(2 3)	(2 3)	(1 2 3)	(1 3 2)	1	(1 2)	(1 3)
(1 2 3)	(1 2 3)	(2 3)	(1 2)	(1 3)	(1 3 2)	1
(1 3 2)	(1 3 2)	(1 3)	(2 3)	(1 2)	1	(1 2 3)

D_8:

$\circ$	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	1	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

Q_8:

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	j	$-j$
$-i$	$-i$	i	1	-1	$-k$	k	$-j$	j
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

□

(3) Find a set of generators and relations for Q_8.

Solution. An extra relation is necessary to intertwine i, j, k together, so a presentation for Q_8 is:

$$Q_8 = \langle -1, i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle$$

□

1.6   Homomorphisms and Isomorphisms

(1) 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 $n \in \mathbb{Z}$.

Solution.

   (a) It is clear for $n = 1$. Supposing it holds for some n, then for $n+1$, we have $\varphi(x^{n+1}) = \varphi(x^n x) = \varphi(x^n)\varphi(x) = \varphi(x)^n \varphi(x) = \varphi(x)^{n+1}$.

   (b) We first prove that φ maps the identity of G to the identity of H. To that end, we have $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$ (which is the case for $n = 0$). By cancellation, then $1_H = \varphi(1_G)$ so that identities map to each other. Now see that $1_H = \varphi(1_G) = \varphi(x x^{-1}) = \varphi(x)\varphi(x^{-1})$. Then $\varphi(x^{-1}) = \varphi(x)^{-1}$. Then for some $n \in \mathbb{Z}^+$, it follows that

$$\varphi(x^{-n}) = \varphi((x^{-1})^n) = \varphi(x^{-1})^n = (\varphi(x)^{-1})^n = \varphi(x)^{-n}$$

                                                                         $\square$

(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?

Solution. Let $|x| = m$ and $|\varphi(x)| = n$ for finite $m, n \in \mathbb{Z}^+$. Then

$$\varphi(x)^m = \varphi(x^m) = \varphi(1) = 1$$

so that $n \leq m$. Moreover,

$$\varphi(x^n) = \varphi(x)^n = 1$$

Since identities map to identities, then $x^n = 1$, or $m \leq n$. Then $m = n$. If m was infinite but n was not, then $\varphi(x^n) = \varphi(x)^n = 1$ implies that $x^n = 1$, contradicting that x had infinite order. Hence, both must have infinite order. Moreover, two isomorphic groups must the same number of elements of some order because φ is a bijection, and $|x| = |\varphi(x)|$ for every $x \in G$.

    The result is not true if φ is only a homomorphism. Take $\varphi : G \to H$, where H is the trivial group $\{1\}$, defined by $\varphi(x) = 1$. Since there are elements in G that would have orders of greater than 1 (except if G is also the trivial group), then φ does not preserve order. $\square$

(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?

Solution. Note that φ^{-1} exists, since φ is bijective. It follows that both directions will be proved very similarly, so one direction is only shown: If G is abelian, then for any $h_1, h_2 \in H$, there exists $g_1, g_2 \in G$ such that $g_1 = \varphi^{-1}(h_1)$ and $g_2 = \varphi^{-1}(h_2)$. Then

$$h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2) = \varphi(g_2 g_1) = \varphi(g_2)\varphi(g_1) = h_2 h_1$$

so that H is abelian. Moreover, the result does not always follow if φ is only a homomorphism. Consider the mapping $\varphi : (\mathbb{R}, +) \to \mathrm{GL}_2(\mathbb{R})$ defined by

$$\varphi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

Clearly, this is a homomorphism as

$$\varphi(x+y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \varphi(x)\varphi(y)$$

Note that upper triangular matrices commute with each other (so that $\varphi(\mathbb{R})$ is abelian), but in general $\mathrm{GL}_2(\mathbb{R})$ is not abelian. It follows that if φ is assumed only to be a homomorphism, then we must add the additional condition that φ is also surjective. Following the proof above, we may conclude that such a g_1 and g_2 must exist because we may pick from the fibers of φ over h_1 and h_2, i.e., $g_1 \in \varphi^{-1}(h_1)$ and $g_2 \in \varphi^{-1}(h_2)$ always exist since φ is surjective. $\square$

(4) Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

Solution. $|i| = 4$ in $\mathbb{C} - \{0\}$, but there are no elements of order 4 in $\mathbb{R} - \{0\}$. □

(5) Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Solution. $|\mathbb{R}| \neq |\mathbb{Q}|$. □

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

Solution. Every nonidentity element in $\mathbb{Z}$ has infinite order, but elements of the form $1/r \in \mathbb{Q}$ where $r \in \mathbb{Z}$ has order r. □

(7) Prove that D_8 and Q_8 are not isomorphic.

Solution. D_8 has only 1 element of order 4, while Q_8 has 3 elements of order 4. □

(8) Prove that if $n \neq m$, then S_n and S_m are not isomorphic.

Solution. If $n \neq m$, then $n! \neq m!$ so that $|S_n| \neq |S_m|$. □

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

Solution. D_{24} has elements of order 12 (e.g. r) but S_4 has no elements of order 12, since every element of S_4 is either a 2-cycle, 3-cycle, 4-cycle, or a combination of 2-cycles. □

(10) Fill in the details of the proof that the symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$ as follows: let $\theta : \Delta \to \Omega$ be a bijection. Define

$$\varphi : S_\Delta \to S_\Omega \quad \text{by} \quad \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \quad \text{for all } \sigma \in S_\Delta$$

and prove the following:

  (a) Prove that φ is well-defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω.
  (b) Prove that φ is a bijection from S_Δ onto S_Ω by finding a two-sided inverse for φ.
  (c) Prove that φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

Note the similarity to the change of basis or similarity transformations for matrices (we shall see the connections between these later in the text).

Solution.

  (a) Clearly $\theta \circ \sigma \circ \theta^{-1}$ is a function from Ω to Ω. To show that it is a bijection, take some $a, b \in \Omega$ such that $\varphi(\sigma)(a) = \varphi(\sigma)(b)$, or $(\theta \circ \sigma \circ \theta^{-1})(a) = (\theta \circ \sigma \circ \theta^{-1})(b)$. Since θ is a bijection, then θ^{-1} is a bijection. Moreover, $\theta \in S_\Delta$ implies that it is a permutation of Δ so it too is a bijection. It then follows that $a = b$, or that $\varphi(\sigma)$ is an injection.

  Now suppose $b \in \Omega$. Put $a = (\theta \circ \sigma^{-1} \circ \theta^{-1})(b)$. Then $\varphi(\sigma)(a) = b$ so that $\varphi(\sigma)$ is a surjection. Hence, it is a bijection and is a permutation of Ω.

  (b) Define $\psi : S_\Omega \to S_\Delta$ as
$$\psi(\pi) = \theta^{-1} \circ \pi \circ \theta \quad \text{for } \pi \in S_\Omega$$

  Using similar reasoning in part (a), it is easy to see that ψ is a well-defined mapping. Moreover, for any $\sigma \in S_\Delta$, we have
$$(\psi \circ \varphi)(\sigma) = \psi(\theta \circ \sigma \circ \theta^{-1}) = \theta^{-1} \circ (\theta \circ \sigma \circ \theta^{-1}) \circ \theta = \sigma$$

  and for any $\pi \in S_\Omega$, we have
$$(\varphi \circ \psi)(\pi) = \varphi(\theta^{-1} \circ \pi \circ \theta) = \theta \circ (\theta^{-1} \circ \pi \circ \theta) \circ \theta^{-1} = \pi$$

  Then ψ is a two-sided inverse of φ, hence $\psi = \varphi^{-1}$, and φ is indeed a bijection.

  (c) Pick $\sigma, \tau \in S_\Delta$. Then
$$\varphi(\sigma) \circ \varphi(\tau) = \theta \circ \sigma \circ \theta^{-1} \circ \theta \circ \tau \circ \theta^{-1} = \theta \circ \sigma \circ \tau \circ \theta^{-1} = \varphi(\sigma \circ \tau) \qquad □$$

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

Solution. Let $\varphi : A \times B \to B \times A$ be defined as $\varphi(a, b) = (b, a)$ for some $(a, b) \in A \times B$. Clearly, it is a homomorphism, since for $(a, b), (c, d) \in A \times B$, we have $\varphi((a, b)(c, d)) = \varphi(ac, bd) = (bd, ac) = (b, a)(d, c) = \varphi(a, b)\varphi(c, d)$. Moreover, for any $(b, a) \in B \times A$, then $\varphi(a, b) = (b, a)$ so that φ is surjective. Finally, suppose $\varphi(a, b) = \varphi(c, d)$ for $(a, b), (c, d) \in A \times B$. Then $(b, a) = (d, c)$, and comparing components results in $b = d$ and $a = c$, or $(a, b) = (c, d)$. Hence, φ is injective so that it is an isomorphism, and $A \times B \cong B \times A$. $\square$

(12) Let A, B, and C be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C \cong A \times H$.

Solution. Let $\varphi : G \times C \to A \times H$ be defined as $\varphi((a, b), c) = (a, (b, c))$. This is easily checked to be an isomorphism. $\square$

(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 (cf. Exercise 26 of Section 1). Prove that if φ is injective then $G \cong \varphi(G)$.

Solution. Pick $\varphi(a), \varphi(b) \in \varphi(G)$. Note that $ab \in G$, since G is a group. Then $\varphi(a)\varphi(b) = \varphi(ab) \in \varphi(G)$ so that $\varphi(G)$ is closed under the operation of H. Moreover, $\varphi(a)^{-1} \in \varphi(G)$ since $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(G)$ because $a^{-1} \in G$. Then $\varphi(G)$ is a subgroup of H.

Suppose now that φ is injective, and define $\psi : G \to \varphi(G)$ as $\psi(g) = \varphi(g)$. Let $g, h \in G$. Then $\psi(gh) = \varphi(gh) = \varphi(g)\varphi(h) = \psi(g)\psi(h)$ so that ψ is a homomorphism. Moreover, if g, h are such that $\psi(g) = \psi(h)$, then $\varphi(g) = \varphi(h)$. Since φ is injective, then $g = h$ so that ψ is also injective. Moreover, for any $\varphi(g) \in \varphi(G)$, then $\psi(g) = \varphi(g)$ so that ψ is surjective. Hence, $G \cong \varphi(G)$. $\square$

(14) Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Define the *kernel* of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$ (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.

Solution. For the remainder of this text, let $\ker(\varphi)$ denote the kernel of φ. Note that if $x, y \in \ker(\varphi)$, then $\varphi(xy) = \varphi(x)\varphi(y) = 1_H 1_H = 1_H$ so that $xy \in \ker(\varphi)$. Moreover, for some $x \in \ker(\varphi)$, then $\varphi(x^{-1}) = \varphi(x)^{-1} = 1_H^{-1} = 1_h$ so that $x^{-1} \in \ker(\varphi)$. Then $\ker(\varphi)$ is a subgroup of G.

Now suppose φ is injective, and pick $x \in \ker(\varphi)$. Then $\varphi(x) = 1_H$. However, $\varphi(1_G) = 1_H$ so that $\varphi(x) = \varphi(1_G)$. Then $x = 1_G$. If $\ker(\varphi)$ was instead trivial, suppose $\varphi(x) = \varphi(y)$ for some $x, y \in G$. In particular, then $\varphi(x)\varphi(y)^{-1} = 1_H$. Then $\varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1}) = 1_H$. Since identities map to each other, then $xy^{-1} = 1_G$, or $x = y$. Then φ is injective. $\square$

(15) Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π.

Solution. Let $(a, b), (c, d) \in \mathbb{R}^2$. Then

$$\pi((a, b) + (c, d)) = \pi(a + c, b + d) = a + c = \pi(a, b) = \pi(c, d)$$

so that π is a homomorphism. Moreover, if $\pi(a, b) = 0$, then $a = 0$ while b varies so that

$$\ker(\pi) = \{(0, b) \mid b \in \mathbb{R}\}$$ $\square$

(16) Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels.

Solution. For $(a, b), (c, d) \in G$, then

$$\pi_1((a, b)(c, d)) = \pi_1(ac, bd) = ac = \pi_1(a, b)\pi_1(c, d)$$

and

$$\pi_2((a, b)(c, d)) = \pi_2(ac, bd) = bd = \pi_2(a, b)\pi_2(c, d)$$

Moreover, the kernels are

$$\ker(\pi_1) = \{(1, b) \mid b \in B\}$$
$$\ker(\pi_2) = \{(a, 1) \mid a \in A\}$$ $\square$

(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.

Solution. Let φ be the aforementioned mapping, and suppose φ is a homomorphism. Then for any $g, h \in G$, we have
$$(gh)^{-1} = \varphi(gh) = \varphi(g)\varphi(h) = g^{-1}h^{-1} = (hg)^{-1}$$
Since inverses are unique, then $gh = hg$, and G is abelian. If instead G was abelian, then
$$\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \varphi(g)\varphi(h)$$
so that φ is a homomorphism. $\square$

(18) Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Solution. Let φ be the mapping, and suppose it it is a homomorphism. Then for $g, h \in G$, we have
$$(gh)^2 = \varphi(gh) = \varphi(g)\varphi(h) = g^2 h^2$$
Then $ghgh = gghh$. Left canceling the g and right canceling the h, we obtain $hg = gh$ so that G is abelian. If G is abelian, then
$$\varphi(gh) = (gh)^2 = g^2 h^2 = \varphi(g)\varphi(h)$$
so that φ is a homomorphism. $\square$

(19) Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

Solution. Recall the polar form of a complex number $z = r(\cos\theta + i\sin\theta) = re^{i\theta}$ for modulus r and argument θ. For every $z \in G$, then $r = 1$, so elements of G taken on the form $e^{i\theta}$. Moreover, because $z^n = 1$, then $e^{in\theta} = 1$. Lastly, the polar representation of 1 is given by $e^{i2\pi m}$ for some $m \in \mathbb{Z}$. Equating the two exponents, or $in\theta = i2\pi m$, then $\theta = 2\pi m/n$, which means we can reformulate G as the following:
$$G = \{e^{i2\pi m/n} \in \mathbb{C} \mid m \in \mathbb{Z}, n \in \mathbb{Z}^+\}$$
To show that φ is a homomorphism, we may fall back to the original formulation of G: for any $z, w \in G$, then
$$\varphi(zw) = (zw)^k = z^k w^k = \varphi(z)\varphi(w)$$
Now suppose $w \in G$. Then $w = e^{i2\pi m/n}$. Since $z = e^{i2\pi m/nk} \in G$ because $nk \in \mathbb{Z}^+$, then $z^k = (e^{i2\pi m/nk})^k = e^{i2\pi m/n} = w$ so that $\varphi(z) = w$, and φ is surjective. Moreover, it is not an isomorphism because $\ker(\varphi)$ consists of the elements $z \in G$ such that $z^k = (e^{i2\pi m/n})^k = 1$. It follows that such z have a polar representation of $n = k$, or more explicitly:
$$\ker(\varphi) = \{e^{i2\pi m/k} \mid m = 0, 1, \ldots, k-1\}$$
where m is cut off after $m = k-1$ since any two elements of $\ker(\varphi)$ are equivalent when they dif and only ifer by a factor of 2π. $\square$

(20) Let G be a group and let $\text{Aut}(G)$ be the set of all isomorphisms from G onto G. Prove that $\text{Aut}(G)$ is a group under function composition (called the *automorphism group* of G and the elements of $\text{Aut}(G)$ are called *automorphisms* of G).

Solution. Function composition is associative in general so that it is associative in $\text{Aut}(G)$. Since a composition of bijections is also a bijection, it suffices to check that a composition of homomorphisms is a homomorphisms. In particular, let $\varphi, \psi \in \text{Aut}(G)$. Then for any $g, h \in G$, we have
$$(\varphi \circ \psi)(gh) = \varphi(\psi(gh)) = \varphi(\psi(g)\psi(h)) = \varphi(\psi(g))\varphi(\psi(h)) = (\varphi \circ \psi)(g)(\varphi \circ \psi)(h)$$
so that a composition of isomorphisms is also an isomorphism, and $\text{Aut}(G)$ is closed under function composition. The identity map $1 : G \to G$ is trivially in $\text{Aut}(G)$ so that it has identity. Lastly, for any $\varphi \in \text{Aut}(G)$, consider the bijective inverse φ^{-1}. Then for any $g, h \in G$, there are elements $a, b \in G$ such that $\varphi(a) = g$ and $\varphi(b) = h$. Then
$$\varphi^{-1}(gh) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(g)\varphi^{-1}(h)$$
so that $\text{Aut}(G)$ is closed under inverses. Then $\text{Aut}(G)$ is a group under function composition. $\square$

(21) Prove that for each fixed nonzero $k \in \mathbb{Q}$ the map from $\mathbb{Q}$ to itself defined by $q \mapsto kq$ is an automorphism of $\mathbb{Q}$.

Solution. Suppose $\varphi(q) = \varphi(r)$ for $q, r \in \mathbb{Q}$. Then $kq = kr$, or $q = r$ so that φ is injective. Similarly, for any $q \in \mathbb{Q}$, then $\varphi(q/k) = k(q/k) = q$ so that φ is surjective. Lastly,

$$\varphi(q + r) = k(q + r) = kq + kr = \varphi(q) = \varphi(r)$$

and φ is a homomorphism. Then it is an automorphism of $\mathbb{Q}$. □

(22) Let A be an abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$ prove that this homomorphism is an isomorphism (i.e., is an automorphism of A).

Solution. Suppose $a, b \in A$. Then

$$\varphi(ab) = (ab)^k = a^k b^k = \varphi(a)\varphi(b)$$

so that it is a homomorphism of A. Moreover, if $k = -1$, refer to Exercise 17. □

(23) Let G be a finite group which possesses an automorphism σ 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.]

Solution. To show that every $g \in G$ is of the form $x^{-1}\sigma(x)$ for some $x \in G$, the natural choice is to show that $\varphi : G \to G$ defined by $\varphi(g) = g^{-1}\sigma(g)$ is a bijective function. To that end, suppose $g, h \in G$ such that $\varphi(g) = \varphi(h)$. Then $g^{-1}\sigma(g) = h^{-1}\sigma(h)$. Since $\sigma^2 = 1$, then $\sigma^{-1} = \sigma$, so that:

$$\begin{aligned}
\varphi(g) = \varphi(h) &\implies g^{-1}\sigma(g) = h^{-1}\sigma(h) \\
&\implies \sigma(g) = gh^{-1}\sigma(h) \\
&\implies g = \sigma(gh^{-1}\sigma(h)) \\
&\implies g = \sigma(gh^{-1})h \\
&\implies gh^{-1} = \sigma(gh^{-1})
\end{aligned}$$

Then $gh^{-1} = 1$ because σ is fixed point free of order 2. It follows that $g = h$ so that φ is injective. Since G is finite, then φ is necessarily surjective so that φ is a bijection. From this, we conclude that each $g \in G$ can be associated with some $h^{-1}\sigma(h)$ for $h \in G$.

Now suppose $g \in G$. Then for some $x \in G$, we have $\sigma(g) = \sigma(x^{-1}\sigma(x)) = \sigma(x)^{-1}x = (x^{-1}\sigma(x))^{-1} = g^{-1}$. Then for any $h \in G$, we have

$$\sigma(gh) = (gh)^{-1} = h^{-1}g^{-1} = \sigma(h)\sigma(g) = \sigma(hg)$$

Since $\sigma \in \text{Aut}(G)$, then $gh = hg$. □

(24) Let G be a finite group and let x and y be distinct elements of order 2 in G that generate G. Prove that $G \cong D_{2n}$, where $n = |xy|$.

Solution. Put $t = xy$. Then $tx = xt^{-1}$, since $x = x^{-1}$ and $y = y^{-1}$. Moreover, $y = x^{-1}t = xt$ so that x and t generate G. Using the relation $tx = xt^{-1}$, then the elements of G may be written in the form $x^i t^j$ for $i \in \{0, 1\}$ and $0 \leq j < n - 1$. Since $|t| = n$, then $x^i t^j$ is unique for any choice of i so that $\langle t \rangle$ has unique elements. It follows that $G = \{1, t, \ldots, t^{n-1}, x, xt, \ldots, xt^{n-1}\}$, and $|G| = 2n$.

Let $\varphi : D_{2n} \to G$ be given by

$$\varphi(s^i r^j) = x^i t^j, \quad \text{for } i, j \in \mathbb{Z} \text{ such that } i = \{0, 1\} \text{ and } 0 \leq j < n - 1$$

It is known that every form of D_{2n} is unique by the representation above so that φ will be well-defined. Moreover, the elements $x, t \in G$ satisfy the relations of D_{2n}, i.e., $(xt)^n = x^2 = 1$, and $tx = xt^{-1}$. Then φ is a homomorphism. Lastly, suppose $x^i t^j \in G$. Then $\varphi(s^i r^j) = x^i t^j$ so that φ is surjective. Since G is finite, then φ is injective, and $G \cong D_{2n}$. □

(25) Let $n \in \mathbb{Z}^+$, let r and s be the usual generators of D_{2n} and let $\theta = 2\pi/n$.

(a) Prove that the matrix
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$
is the matrix of the linear transformation which rotates the x, y-plane about the origin in a counter-clockwise direction by θ radians.

(b) Prove that the map $\varphi : D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ defined on generators by
$$\varphi(r) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{and} \quad \varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
extends to a homomorphism of D_{2n} into $\mathrm{GL}_2(\mathbb{R})$.

(c) Prove that the homomorphism φ defined above is injective.

Solution.

(a) Take any $\vec{v} = (x \quad y)^T \in \mathbb{R}^2$. Then
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix} = \vec{u}$$

Note that $|\vec{v}| = \sqrt{x^2 + y^2}$. The distance of this vector is
$$\begin{aligned}
|\vec{u}| &= \sqrt{(x\cos\theta - y\sin\theta)^2 + (x\sin\theta + y\cos\theta)^2} \\
&= \sqrt{(x^2\cos^2\theta - 2xy\cos\theta\sin\theta + y^2\sin^2\theta + x^2\sin^2\theta + 2xy\cos\theta\sin\theta + y^2\cos^2\theta} \\
&= \sqrt{x^2(\cos^2\theta + \sin^2\theta) + y^2(\cos^2\theta + \sin^2\theta)} \\
&= \sqrt{x^2 + y^2}
\end{aligned}$$

so that $|\vec{u}| = |\vec{v}|$. Moreover, the angle θ' between $\vec{v}$ and $\vec{u}$ is
$$\begin{aligned}
\cos(\theta') &= \frac{\vec{v} \cdot \vec{u}}{|\vec{v}||\vec{u}|} \\
&= \frac{x(x\cos\theta - y\sin\theta) + y(x\sin\theta + y\cos\theta)}{x^2 + y^2} \\
&= \frac{x^2\cos\theta - xy\sin\theta + xy\sin\theta + y^2\cos\theta}{x^2 + y^2} \\
&= \cos\theta
\end{aligned}$$

so that $\theta' = \theta$. Then $\vec{u}$ is $\vec{v}$ rotated $\theta = 2\pi/n$ radians.

(b) We first show that
$$\varphi(r)^k = \begin{pmatrix} \cos(k\theta) & -\sin(k\theta) \\ \sin(k\theta) & \cos(k\theta) \end{pmatrix}$$

The case for $k = 1$ is clear. Supposing it holds true for some k, then for $k + 1$, we have
$$\begin{aligned}
\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{k+1} &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^k \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \\
&= \begin{pmatrix} \cos(k\theta) & -\sin(k\theta) \\ \sin(k\theta) & \cos(k\theta) \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \\
&= \begin{pmatrix} \cos(k\theta)\cos\theta - \sin(k\theta)\sin\theta & -\cos(k\theta)\sin\theta - \sin(k\theta)\cos\theta \\ \sin(k\theta)\cos\theta + \cos(k\theta)\sin\theta & -\sin(k\theta)\sin\theta + \cos(k\theta)\cos\theta \end{pmatrix} \\
&= \begin{pmatrix} \cos((k+1)\theta) & -\sin((k+1)\theta) \\ \sin((k+1)\theta) & \cos((k+1)\theta) \end{pmatrix}
\end{aligned}$$

so the result follows by induction. From this, it is clear that $\varphi(r)^n = I$, since $\cos(2\pi) = 1$ and $\sin(2\pi) = 0$. Additionally, for $k = -1$, note that $\det(\varphi(r)) = 1$. Then

$$\varphi(r)^{-1} = \begin{pmatrix} \cos\theta & -(-\sin\theta) \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

Moreover, $\varphi(s)^2 = I$. Lastly,

$$\varphi(s)\varphi(r) = \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix} = \varphi(r)^{-1}\varphi(s)$$

Since $\varphi(r)^n = \varphi(s)^2 = I$, and $\varphi(s)\varphi(r) = \varphi(r)^{-1}\varphi(s)$, i.e., the relations in D_{2n} hold in $\mathrm{GL}_2(\mathbb{R})$, then φ is a homomorphism.

(c) Suppose $\varphi(g) = I$. Then g can take on two forms:
- If $g = r^k$, then $\varphi(r)^k \neq I$ for any $k = 0, 1, \ldots, n-1$, since $\theta = 2\pi k/n$.
- If $g = sr^k$, then $\varphi(s)\varphi(r)^k = I$, or $\varphi(s) = \varphi(r)^{-k}$. Note that $\det(\varphi(s)) = -1$, while $\det(\varphi(r)^k) = 1$. Since $\det(\varphi(s)) \neq \det(\varphi(r)^{-k})$, then $\varphi(s) \neq \varphi(r)^{-k}$ (this follows from $A = B \implies \det(A) = \det(B)$ for any $A, B \in \mathrm{GL}_n(\mathbb{R})$).

This shows that $\ker(\varphi) = 1$, so that φ is injective. $\qquad\square$

(26) Let i and j be the generators of Q_8 described in Section 5. Prove that the map φ from Q_8 to $\mathrm{GL}_2(\mathbb{C})$ defined on generators by

$$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \quad \text{and} \quad \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

extends to a homomorphism. Prove that φ is injective.

Solution. It is easy to see that

$$\varphi(i)^2 = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

and

$$\varphi(j)^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

Also note that

$$\varphi(i)\varphi(j) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix}$$

So we may set $\varphi(i)\varphi(j) = \varphi(k)$. We can calculate that $\varphi(k)^2 = -I$. It then follows that

$$\varphi(i)^2 = \varphi(j)^2 = \varphi(k)^2 = \varphi(i)\varphi(j)\varphi(k) = \varphi(-1)$$

Clearly these elements satisfy the same relations we found in Q_8 so that φ extends to a homomorphism from Q_8 to $\mathrm{GL}_2(\mathbb{C})$. Moreover, it follows that $\varphi(x) = I$ only when $x = 1 \in Q_8$ as any nonidentity element in Q_8 does not map to I. Hence, $\ker(\varphi)$ is trivial and is then injective. $\qquad\square$

1.7   Group Actions

(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 $g \cdot a = ga$, 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).

Solution. Suppose $g, h \in F^\times$. Then for any $a \in A$, we have

$$g \cdot (h \cdot a) = g \cdot (ha) = \underbrace{g(ha) = (gh)a}_{\text{Associativity}} = (gh) \cdot a$$

Moreover, $1 \cdot a = 1a = a$ by definition of $1 \in F^\times$. Lastly, note that $1(0) = 1(0 + 0) = 1(0) + 1(0)$. By cancellation, then $0 = 1(0) = 1 \cdot 0$ so that all $a \in F$ is accounted for. $\qquad\square$

(2) Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.

   Solution. Let $z, w \in \mathbb{Z}$. Then

$$z \cdot (w \cdot a) = z \cdot (w + a) = z + (w + a) = (z + w) + a = (z + w) \cdot a$$

   Moreover, $0 \cdot a = 0 + a = a$ so that $\cdot$ is a group action. □

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

   Solution. Suppose $r, s \in \mathbb{R}$. Then for any $(x, y) \in \mathbb{R} \times \mathbb{R}$, we have

$$r \cdot (s \cdot (x, y)) = r \cdot (x + s, y) = ((x + s) + r, y) = (x + (r + s), y) = (r + s) \cdot (x, y)$$

   Moreover, $0 \cdot (x, y) = (x + 0, y) = (x, y)$ so that $\cdot$ is a group action. □

(4) Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G (cf. Exercise 26 of Section 1):

  (a) the kernel of the action,

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

   Solution.

  (a) Recall that $\ker(\cdot) = \{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$. Suppose $g, h \in \ker(\cdot)$. Then for any $a \in A$, we have

$$(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a$$

   so that $gh \in \ker(\cdot)$. Moreover,

$$a = 1 \cdot a = (g^{-1}g) \cdot a = g^{-1}(g \cdot a) = g^{-1} \cdot a$$

   so that $g^{-1} \in \ker(\cdot)$. Then $\ker(\cdot)$ is closed under the operation of G and inverses so that it is a subgroup of G.

  (b) Let $a \in A$ be fixed, and let H be as described. Note that $1 \in H$ so that it is nonempty. Suppose $g, h \in H$. Then

$$(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a$$

   so that $gh \in H$. Moreover,

$$a = 1 \cdot a = (g^{-1}g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot a$$

   so that $g^{-1} \in H$. Then H is closed under the operation of G and inverses, hence it is a subgroup of G. □

(5) Prove that the kernel of an action of the group G on the set A is the same as the kernel of the corresponding permutation representation $G \to S_A$ (cf. Exercise 14 in Section 6).

   Solution. Let $\ker(\cdot)$ be the kernel of the action and $\varphi : G \to S_A$ be the permutation representation so that $\varphi(g)(a) = g \cdot a$. Let $g \in \ker(\cdot)$. Then $\varphi(g)(a) = g \cdot a = a$ so that $g \in \ker(\varphi)$. If $g \in \ker(\varphi)$, then $\varphi(g) = 1 \in S_A$, or the identity permutation. It follows that $\varphi(g)(a) = 1(a) = g \cdot a$ so that $g \in \ker(\cdot)$. It follows that $\ker(\cdot) = \ker(\varphi)$. □

(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.

   Solution. Suppose G acts faithfully on a set A, and pick $g \in \ker(\cdot)$. Then $g \cdot a = a$ for every $a \in A$. But $1 \cdot a = a$ as well. Since the action is faithful, it must be that $g = 1$ so that $\ker(\cdot) = \{1\}$.
   Suppose now that $\ker(\cdot) = \{1\}$, and pick some $g, h \in G$ such that $g \cdot a = h \cdot a$ for any $a \in A$. Then

$$a = (g^{-1}g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot (h \cdot a) = (g^{-1}h) \cdot a$$

   so that $g^{-1}h \in \ker(\cdot)$. Then $g^{-1}h = 1$, or $g = h$. Hence, G acts on A faithfully. □

(7) Prove that in Example 2 in this section the action is faithful.

Solution. Let V be a vector space with a field F. For any $v \in V$ and $r \in F^\times$, let the group action be defined as $r \cdot v = rv$. Now suppose $r \cdot v = s \cdot v$ for some $r, s \in F^\times$. Then

$$
\begin{aligned}
\mathbf{0} = 0 \cdot v &= a \cdot v + (-a) \cdot v \\
&= b \cdot v + (-a) \cdot v \\
&= (b + (-a)) \cdot v \\
&= (b - a) v
\end{aligned}
$$

Since $(b - a)v = \mathbf{0}$ even for $v \neq \mathbf{0}$, it must be that $b - a = 0$, or $b = a$. Then the action is faithful.   □

(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

$$
\sigma(\{a_1, \ldots, a_k\}) = \{\sigma(a_1), \ldots, \sigma(a_k)\}.
$$

(a) Prove that this is a group action.

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

Solution.

(a) Let $\sigma, \tau \in S_A$. Then for any cardinality k subset $\{x_1, \ldots, x_k\}$ of A, we have

$$
\begin{aligned}
\sigma \cdot (\tau \cdot \{x_1, \ldots, x_k\}) &= \sigma \cdot \{\tau(x_1), \ldots, \tau(x_k)\} \\
&= \{\sigma(\tau(x_1)), \ldots, \sigma(\tau(x_k))\} \\
&= (\sigma \circ \tau) \cdot \{x_1, \ldots, x_k\}
\end{aligned}
$$

Moreover, $1 \cdot \{x_1, \ldots, x_k\} = \{1(x_1), \ldots, 1(x_k)\} = \{x_1, \ldots, x_k\}$. Then it is a group action.

(b)

A	$(1\ 2) \cdot A$	$(1\ 2\ 3) \cdot A$
$\{1, 2\}$	$\{2, 1\}$	$\{2, 3\}$
$\{1, 3\}$	$\{2, 3\}$	$\{2, 1\}$
$\{1, 4\}$	$\{2, 4\}$	$\{2, 4\}$
$\{2, 3\}$	$\{1, 3\}$	$\{3, 1\}$
$\{2, 4\}$	$\{1, 4\}$	$\{3, 4\}$
$\{3, 4\}$	$\{3, 4\}$	$\{1, 4\}$

□

(9) Do both parts of the preceding exercise with "ordered k-tuples" in place of "k-element subsets," where the action on k-tuples is defined as above but with set braces replaced by parentheses (note that, for example, the 2-tuples $(1, 2)$ and $(2, 1)$ are dif and only iferent even though the sets $\{1, 2\}$ and $\{2, 1\}$ are the same, so the sets being acted upon are dif and only iferent).

Solution. The work is similar as above, except there are 12 2-tuples as $(1, 2) \neq (2, 1)$.   □

(10) With reference to the preceding two exercises determine:

(a) for which values of k the action of S_n on k-element subsets is faithful, and

(b) for which values of k the action of S_n on ordered k-tuples is faithful.

Solution.

(a) for $k = |A|$, the action is not faithful: if there exist a subset $S \subseteq A$ such that $|S| = |A|$, then $S = A$. Then if we have any distinct permutations $\sigma, \tau \in S_A$, then $\sigma \cdot S = S = \tau \cdot S$.

To that end, suppose we have a subset S of cardinality k where $1 \leq k < |A|$, and let $\sigma, \tau \in S_A$ such that $\sigma \neq \tau$. Let $A = \{a_1, \ldots, a_n\}$ such that $\sigma(a_i) \neq \tau(a_i)$ for any such a_i. Let $S \subset A$ have cardinality k such that $(\sigma^{-1} \circ \tau)(a_i) \notin S$ and $a_i \in S$, where such an element exist since S is a proper subset of A. Then $\sigma(a_i) \notin \sigma \cdot S$, but $\tau(a_i) \in S$ so that distinct permutations are induced on S. Then the action of S_A on A is faithful for all k where $1 \leq k < |A|$.

(b) Let $1 \le k \le |A|$ and consider the k-tuple $(a_1, \ldots, a_k)$. Let $\sigma, \tau \in S_A$ such that $\sigma \ne \tau$. Then there is some $a_i \in A$ where $\sigma(a_i) \ne \tau(a_i)$. Then $\sigma \cdot (a_1, \ldots, a_k) \ne \tau \cdot (a_1, \ldots, a_k)$ so that they induce dif and only iferent permutations on the k-tuples. Hence, the action is faithful. $\qquad\square$

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

Solution. Let $\varphi : D_8 \to S_4$ be the permutation representation of the action of D_8 on the vertices of a square $\{1, 2, 3, 4\}$. Then

$$
\begin{aligned}
\varphi(1) &= 1 \\
\varphi(r) &= (1\ 2\ 3\ 4) \\
\varphi(r^2) &= (1\ 3)(2\ 4) \\
\varphi(r^3) &= (1\ 4\ 3\ 2) \\
\varphi(s) &= (2\ 4) \\
\varphi(sr) &= (1\ 4)(2\ 3) \\
\varphi(sr^2) &= (1\ 3) \\
\varphi(sr^3) &= (1\ 2)(3\ 4)
\end{aligned}
$$
$\qquad\square$

(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).

Solution. Let P_k denote the pair of opposite vertices. In particular, define it as the set

$$P_k := \{k, k + n/2\}$$

Moreover, let $P = \{P_1, P_2, \ldots, P_{n/2}\}$. Define a mapping $D_{2n} \times P \to P$ as $r \cdot P_k = r(P_k) = P_m$, where P_m consists of the vertices that r maps the vertices in P_k to.

By definition, for any $x, y \in D_{2n}$, then $x \cdot (y \cdot P_k) = x \cdot (y(P_k)) = x(y(P_k)) = (xy)(P_k)$. Moreover, $1(P_k) = P_k$ since 1 fixes all vertices in the n-gon so that the mapping is a group action. Since no action in D_{2n} fixes some vertices and sends others to other vertices except 1 and $r^{n/2}$, the only candidates for the kernel of this group action is the identity and the $180°$ rotation, or $r^{n/2}$. Note that for $n = 2$, then s and sr^2 are also in the kernel. $\qquad\square$

(13) Find the kernel of the left regular action.

Solution. See item 3 in Definition 1.22 for the solution. $\qquad\square$

(14) Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by

$$g \cdot a = ag \quad \text{for all } g, a \in G$$

do not satisfy the axioms of a (left) group action of G on itself.

Solution. Since G is non-abelian, there exists $g, h \in G$ such that $gh \ne hg$. Assuming that the above is a group action, then it must be that

$$g \cdot (h \cdot a) = g \cdot (ah) = (ah)g = a(hg) = a(gh) = (gh) \cdot a$$

for any $a \in A$. Left cancelling results in $hg = gh$, contradicting that G is non-abelian. $\qquad\square$

(15) Let G be any group and let $A = G$. Show that the maps defined by

$$g \cdot a = ag^{-1} \quad \text{for all } g, a \in G$$

do satisfy the axioms of a (left) group action of G on itself.

Solution. Let $g, h \in G$. Then for any $a \in A$, we have

$$g \cdot (h \cdot a) = g \cdot (ah^{-1}) = a(h^{-1}g^{-1}) = a(gh)^{-1} = (gh) \cdot a$$

Moreover, $1 \cdot a = a1^{-1} = a1 = a$. Then the above is a left group action. $\qquad\square$

(16) Let G be any group and let $A = G$. Show that the maps defined by

$$g \cdot a = gag^{-1} \quad \text{for all } g, a \in G$$

do satisfy the axioms of a (left) group action (this action of G on itself is called *conjugation*).

Solution. Let $g, h \in G$. For any $a \in A$, then

$$g \cdot (h \cdot a) = g \cdot (hah^{-1}) = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = (gh) \cdot a$$

Moreover, $1 \cdot a = 1a1^{-1} = a$. Then it is a group action. □

(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. an automorphism of G). Deduce that x and gxg^{-1} have the same order for all $x \in G$ and that for any subset A of G, $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1} \mid a \in A\}$).

Solution. Let g be fixed and define the map

$$\varphi : G \to G \text{ where } x \mapsto gxg^{-1}$$

Then for $x, y \in G$, we have

$$\varphi(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi(x)\varphi(y)$$

so that φ is a homomorphism. Now suppose $\varphi(x) = \varphi(y)$. Then $gxg^{-1} = gyg^{-1}$. Cancellation shows that $x = y$ so that φ is injective. Finally, suppose $y \in G$ such that $\varphi(x) = y$. Then $gxg^{-1} = y$, or $x = g^{-1}yg \in G$. Then φ is surjective. It follows that φ is an automorphism of G and that $|x| = |gxg^{-1}|$ since isomorphisms preserve order. Moreover, for $A \subseteq G$, then $\varphi|_A : A \to gAg^{-1}$ is still a bijection so that $|A| = |gAg^{-1}|$. □

(18) Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by

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

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

Solution. Since $a = 1a$, then $a \sim a$. If $a \sim b$, then there exists some $h \in H$ where $a = hb$. Then $h^{-1}a = b$ so that $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, there exists $h, h' \in H$ where $a = hb$ and $b = h'c$. Then $a = (hh')c$ so that $a \sim c$. Then $\sim$ is an equivalence relation. □

(19) Let H be a subgroup of the 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 this action of H. Prove that the map

$$H \to \mathcal{O}, \qquad h \mapsto hx$$

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 $|G|$*

Solution. Let $\varphi : H \to \mathcal{O}$ be the mapping $h \mapsto hx$ for fixed $x \in G$. Suppose $\varphi(h) = \varphi(k)$ for $h, k \in H$. Then $hx = kx$, implying $h = k$. Surjectivity is a given, so φ is a bijection. Then $|H| = |\mathcal{O}|$. The previous exercise shows that G is partitioned into the orbits under the action of H so that $|G| = n|H|$, where n represents the number of orbits. This is exactly Lagrange's Theorem. □

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

Solution. Let G be the rigid motions of a tetrahedron, and let $A = \{1, 2, 3, 4\}$ be the set that G acts on. In particular, each $\alpha \in G$ is associated with a permutation σ_α of A such that $\alpha i = \sigma_\alpha(i)$.

Consider the injective map

$$\varphi : G \to S_4 \text{ where } \varphi(\alpha) = \sigma_\alpha$$

It is clear that $\varphi(G)$ is a subgroup of S_4, and we may restrict S_4 to consider the elements from $\varphi(G)$ only to obtain an isomorphism. $\square$

(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.)

Solution. As per Section 2, Exercise 10, recall that $|G| = 24 = |S_4|$. Now let G be a group of rigid motions of a cube with $A = \{a_1, a_2, a_3, a_4\}$, where each a_i consists of a pair of opposing vertices of a cube. Clearly, each $\alpha \in G$ sends some a_i to another a_j so that G acts on A.

Consider now the homomorphism $\varphi : G \to S_4$ where $\varphi(\alpha)(a_i) = \alpha a_i$. Because each rigid motion is distinct, then this is injective. Then $G \cong S_4$. $\square$

(22) Show that the group of rigid motions of an octahedron is isomorphic to a subgroup of S_4. (This group acts on the set of four pairs of opposite faces.) Deduce that the groups of rigid motions of a cube and of an octahedron are isomorphic. (These two groups are isomorphic because these solids are "dual.")

Solution. Let G be the group of rigid motions of an octahedron with $A = \{f_1, f_2, f_3, f_4\}$, where each f_i corresponds to opposing faces of an octahedron. Then $\alpha \in G$ sends some pair of faces to another pair of faces so that G acts on A.

As in the last exercise, consider the injective homomorphism $\varphi : G \to S_4$, where $\varphi(\alpha)(f_i) = \alpha f_i$. Since $|G| = 24$ from Section 2, Exercise 11, it follows that $G \cong S_4$. Hence, G is isomorphic to the group of rigid motions of a cube. $\square$

(23) Explain why the action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful. Find the kernel of this action.

Solution. The group of rigid motions of a cube has 24 elements, while permutations of the set of three pairs of opposing faces has 6 elements, so the action cannot be faithful as no homomorphism can be injective between finite groups of dif and only ifering sizes (if there was some injective homomorphism, it would imply bijectivity between the two groups of dif and only ifering cardinality, which is impossible).

Consider a cube such that its center is at the origin of $\mathbb{R}^3$ space. Then any rotation around the axes fixes a pair of faces, while sends the other two pairs back to themselves (to visualize this explicitly, consider the cube with vertices $(\pm 1, \pm 1, \pm 1)$ and the z-axis. A rotation around the z-axis would fix the faces $(\pm 1, \pm 1, 1)$ and $(\pm 1, \pm 1, -1)$, while it rotates the pair of faces $(1, \pm 1, \pm 1)$ and $(-1 \pm 1, \pm 1)$ back to each other–these are the faces that vary along the x-axis. One can construct the same for the pair of faces that lie along the y-axis and deduce the same thing). There are exactly 3 of these $180°$ rotations, so the kernel of this action consists of these rotations and the identity. $\square$

2   Subgroups

2.1   Definitions and Examples

(1) In each of (a)–(e) prove that the specified subset is a subgroup of the given group:

    (a) the set of complex numbers of the form $a + ai$, $a \in \mathbb{R}$ (under addition)

    (b) the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication)

    (c) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n (under addition)

    (d) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n (under addition)

    (e) the set of nonzero real numbers whose square is a rational number (under multiplication)

Solution. Let G be the group in question and let H be the set that we are trying to prove is a subgroup of G.

    (a) Clearly $0 = 0 + 0i \in H$ so that H is nonempty. Suppose $a + ai, b + bi \in H$. Then $a - b \in \mathbb{R}$ so that $(a + ai) - (b + bi) = (a - b) + (a - b)i \in H$ so that $H \leq G$.

    (b) Since $|1| = 1$, then $1 \in H$ so that it is nonempty. Suppose $z, w \in H$. Note that $|w^{-1}| = 1$ since $|w^{-1}| = |\overline{w}|/|w|^2 = 1/1 = 1$. Then

$$|z w^{-1}| = |z||w^{-1}| = (1)(1) = 1$$

    so that $z w^{-1} \in H$. Then $H \leq G$.

    (c) Let $n \in \mathbb{Z}^+$ be fixed. Since $0 = 0/k$ where $k \mid n$, then $0 \in H$ so that it is nonempty. Suppose $a/b, c/d \in H$, where $(a, b) = (c, d) = 1$, and $br = ds = n$ for $r, s \in \mathbb{Z}$. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{ar}{n} - \frac{cs}{n} = \frac{ar - bs}{n}$$

    After reduction, the denominator will still be a divisor of n, so $a/b - c/d \in H$, and $H \leq G$.

    (d) Fix $n \in \mathbb{Z}^+$, and note that $0 = 0/1 \in H$ so that H is nonempty. Suppose $a/b, c/d \in H$ such that $(b, n) = (d, n) = 1$. For any prime p such that $p \mid n$, then $p \nmid b$ and $p \nmid d$. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$$

    Consider $x = (bd, n)$. Then $p \nmid x$, for otherwise $p \mid bd$ implying that $p \mid b$ or $p \mid d$. Then $x = 1$, and $a/b - c/d \in H$ so that $H \leq G$.

    (e) Since $1 = 1^2 = 1/1 \in H$, then H is nonempty. Suppose $a, b \in H$. Then $a^2, b^2 \in \mathbb{Q}$ so that

$$\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} \in H$$

    then $a/b \in H$, and $H \leq G$. $\hspace{2cm}$ $\square$

(2) In each of (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 $\{x \in G \mid |x| = n\} \cup \{1\}$

    (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)

Solution. Let H be the set in question and G be the group.

    (a) Note that $(1\,2), (1\,3) \in H$, but $(1\,2)(1\,3) = (1\,3\,2) \notin H$.

    (b) $s, sr \in H$, but $s(sr) = r \notin H$ as r is not a reflection.

    (c) Let $p \in \mathbb{Z}^+$ such that $p \mid n$. Pick $x \in H$ so that $x^{n/p} \in H$. But $|x^{n/p}| < n$, since $(x^{n/p})^p = x^n = 1$, so H is not closed under the operation.

(d) $1 \in H$, but $1 + 1 = 2 \notin H$.

(e) $\sqrt{2}, \sqrt{3} \in H$, but $(\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{6} + 3 \notin H$, so $\sqrt{2} + \sqrt{3} \notin H$. $\qquad\qquad\square$

(3) Show that the following subsets of the dihedral group D_8 are actually subgroups:

(a) $\{1, r^2, s, sr^2\}$

(b) $\{1, r^2, sr, sr^3\}$

Solution.

(a)

$\circ$	1	r^2	s	sr^2
1	1	r^2	s	sr^2
r^2	r^2	1	sr^2	s
s	s	sr^2	1	r^2
sr^2	sr^2	s	r^2	1

(b)

$\circ$	1	r^2	sr	sr^3
1	1	r^2	sr	sr^3
r^2	r^2	1	sr^3	sr
sr	sr	sr^3	1	r^2
sr^3	sr^3	sr	r^2	1

Both tables show closure, since no product is an element outside of the subset. $\qquad\square$

(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.

Solution. Consider $\mathbb{Z}^+$ and $\mathbb{Z}$ under addition. Then $|\mathbb{Z}^+| = \infty$ and $m + n \in \mathbb{Z}^+$ for any $m, n \in \mathbb{Z}^+$, but $m - n \notin \mathbb{Z}^+$ when $m < n$. Then $\mathbb{Z}^+$ is not a subgroup of $\mathbb{Z}$. $\qquad\square$

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

Solution. Suppose that there did exist H such that $|H| = n - 1$. By Lagrange's Theorem, then $n - 1 \mid n$. Then there exists k such that $k(n - 1) = kn - k = n$, or that $n = k/(k - 1)$. Since $n > 2$, we may safely assume that $k > 2$. Since $n \notin \mathbb{Z}^+$ for any $k > 2$, this contradicts Lagrange's Theorem. $\qquad\square$

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

Solution. Let $\mathrm{Tor}(G)$ denote the torsion subgroup of G. Since $|1| = 1$, then $1 \in \mathrm{Tor}(G)$. Now suppose $g, h \in \mathrm{Tor}(G)$, and put $|g| = m$ and $|h| = n$ for finite m, n. Then

$$(gh^{-1})^{mn} = g^{mn}(h^{-1})^{mn} = (g^m)^n((h^{-1})^n)^m = 1^n 1^m = 1$$

so that $gh^{-1} \in \mathrm{Tor}(G)$. Then $\mathrm{Tor}(G) \leq G$.

Now suppose $G = \mathrm{Aut}(\mathbb{R})$ and consider $\mathrm{Tor}(G) = \{f \in \mathrm{Aut}(\mathbb{R}) \mid |f| < \infty\}$. Then $f(x) = -x$ and $g(x) = 1/x$ are both in $\mathrm{Tor}(G)$, since $f^2(x) = g^2(x) = x$, but $f(g(x)) = -1/x \notin \mathrm{Tor}(G)$, since $(f \circ g)^n(x) = (-1)^n x^{(-1)^n} \neq 1$ for any $n \in \mathbb{Z}$. $\qquad\square$

(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.

Solution. Since every nonidentity element of $\mathbb{Z}$ has infinite order, then $\mathrm{Tor}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \{(0, x) \mid x \in \mathbb{Z}/n\mathbb{Z}\}$, since every $x \in \mathbb{Z}/n\mathbb{Z}$ has finite order as $\mathbb{Z}/n\mathbb{Z}$ is finite. Moreover, if we let H be the set of elements of infinite order along with the identity $(0, 0)$, then $(1, 1), (-1, 0) \in H$, but $(1, 1) + (-1, 0) = (0, 1) \notin H$ because it belongs to the torsion subgroup. $\qquad\square$

(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 $K \subseteq H$.

Solution. Suppose $H \cup K$ is a subgroup. If $H \subseteq K$, we are done. Now suppose $H \nsubseteq K$. Then there exists $h \in H$ such that $h \notin K$. Let $k \in K$. Then $hk \in H \cup K$. If $hk \in K$, then $hk(k^{-1}) = h \in K$, which is a contradiction. Then $hk \in H$. Then $h^{-1} \in H$ so that $h^{-1}(hk) = k \in H$ so that $K \subseteq H$.

   If $H \subseteq K$ then $H \cup K = K$. If $K \subseteq H$, then $H \cup K = H$, both of which are subgroups of G. The result follows. □

(9) Let $G = \mathrm{GL}_n(F)$, where F is any field. Define

$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) \mid \det(A) = 1\}$$

(called the special linear group). Prove that $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$.

Solution. Since $\det(I_n) = 1$, then $I_n \in \mathrm{SL}_n(F)$ so that $\mathrm{SL}_n(F)$ is nonempty. Suppose $A, B \in \mathrm{SL}_n(F)$. Then

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \frac{\det(A)}{\det(B)} = \frac{1}{1} = 1$$

so that $AB^{-1} \in \mathrm{SL}_n(F)$. It follows that $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$. □

(10) (a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.
      (b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable).

Solution.
   (a) Put $L = H \cap K$. Since $1 \in H$ and $1 \in K$, then $1 \in L$ so that L is nonempty. Pick $a, b \in L$. Then $a, b \in H$ and $a, b \in K$. Then $ab^{-1} \in H$ and $ab^{-1} \in K$ so that $ab^{-1} \in L$, hence $L \leq G$.
   (b) Let H_i be a subgroup of G with i belonging to an indexing set I. Let

$$H = \bigcap_{i \in I} H_i$$

   Since $1 \in H_i$ for all i, then $1 \in H$. Suppose $a, b \in H$. Then $a, b \in H_i$ so that $ab^{-1} \in H_i$ for all $i \in I$. It follows that $ab^{-1} \in H$, hence $H \leq G$. □

(11) Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$:
   (a) $\{(a, 1) \mid a \in A\}$
   (b) $\{(1, b) \mid b \in B\}$
   (c) $\{(a, a) \mid a \in A\}$, where we assume $B = A$ (called the diagonal subgroup)

Solution. Let C be the set in each part.
   (a) Since $1 \in A$, then $(1, 1) \in C$ so that C is nonempty. Suppose $(a_1, 1), (a_2, 1) \in C$ for $a_1, a_2 \in A$. Then $a_1 a_2^{-1} \in A$. Then

$$(a_1, 1)(a_2, 1)^{-1} = (a_1, 1)(a_2^{-1}, 1) = (a_1 a_2^{-1}, 1) \in C$$

   so that $C \leq A \times B$.
   (b) See above proof, but suppose $(1, b_1), (1, b_2) \in C$ for $b_1, b_2 \in B$.
   (c) $1 \in A$ so $(1, 1) \in C$, and C is nonempty. For $a_1, a_2 \in A$, then $a_1 a_2^{-1} \in A$ so that

$$(a_1, a_1)(a_2, a_2)^{-1} = (a_1 a_2^{-1}, a_1 a_2^{-1}) \in C$$

   so that $C \leq A^2$. □

(12) Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:
   (a) $\{a^n \mid a \in A\}$
   (b) $\{a \in A \mid a^n = 1\}$

Solution. Let B be the sets in question.

(a) $1^n = 1$, so $1 \in B$. Suppose $a^n, b^n \in B$. Then

$$(a^n)(b^n)^{-1} = (a^n)(b^{-1})^n = (a b^{-1})^n$$

where the last equality follows, since A is abelian. Then $a b^{-1} \in B$, hence $B \le A$.

(b) $1^n = 1$, so $1 \in B$. Suppose $a, b \in B$. Then

$$(a b^{-1})^n = a^n (b^n)^{-1} = 1(1^{-1}) = 1$$

so that $a b^{-1} \in B$, and $B \le A$.   □

(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 $\mathbb{Q}$.

Solution. Let $H \le \mathbb{Q}$. Then $0 \in H$. If no other element is in H, then $H = 0$ and we are done. Suppose that $H \ne 0$ so that there exists $x = a/b \in H$. Moreover, we may take $x > 0$, because if $x < 0$, take $-x > 0$ instead since H has inverses. Note that $b x = a \in H$ so that $1/a \in H$. Then $a(1/a) = 1 \in H$. Then $\mathbb{Z} \subseteq H$, since we may use 1 to build every integer.

Now suppose $r \in \mathbb{Q}$, and put $r = p/q$ for $p, q \in \mathbb{Z}$. Then $q \in H$ so that $1/q \in H$, hence $p(1/q) = r \in H$. Then $\mathbb{Q} \subseteq H$, and $H = \mathbb{Q}$.   □

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

Solution. Let H be the set in question. Then $s, s r \in H$, since $|s| = 2$, and $(s r)^2 = s(s r^{-1}) r = 1$. But $s(s r) = r \notin H$, because $|r| \ge 3$.   □

(15) Let $H_1 \subseteq H_2 \subseteq \cdots$ be an ascending chain of subgroups of G. Prove that $\bigcup_{i=1}^{\infty} H_i$ is a subgroup of G.

Solution. Let $H = \bigcup_{i=1}^{\infty} H_i$. Since $1 \in H_i$ for all i, then $1 \in H$ so that H is nonempty. Pick $a, b \in H$. Then $a \in H_i$ and $b \in H_j$ for some $i, j \in \mathbb{Z}^+$. Then $a, b \in H_k$, where $k = \max(i, j)$. Then $a b^{-1} \in H_k$ so that $a b^{-1} \in H$, hence $H \le G$.   □

(16) Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in \mathrm{GL}_n(F) \mid a_{ij} = 0 \text{ for all } i > j\}$ is a subgroup of $\mathrm{GL}_n(F)$ (called the group of upper triangular matrices).

Solution. Let $\mathrm{UT}_n(F)$ denote the set of $n \times n$ upper triangular matrices with entries from F. Since I_n has all 0s except the diagonal, then $I_n \in \mathrm{UT}_n(F)$ so that $\mathrm{UT}_n(F)$ is nonempty. Suppose $A, B \in \mathrm{UT}_n(F)$. Since $A, B \in \mathrm{GL}_n(F)$, then $\det(A)$ and $\det(B)$ are nonzero. Putting $AB = C = (c_{ij})$ it follows that $\det(C)$ is also nonzero. Note that

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

Suppose $i > j$. Then if $i > k$, then $a_{ik} = 0$, and if $k > j$, then $b_{kj} = 0$ so that $c_{ij} = 0$, hence $C \in \mathrm{UT}_n(F)$.

To show that $A^{-1} \in \mathrm{UT}_n(F)$, put $D \in \mathrm{UT}_n(F)$ such that $AD = DA = I_n$. Proceeding by induction, we show the case for $n = 2$: Consider the matrices

$$A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}, \quad D = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}$$

such that $AD = I_2$. While we may solve for each d_{ij} explicitly, since $D \in \mathrm{GL}_2(F)$, it must be that $d_{ii} \ne 0$, and $d_{12} \in F$, so it remains to show that $d_{21} = 0$. To that end, note that $a_{22} d_{21} = 0$. Since $a_{22} \ne 0$ (otherwise $\det(A) = 0$ and $A \notin \mathrm{GL}_2(F)$), it must be that $d_{21} = 0$, hence $D \in \mathrm{UT}_2(F)$. Suppose now that the inverse D of $A \in \mathrm{GL}_n(F)$ is also upper triangular, and consider $A \in \mathrm{UT}_{n+1}(F)$ and $D \in \mathrm{GL}_{n+1}(F)$ such that $AD = DA = I_{n+1}$. Using block matrices, we may write this as

$$\begin{pmatrix} A_0 & \mathbf{a}_{12} \\ 0 & a_{22} \end{pmatrix} \begin{pmatrix} D_0 & \mathbf{d}_{12} \\ \mathbf{d}_{21}^T & d_{22} \end{pmatrix} = \begin{pmatrix} D_0 & \mathbf{d}_{12} \\ \mathbf{d}_{21}^T & d_{22} \end{pmatrix} \begin{pmatrix} A_0 & \mathbf{a}_{12} \\ 0 & a_{22} \end{pmatrix} = \begin{pmatrix} I_n & \mathbf{0}_{n \times 1} \\ \mathbf{0}_{n \times 1}^T & 1 \end{pmatrix}$$

where $\mathbf{a}_{12}, \mathbf{d}_{12}, \mathbf{d}_{21}^T, \mathbf{0}_{n \times 1}^T$ are $n \times 1$ column vectors, and $a_{22}, d_{22} \in F$. We can see that $D_0 A_0 = I_n$ so that $D_0 \in \mathrm{UT}_n(F)$ by assumption. Moreover, $a_{22} \mathbf{d}_{21}^T = \mathbf{0}_{n \times 1}^T$. Since $a_{22} \ne 0$ because $A \in \mathrm{UT}_{n+1}(F)$, then $\mathbf{d}_{21}^T = \mathbf{0}_{n \times 1}^T$. By induction, then $D \in \mathrm{UT}_{n+1}(F)$, hence the inverse of any upper triangular matrix is also upper triangular.   □

(17) Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in \mathrm{GL}_n(F) \mid a_{ij} = 0 \text{ for all } i > j, \text{ and } a_{ii} = 1 \text{ for all } i\}$ is a subgroup of $\mathrm{GL}_n(F)$.

Solution. Let H be the set in question. Since the diagonal of I_n is only 1's, then $I_n \in H$. Suppose $A, B \in H$. By the previous exercise, $A, B \in \mathrm{UT}_n(F)$, so it remains to show that $a_{ii} = b_{ii} = 1$ for all $1 \le i \le n$. Then

$$(AB)_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki}$$

Since $a_{ik} = 0$ for $k < i$ and $b_{ki} = 0$ for $k > i$, then the sum degrades to $a_{ii} b_{ii} = 1$. Then H is closed under multiplication. Moreover, suppose $D \in \mathrm{UT}_n(F)$ such that $DA = I_n$. Then

$$1 = (DA)_{ii} = d_{ii} a_{ii}$$

where we use the above to collapse the ii-th term of DA. Then $d_{ii} = 1$, hence $D \in H$, and H is closed under inverses. Hence, $H \le \mathrm{GL}_n(F)$. $\qquad\square$

2.2 Centralizers and Normalizers, Stabilizers and Kernels

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

Solution. $g \in C_G(A)$ if and only if $gag^{-1} = a$ if and only if $a = g^{-1} a g$. $\qquad\square$

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

Solution. Recall that $C_G(Z(G)) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in Z(G)\}$. Clearly $C_G(Z(G)) \subseteq G$. Now suppose $g \in G$ and pick $z \in Z(G)$. Then $gz = zg$, or $gzg^{-1} = z$. Then $g \in C_G(Z(G))$, hence $G \subseteq C_G(Z(G))$. It follows that $C_G(Z(G)) = G$. Moreover, because $G = C_G(Z(G)) \le N_G(Z(G))$ and $N_G(Z(G)) \le G$ by definition, then $N_G(Z(G)) = 0$. $\qquad\square$

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

Solution. Pick $g \in C_G(B)$. Then $gbg^{-1} = b$ for all $b \in B$. In particular, $gag^{-1} = a$ for all $a \in A$ because $A \subseteq B$. Then $C_G(B) \subseteq C_G(A)$. Since $C_G(B)$ and $C_G(A)$ are subgroups of G, then $C_G(B) \le C_G(A)$. $\qquad\square$

(4) For each of S_3, D_8, and Q_8 compute the centralizers of each element and find the center of each group. Does Lagrange's Theorem (Section 1.7, Exercise 19) simplify your work?

Solution. Note that for any group G, then $C_G(1) = G$ since every element of G commutes with the identity. Now take $a = (1\,2) \in S_3$. Note that $A = \{1, a\} \le C_{S_3}(a)$ so that 2 divides $|C_{S_3}(a)|$ by Lagrange's Theorem. Similarly, $|C_{S_3}(a)|$ divides $6 = |S_3|$. Since $(1\,3) \notin C_{S_3}(a)$ as $a(1\,3) \ne (1\,3)a$, and a and $(1\,3)$ generate S_3, then no other element of S_3 lies in $C_{S_3}(a)$, hence $C_{S_3}(a) = A$. One can use a similar argument to show that $C_{S_3}((1\,3)) = \{1, (1\,3)\}$ and $C_{S_3}((2\,3)) = \{1, (2\,3)\}$. Moving on to the 3-cycles of S_3, let $a = (1\,2\,3)$ and consider $A = \{1, a, a^2\}$, where $a \ne a^2$ since $|a| = 3$. It similarly follows that $A \le C_{S_3}(a)$ so that 3 divides $|C_G(A)|$ and again, $|C_G(a)|$ divides 6. Since $(1\,2)a \ne a(1\,2)$, then $(1,2) \notin C_{S_3}(a)$ so that $|C_{S_3}(a)| = 3$, and $C_{S_3}(a) = A$. Similarly, $C_{S_3}((1\,3\,2)) = \{1, (1\,3\,2), (1\,2\,3)\}$. Lastly, there is no element in S_3 that commutes with other elements of S_3 except for the identity, so $Z(S_3) = 1$.

The following are the centralizers for each element in D_8:

$$C_{D_8}(r) = \{1, r, r^2, r^3\}$$
$$C_{D_8}(r^2) = D_8$$
$$C_{D_8}(r^3) = \{1, r, r^2, r^3\}$$
$$C_{D_8}(s) = \{1, r^2, s, sr^2\}$$
$$C_{D_8}(sr) = \{1, r^2, sr, sr^3\}$$
$$C_{D_8}(sr^2) = \{1, r^2, s, sr^2\}$$
$$C_{D_8}(sr^3) = \{1, r^2, sr, sr^3\}$$

and $Z(D_8) = \{1, r^2\}$. Lastly, the centralizers of Q_8 are

$$C_{Q_8}(-1) = Q_8$$
$$C_{Q_8}(i) = \{1, -1, i, -i\}$$
$$C_{Q_8}(-i) = \{1, -1, i, -i\}$$
$$C_{Q_8}(j) = \{1, -1, j, -j\}$$
$$C_{Q_8}(-j) = \{1, -1, j, -j\}$$
$$C_{Q_8}(k) = \{1, -1, k, -k\}$$
$$C_{Q_8}(-k) = \{1, -1, k, -k\}$$

and $Z(Q_8) = \{1, -1\}$. $\qquad\qquad\square$

(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 $A = \{1, (1\,2\,3), (1\,3\,2)\}$.
   (b) $G = D_8$ and $A = \{1, s, r^2, s r^2\}$.
   (c) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

Solution.

   (a) Since A is generated by $(1\,2\,3)$, then $A \leq C_G(A)$. By Lagrange's Theorem, then 3 divides $|C_G(A)|$ and $|C_G(A)|$ divides 6. Since $(1\,2) \notin C_G(A)$ because $(1\,2)(1\,2\,3) \neq (1\,2\,3)(1\,2)$, then $C_G(A) = A$.
   Since $C_G(A) \leq N_G(A)$, check $(1\,2)$:

   $$(1\,2)A(1\,2) = \{(1\,2)(1\,2), (1\,2)(1\,2\,3)(1\,2), (1\,2)(1\,3\,2)(1\,2)\} = \{1, (1\,3\,2), (1\,2\,3)\} = A$$

   so that $(1\,2) \in N_G(A)$. Then $N_G(A) = G$, since $(1\,2\,3)(1\,2) = (1\,3)$.
   (b) Note that A is a subgroup so that $A \leq C_G(A)$. Then Lagrange's implies that 4 divides $|C_G(A)|$ and 8 divides $|C_G(A)|$. Since $r \notin C_G(A)$, then $|C_G(A)| = 4$ so that $C_G(A) = A$.
   Take $r \in G$, so that

   $$r A r^{-1} = \{r 1 r^{-1}, r s r^{-1}, r r^2 r^{-1}, r s r^2 r^{-1}\} = \{1, s r^2, r^2, s\} = A$$

   so that $r \in N_G(A)$. Since $C_G(A) \leq N_G(A)$ and $N_G(A) \leq G$, then 4 divides $|N_G(A)|$ which divides 8. Then $N_G(A) = D_8$.
   (c) A is the subgroup of rotations, so 5 divides $|C_G(A)|$ which divides 10. Since $s \notin C_G(A)$ as it doesn't commute with rotations, then $C_G(A) = A$. Moreover,

   $$s A s = \{s 1 s, s r s, s r^2 s, s r^3 s, s r^4 s\} = \{1, r^4, r^3, r^2, r\} = A$$

   so that $s \in N_G(A)$, hence $N_G(A) = G$. $\qquad\qquad\square$

(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.

Solution.

   (a) Fix $h \in H$, and pick $x \in h H h^{-1}$. Then $h x h^{-1} \in H$ since H is closed under inverses and the operation. Moreover, if $x \in H$, then $x \in h H h^{-1}$ by definition so that $h H h^{-1} = H$, hence $h \in N_G(H)$ so that $H \leq N_G(H)$.
   Consider the set $G = D_6$ and $H = \{1, r, s\}$. Then $r H r^{-1} = \{1, r, s r\}$ so that $r \notin N_G(H)$, hence $H \not\leq N_G(H)$.
   (b) Suppose $H \leq C_G(H)$, and consider any $g, h \in H$. In particular, $g \in G$ so that $g h g^{-1} = h$, or $g h = h g$. Then H is abelian.
   If H was abelian, pick $h \in H$. Then for any $g \in H$, we have $h g = g h$, or $h g h^{-1} = g$. Then $h \in C_G(H)$, and $H \leq C_G(H)$. $\qquad\qquad\square$

(7) Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:

(a) $Z(D_{2n}) = \{1\}$ if n is odd.

(b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.

Solution. Instead of solving each problem individually, we proceed as follows: First, we show that every element of $Z(D_{2n})$ must be a rotation. To that end, consider sr^k for some $0 \le k < n$, and consider $r \in D_{2n}$. Then

$$sr^k r = rsr^k \implies sr^{k+1} = sr^{k-1}$$

so that $r^{k+1} = r^{k-1}$, or $r^2 = 1$, contradicting that $n \ge 3$. Then no reflection lies in $Z(D_{2n})$, hence every element of the center must be a rotation.

Since rotations commute with other rotations, it suffices to check whether an arbitrary rotation r^k commutes with s:

$$r^k s = sr^k \implies r^k s = r^{-k} s$$

so that $r^{2k} = 1$. Since $|r| = n$, then $n \mid 2k$. Hence, $r^k \in Z(D_{2n})$ if and only if $n \mid 2k$.

(a) If n is odd, then $2 \nmid n$. Since $n \mid 2k$, it must be that $n \mid k$. Since $0 \le k < n$, then $k = 0$ so that $Z(D_{2n}) = \{1\}$.

(b) If $n = 2m$, then $2m \mid 2k$ implies that $m \mid k$. Then $k = 0$ or $k = m = n/2 < n$ so that $Z(D_{2n}) = \{1, r^m\}$.   □

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

Solution. Since $1(i) = i$, then $1 \in G_i$. Let $\sigma, \tau \in G_i$. Then

$$(\sigma \circ \tau^{-1}) \cdot i = \sigma \cdot (\tau^{-1} \cdot i) = \sigma \cdot (\tau^{-1}(i)) = \sigma \cdot i = \sigma(i) = i$$

where $\tau^{-1}(i) = i$ because $\tau \in S_n$ so that τ^{-1} exists. Then $\sigma \circ \tau^{-1} \in G_i$, hence $G_i \le G$. Moreover, G_i is the set of permutations on $\{1, \ldots, n\}$ such that i is fixed while every other integer may be moved, i.e., $n - 1$ elements may be permuted. Hence, $G_i \cong S_{n-1}$ so that $|G_i| = (n-1)!$.   □

(9) For any subgroup H of G and any nonempty subset A of G define $N_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H (note that A need not be a subset of H).

Solution. Suppose $g \in N_H(A)$. By definition, $g \in H$. Moreover, $gAg^{-1} = A$ and that $g \in H \le G$ implies that $g \in N_G(A)$. Hence, $g \in N_G(A) \cap H$.

Suppose $h \in N_G(A) \cap H$. Since $h \in N_G(A)$. then $hAh^{-1} = A$. Moreover, $h \in H$ implies that $h \in N_H(A)$. It follows that $N_H(A) = N_G(A) \cap H$. Since the intersection of two subgroups is a subgroup (see Section 2.1, Exercise 10), then $N_H(A) \le H$.   □

(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 $H \le Z(G)$.

Solution. Since $|H| = 2$, then $H = \{1, h\}$ for some $h \in G$ where $|h| = 2$. Suppose $g \in N_G(H)$. Then $gHg^{-1} = \{gg^{-1}, ghg^{-1}\} = \{1, ghg^{-1}\} = H$. If $ghg^{-1} = 1$, then $h = 1$ which contradicts that $|H| = 2$. Then $ghg^{-1} = h$ so that $g \in C_G(H)$. From Definition 2.6, we see that $C_G(H) \le N_G(H)$ so that $N_G(H) = C_G(H)$.

Now suppose $N_G(H) = G$, It follows that for any $g \in N_G(H) = G$, then $gHg^{-1} = H$. In particular, we have that $ghg^{-1} = h$ for any $h \in H$. Then $gh = hg$ so that $h \in Z(G)$. Hence, $H \le Z(G)$.   □

(11) Prove that $Z(G) \le N_G(A)$ for any subset A of G.

Solution. Let $g \in Z(G)$. Then $ga = ag$ for any $a \in A$ so that $gag^{-1} = a$. Hence, $gAg^{-1} = A$ so that $Z(G) \subseteq N_G(A)$.   □

(12) Let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 i.e., the members of R are finite sums of elements of the form $a x_1^{r_1} x_2^{r_2} x_3^{r_3} x_4^{r_4}$ where a is any integer and $r_1, \ldots, r_4$ are nonnegative integers. For example,

$$12 x_1^5 x_2^7 x_4 - 18 x_2^3 x_3 + 11 x_1^6 x_2 x_3^3 x_4^{23} \tag{$*$}$$

is a typical element of R. Each $\sigma \in S_4$ gives a permutation of $\{x_1, \ldots, x_4\}$ by defining $\sigma \cdot x_i = x_{\sigma(i)}$. This may be extended to a map from R to R by defining

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$

for all $p(x_1, x_2, x_3, x_4) \in R$ (i.e., σ simply permutes the indices of the variables). For example, if $\sigma = (1\ 2)(3\ 4)$ and $p(x_1, \ldots, x_4)$ is the polynomial in $(*)$ above, then

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = 12x_2^5 x_1^7 x_4 - 18x_1^3 x_4 + 11x_2^6 x_1 x_4^3 x_3^{23}$$
$$= 12x_1^7 x_2^5 x_4 - 18x_1^3 x_4 + 11x_1 x_2^6 x_3^{23} x_4^3.$$

(a) Let $p = p(x_1, \ldots, x_4)$ be the polynomial in $(*)$ above, let $\sigma = (1\ 2\ 3\ 4)$ and let $\tau = (1\ 2\ 3)$. Compute $\sigma \cdot p$, $\tau \cdot (\sigma \cdot p)$, $(\tau \circ \sigma) \cdot p$, and $(\sigma \circ \tau) \cdot p$.

(b) Prove that these definitions give a (left) group action of S_4 on R.

(c) Exhibit all permutations in S_4 that stabilize x_4 and prove that they form a subgroup isomorphic to S_3.

(d) Exhibit all permutations in S_4 that stabilize the element $x_1 + x_2$ and prove that they form an abelian subgroup of order 4.

(e) Exhibit all permutations in S_4 that stabilize the element $x_1 x_2 + x_3 x_4$ and prove that they form a subgroup isomorphic to the dihedral group of order 8.

(f) Show that the permutations in S_4 that stabilizes the element $(x_1 + x_2)(x_3 + x_4)$ are exactly the same as those found in part (e). (The two polynomials appearing in parts (e) and (f) and the subgroup that stabilizes them will play an important role in the study of roots of quartic equations in Section 14.6.)

Solution.

(a) Note that $\tau \circ \sigma = (1\ 3\ 4\ 2)$ and $\sigma \circ \tau = (1\ 3\ 2\ 4)$. Then

$$\sigma \cdot p = 12x_1 x_2^5 x_3^7 - 18x_3^3 x_4 + 11x_1^{23} x_2^6 x_3 x_4^3$$
$$\tau \cdot (\sigma \cdot p) = 12x_1^7 x_2 x_3^5 - 18x_1^3 x_4 + 11x_1 x_2^{23} x_3^6 x_4^3$$
$$(\tau \circ \sigma) \cdot p = 12x_1^7 x_2 x_3^5 - 18x_1^3 x_4 + 11x_1 x_2^{23} x_3^6 x_4^3$$
$$(\sigma \circ \tau) \cdot p = 12x_1 x_3^5 x_4^7 - 18x_2 x_4^3 + 11x_1^{23} x_2^3 x_3^6 x_4$$

(b) Note that $1 \cdot p = p$ for any $p \in R$. Let $\sigma, \tau \in S_4$, then

$$\sigma \cdot (\tau \cdot p(x_1, x_2, x_3, x_4)) = \sigma \cdot p(x_{\tau(1)}, x_{\tau(2)}, x_{\tau(3)}, x_{\tau(4)})$$
$$= p(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, x_{\sigma(\tau(3))}, x_{\sigma(\tau(4))})$$
$$= (\sigma \circ \tau) \cdot p(x_1, x_2, x_3, x_4)$$

(c) To stabilize x_4 means that $\sigma(4) = 4$ which are the permutations: $1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$. Note that these correspond to the elements of S_3 so that they are a subgroup of S_4 that is isomorphic to S_3.

(d) If $\sigma \in S_{4_{x_1+x_2}}$, then $\sigma \cdot (x_1 + x_2) = x_1 + x_2$. This occurs in one of three ways: all digits are fixed, 1 and 2 get swapped, or 1 and 2 are the only digits fixed. The first is the identity permutation, the second are the permutations $(1\ 2)$ and $(1\ 2)(3\ 4)$, and the third is $(3\ 4)$. Since $(1\ 2)$ and $(3\ 4)$ are disjoint, they commute with each other and thus the subset $\{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$ is an abelian subgroup of S_4 with order 4.

(e) To stabilize $x_1 x_2 + x_3 x_4$, note that the identity permutation does this. Another way is to maintain the product $x_3 x_4$ but interchange 1 and 2, or the permutation $(1\ 2)$. Analogously, $(3\ 4)$ is another permutation by interchanging 3 and 4 but fixing 1 and 2. Alternatively, we may also combine these two permutations as $(1\ 2)(3\ 4)$ so that both interchanges occur at the same time. The next way is to interchange the placement of the products themselves, i.e., $x_1 x_2$ in the place of $x_3 x_4$, and vice versa. We obtain two more permutations $(1\ 3)(2\ 4)$ and $(1\ 4)(2\ 3)$, where 1 takes the place of 3 and 2 the place of 4 in the first product, and the second is explained similarly. Lastly, we may perform these interchanges in one full action, which results in the permutations $(1\ 3\ 2\ 4)$ and $(1\ 4\ 2\ 3)$.

Now consider the mapping $\varphi : S_{4_{x_1 x_2 + x_3 x_4}} \to D_8$ given by the following:

$$\varphi((1\ 2)) = s \quad \text{and} \quad \varphi((1\ 3\ 2\ 4)) = r$$

Since $(1\ 2)^2 = (1\ 3\ 2\ 4)^4 = 1$ and $(1\ 2)(1\ 3\ 2\ 4) = (1\ 3\ 2\ 4)^{-1}(1\ 2)$, then φ is an isomorphism. □

(13) Let n be a positive integer and let R be the set of all polynomials with integer coefficients in the independent variables $x_1, x_2, \ldots, x_n$, i.e., the members of R are finite sums of elements of the form $a x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n}$ where a is any integer and $r_1, \ldots, r_n$ are nonnegative integers. For each $\sigma \in S_n$ define a map

$$\sigma : R \to R \quad \text{by} \quad \sigma \cdot p(x_1, x_2, \ldots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

Prove that this defines a (left) group action of S_n on R.

Solution.   Clearly $1 \cdot p(x_1, x_2, \ldots, x_n) = p(x_1, x_2, \ldots, x_n)$. Moreover, for $\sigma, \tau \in S_n$, then

$$
\begin{aligned}
\sigma \cdot (\tau \cdot p(x_1, x_2, \ldots, x_n)) &= \sigma \cdot p(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) \\
&= p(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, \ldots, x_{\sigma(\tau(n))}) \\
&= (\sigma \circ \tau) \cdot p(x_1, x_2, \ldots, x_n)
\end{aligned}
$$

Then it is a group action on R. $\square$

(14) Let $H(F)$ be the Heisenberg group over the field F introduced in Section 1.4, Exercise 11. Determine which matrices lie in the center of $H(F)$ and prove that $Z(H(F))$ is isomorphic to the additive group F.

Solution.   Let $X, Y \in H(F)$ be written as

$$
X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}
$$

where $X \in Z(H(F))$. Then $XY = YX$, implying that

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

Comparing entries, it follows that $af = dc$. Since $d, e, f \in F$ are arbitrary, it follows that this only occurs when $a = c = 0$, for otherwise if at least one of a or c were nonzero, then set f or d to be nonzero respectively to not have equality. Then elements of $Z(H(F))$ must be of the form

$$
Z(H(F)) = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in H(F) \ \middle|\ x \in F \right\}
$$

Moreover, the mapping $\varphi : F \to Z(H(F))$ defined by

$$
\varphi(x) = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
$$

is clearly an isomorphism, so $Z(H(F)) \cong F$. $\square$

2.3   Cyclic Groups and Cyclic Subgroups

(1) Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

Solution.   Recall that the containment relation is the following:

$$
\langle x^a \rangle \leq \langle x^b \rangle \iff (b, 45) \mid (a, 45)
$$

The subgroups of Z_{45} are:

$$
\begin{aligned}
Z_{45} = \langle x \rangle &> \langle x^3 \rangle, \langle x^5 \rangle, \langle x^9 \rangle, \langle x^{15} \rangle, 1 \\
\langle x^3 \rangle &> \langle x^9 \rangle, \langle x^{15} \rangle \\
\langle x^5 \rangle &> \langle x^{15} \rangle \\
\langle x^9 \rangle &> 1 \\
\langle x^{15} \rangle &> 1 \\
1 = \langle x^0 \rangle &
\end{aligned}
$$

$\square$

(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.

Solution. For some $x \in G$ where $|x| = |G| = n$, then **??** says that $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements of G. Since G has n elements only, it follows that these are the elements of G, hence $G = \langle x \rangle$. Moreover, this is not true if G is infinite, since $|\mathbb{Z}| = |2| = \infty$, but $\langle 2 \rangle$ generates only the even integers. $\qquad\square$

(3) Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

Solution. Using **??** and $|\mathbb{Z}/48\mathbb{Z}| = 48$, then $\langle \overline{a} \rangle$ generates $\mathbb{Z}/48\mathbb{Z}$ when $(a, 48) = 1$. We then have $a = 1, 5, 7, 11, 13, 17, 19, 23, 25, 29,$ $\qquad\square$

(4) Find all generators for $\mathbb{Z}/202\mathbb{Z}$.

Solution. Note that $202 = 2 \cdot 101$, which are both prime numbers. Then its generators is every number between 1 and 202, except 101 and even numbers. $\qquad\square$

(5) Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.

Solution. Let φ denote the Euler-φ function. Then

$$\begin{aligned} \varphi(49000) &= \varphi(2^3)\varphi(5^3)\varphi(7^2) \\ &= 2^2(2-1)5^2(5-1)7(7-1) \\ &= 16800 \end{aligned}$$

$\qquad\square$

(6) In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle \overline{a} \rangle$ for every $\overline{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

Solution. The elements of each subgroup are

$$\begin{aligned} \mathbb{Z}/48\mathbb{Z} = \langle \overline{1} \rangle &= \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{46}, \overline{47}\} \\ \langle \overline{2} \rangle &= \{\overline{0}, \overline{2}, \overline{4}, \ldots, \overline{44}, \overline{46}\} \\ \langle \overline{3} \rangle &= \{\overline{0}, \overline{3}, \overline{6}, \ldots, \overline{42}, \overline{45}\} \\ \langle \overline{4} \rangle &= \{\overline{0}, \overline{4}, \overline{8}, \ldots, \overline{40}, \overline{44}\} \\ \langle \overline{6} \rangle &= \{\overline{0}, \overline{6}, \overline{12}, \ldots, \overline{36}, \overline{42}\} \\ \langle \overline{8} \rangle &= \{\overline{0}, \overline{8}, \overline{16}, \overline{24}, \overline{32}, \overline{40}\} \\ \langle \overline{12} \rangle &= \{\overline{0}, \overline{12}, \overline{24}, \overline{36}\} \\ \langle \overline{16} \rangle &= \{\overline{0}, \overline{16}, \overline{32}\} \\ \langle \overline{24} \rangle &= \{\overline{0}, \overline{24}\} \\ \langle \overline{0} \rangle &= \{\overline{0}\} \end{aligned}$$

Moreover, the subgroup inclusions are

$$\begin{aligned} \langle \overline{1} \rangle &\geq \langle \overline{0} \rangle, \langle \overline{1} \rangle, \langle \overline{2} \rangle, \langle \overline{3} \rangle, \langle \overline{4} \rangle, \langle \overline{6} \rangle, \langle \overline{8} \rangle, \langle \overline{12} \rangle, \langle \overline{16} \rangle, \langle \overline{24} \rangle \\ \langle \overline{2} \rangle &\geq \langle \overline{0} \rangle, \langle \overline{2} \rangle, \langle \overline{4} \rangle, \langle \overline{6} \rangle, \langle \overline{8} \rangle, \langle \overline{12} \rangle, \langle \overline{24} \rangle \\ \langle \overline{3} \rangle &\geq \langle \overline{3} \rangle, \langle \overline{6} \rangle, \langle \overline{12} \rangle, \langle \overline{24} \rangle \\ \langle \overline{4} \rangle &\geq \langle \overline{0} \rangle, \langle \overline{4} \rangle, \langle \overline{8} \rangle, \langle \overline{12} \rangle, \langle \overline{16} \rangle, \langle \overline{24} \rangle \\ \langle \overline{6} \rangle &\geq \langle \overline{0} \rangle, \langle \overline{6} \rangle, \langle \overline{12} \rangle, \langle \overline{24} \rangle \\ \langle \overline{8} \rangle &\geq \langle \overline{0} \rangle, \langle \overline{8} \rangle, \langle \overline{16} \rangle, \langle \overline{24} \rangle \\ \langle \overline{12} \rangle &\geq \langle \overline{0} \rangle, \langle \overline{12} \rangle, \langle \overline{24} \rangle \\ \langle \overline{16} \rangle &\geq \langle \overline{0} \rangle, \langle \overline{16} \rangle \\ \langle \overline{24} \rangle &\geq \langle \overline{0} \rangle, \langle \overline{24} \rangle \\ \langle \overline{0} \rangle &\geq \langle \overline{0} \rangle \end{aligned}$$

$\qquad\square$

(7) Let $Z_{48} = \langle x \rangle$ and use the isomorphism $\mathbb{Z}/48\mathbb{Z} \cong Z_{48}$ given by $\overline{1} \mapsto x$ to list all subgroups of Z_{48} as computed in the preceding exercise.

Solution. The subgroups of Z_{48} are $\langle x \rangle, \langle x^2 \rangle, \langle x^3 \rangle, \langle x^4 \rangle, \langle x^6 \rangle, \langle x^8 \rangle, \langle x^{12} \rangle, \langle x^{16} \rangle, \langle x^{24} \rangle$, and 1. $\qquad\square$

(8) Let $Z_{48} = \langle x \rangle$. For which integers a does the map φ_a defined by $\varphi_a : \overline{1} \mapsto x^a$ extend to an isomorphism from $\mathbb{Z}/48\mathbb{Z}$ to Z_{48}?

Solution. Let a such that $(a, 48) = d > 1$, and put $b = 48/d$. Since φ_a is a homomorphism, then

$$\varphi_a(\overline{b}) = \varphi_a(b \cdot \overline{1}) = \varphi_a(\overline{1})^b = x^{ab} = (x^{48})^{a/d} = 1 = \varphi_a(\overline{0})$$

Since $\overline{1} \in \ker(\varphi_a)$, then φ_a is not injective. Now suppose we pick a such that $(a, 48) = 1$. Suppose $\overline{b} = \overline{c}$ in $\mathbb{Z}/48\mathbb{Z}$. Then $b - c = 48k$ for some $k \in \mathbb{Z}$, and

$$\varphi_a(\overline{b}) = \varphi_a(b \cdot \overline{1}) = x^{ab} = x^{ac+48ka} = x^{ac} = \varphi_a(\overline{c})$$

so that φ_a is well-defined when a is relatively prime to 48. Moreover,

$$\varphi_a(\overline{b} + \overline{c}) = x^{a(b+c)} = x^{ab+ac} = x^{ab} x^{ac} = \varphi_a(\overline{b})\varphi_a(\overline{c})$$

so that φ_a is a homomorphism. Now suppose $\varphi_a(\overline{b}) = \varphi_a(\overline{c})$ for $\overline{b}, \overline{c} \in \mathbb{Z}/48\mathbb{Z}$. Then $x^{ab} = x^{ac}$, or $x^{a(b-c)} = 1$. Then $48 \mid a(b-c)$, and since $(a, 48) = 1$, then $48 \mid b - c$ so that $\overline{b} = \overline{c}$, and φ_a is injective. Moreover, $|\mathbb{Z}/48\mathbb{Z}| = |Z_{48}|$ implies that φ_a is also surjective, hence it is an isomorphism. $\qquad\square$

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

Solution. Suppose $\overline{b} = \overline{c}$ for $\overline{b}, \overline{c} \in \mathbb{Z}/48\mathbb{Z}$. Suppose ψ_a is already well-defined. Then $\psi_a(\overline{b}) = \psi_a(\overline{c})$, or $x^{ab} = x^{ac}$, which implies that $x^{a(b-c)} = 1$. Then $36 \mid a(b-c)$, but recall that $48 \mid b - c$. Then $36m = a(b-c)$ and $48n = b - c$ for $m, n \in \mathbb{Z}$, or $36m = 48an$. If we choose b, c such that $n = 1$, then this reduces to $36m = 48a$ so that $36 \mid 48a$. Equivalently, we may reduce by $(36, 48)$ so that $3 \mid 4a$. Since $3 \nmid 4$, it must be that $3 \mid a$ so that ψ_a is well-defined only when $3 \mid a$. Moreover,

$$\psi_a(\overline{b} + \overline{c}) = x^{a(b+c)} = x^{ab} x^{ac} = \psi_a(\overline{b})\psi_a(\overline{c})$$

so that ψ_a is a homomorphism. Lastly, if ψ_a were to be surjective, then x^a must have order 36. But by **??**, we have $|x^a| = 36/(36, a)$, and $(36, a) \geq 3$ because $3 \mid a$. Hence, ψ_a can never be surjective. $\qquad\square$

(10) What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all of the elements and their orders in $\langle \overline{30} \rangle$.

Solution. By **??**, we have $|\overline{1}| = 54$. Then

$$|\overline{30}| = |30 \cdot \overline{1}| = \frac{54}{(54, 30)} = \frac{54}{6} = 9$$

The first element of order 9 in $\mathbb{Z}/54\mathbb{Z}$ is $\overline{6}$, so

$$\langle \overline{30} \rangle = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}, \overline{42}, \overline{48}\}$$

Moreover, the orders are

$$
\begin{array}{lll}
|\overline{0}| = 1 & |\overline{6}| = 9 & |\overline{12}| = 9 \\
|\overline{18}| = 3 & |\overline{24}| = 9 & |\overline{30}| = 9 \\
|\overline{36}| = 3 & |\overline{42}| = 9 & |\overline{48}| = 9
\end{array}
$$

$\qquad\square$

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

Solution. The cyclic subgroups of D_8 are

$$
\begin{aligned}
\langle 1 \rangle &= \{1\} \\
\langle r \rangle = \langle r^3 \rangle &= \{1, r, r^2, r^3\} \\
\langle r^2 \rangle &= \{1, r^2\} \\
\langle s \rangle &= \{1, s\} \\
\langle sr \rangle &= \{1, sr\} \\
\langle sr^2 \rangle &= \{1, sr^2\} \\
\langle sr^3 \rangle &= \{1, sr^3\}
\end{aligned}
$$

Moreover, a proper subgroup that is not cyclic is $\langle r^2, s \rangle = \{1, r^2, s, sr^2\}$. $\qquad\square$

(12) Prove that the following groups are *not* cyclic:
  (a) $Z_2 \times Z_2$
  (b) $Z_2 \times \mathbb{Z}$
  (c) $\mathbb{Z} \times \mathbb{Z}$

Solution.

(a) Put $Z_2 = \langle x \rangle$. We may inspect all four elements:

$$\langle (1,1) \rangle = \{(1,1)\}$$
$$\langle (x,1) \rangle = \{(1,1),(x,1)\}$$
$$\langle (1,x) \rangle = \{(1,1),(1,x)\}$$
$$\langle (x,x) \rangle = \{(1,1),(x,x)\}$$

No subgroup has order 4, hence no subgroup generates $Z_2 \times Z_2$.

(b) If (a,b) generates $Z_2 \times \mathbb{Z}$, then it must be one of the forms $(1,\pm 1)$ or $(x,\pm 1)$, since $\langle \pm 1 \rangle = \mathbb{Z}$. But $(1,\pm 1)$ generates elements whose first component is only 1. If we consider $(x,\pm 1)$, then this also doesn't generate $Z_2 \times \mathbb{Z}$ since $(1,1) \notin \langle (x,\pm 1) \rangle$.

(c) The only candidates for generators of $\mathbb{Z} \times \mathbb{Z}$ is $(\pm 1, \pm 1)$. But any subgroup generated by $(\pm 1, \pm 1)$ contain elements that differ only in sign as $(x,y) \notin \langle (\pm 1, \pm 1) \rangle$ when $|x| \neq |y|$.   □

(13) Prove that the following pairs of groups are *not* isomorphic:

(a) $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$

(b) $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$.

Solution.

(a) $(0,x) \in \mathbb{Z} \times Z_2$ has order 2, but no element in $\mathbb{Z}$ has order 2.

(b) Same reason as above.   □

(14) Let $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$. For each of the following integers a compute σ^a: $a = 13, 65, 626, 1195, -6, -81, -570,$ and -1211.

Solution. Since $|\sigma| = 12$, then we know that $\langle \sigma \rangle$ has 12 distinct elements. We may then use the Division Algorithm to reduce the integers to their least residue:

$$\sigma^{13} = \sigma^{12+1} = \sigma$$
$$\sigma^{65} = \sigma^{5(12)+5} = \sigma^5 = (1\ 6\ 11\ 4\ 9\ 2\ 7\ 12\ 5\ 10\ 3\ 8)$$
$$\sigma^{626} = \sigma^{52(12)+2} = \sigma^2 = (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12)$$
$$\sigma^{1195} = \sigma^{99(12)+7} = \sigma^7 = (1\ 8\ 3\ 10\ 5\ 12\ 7\ 2\ 9\ 4\ 11\ 6)$$
$$\sigma^{-6} = \sigma^{-1(12)+6} = \sigma^6 = (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12)$$
$$\sigma^{-81} = \sigma^{-7(12)+3} = \sigma^3 = (1\ 4\ 7\ 10)(2\ 5\ 8\ 11)(3\ 6\ 9\ 12)$$
$$\sigma^{-570} = \sigma^{-48(12)+6} = \sigma^6$$
$$\sigma^{-1211} = \sigma^{-101(12)+1} = \sigma \qquad\qquad □$$

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

Solution. If it were cyclic, then all subgroups are also cyclic, by **??**. But $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.   □

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

Solution. Let ℓ be the least common multiple of m and n. Then there exist $a,b \in \mathbb{Z}$ such that $\ell = am = bn$. Then

$$(xy)^\ell = x^\ell y^\ell = x^{bn} y^{am} = 1 \cdot 1 = 1$$

so that by **??**, then $|xy|$ divides ℓ. Moreover, this is not true if x and y do not commute. If we consider $r,s \in D_8$, then $|r| = 4$ and $|s| = 2$, but $|rs| = 2$ which 4 does not divide. Lastly, consider $\mathbb{Z}/2\mathbb{Z}$. Then $|\bar{1}| = 2$, but $|\bar{1} + \bar{1}| = |\bar{0}| = 1$.   □

(17) Find a presentation for Z_n with one generator.

Solution. $Z_n = \langle x \mid x^n = 1 \rangle$. $\square$

(18) Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $Z_n = \langle x \rangle$ to h such that $x \mapsto h$.

Solution. Define the map $\varphi : Z_n \to H$ by
$$\varphi(x^k) = h^k$$

We first prove that it is well-defined. If $x^a = x^b$, then $x^{a-b} = 1$ so that $n \mid (a-b)$. Then there exists $c \in \mathbb{Z}$ such that $cn = a - b$, or $a = cn + b$. Then

$$\varphi(x^a) = h^a = h^{cn+b} = h^b = \varphi(x^b)$$

Moreover, let $x^s, x^t \in Z_n$. Then

$$\varphi(x^s x^t) = \varphi(x^{s+t}) = h^{s+t} = h^s h^t = \varphi(x^s)\varphi(x^t)$$

so that φ is a homomorphism. To show uniqueness, suppose $\psi : Z_n \to H$ is another homomorphism such that $\psi(x) = h$. It follows that we need to show $\psi(x^k) = h^k$. Proceeding by induction, we have $\psi(x) = h$ so the base case is established. Assuming it holds for some k, then

$$\psi(x^{k+1}) = \psi(x^k x) = h^k h = h^{k+1}$$

so that $\psi = \varphi$ by induction. $\square$

(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 $1 \mapsto h$.

Solution. Define the map $\varphi : \mathbb{Z} \to H$ as
$$\varphi(n) = h^n$$

Then $\varphi(1) = h$. Moreover, for any $s, t \in \mathbb{Z}$, then

$$\varphi(s + t) = h^{s+t} = h^s h^t = \varphi(s)\varphi(t)$$

so that φ is a homomorphism. Lastly, if $\psi : \mathbb{Z} \to H$ is another homomorphism such that $\psi(1) = h$, it must satisfy $\psi(n) = \psi(n \cdot 1) = \psi(1)^n = h^n$. $\square$

(20) Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{p^n} = 1$, then $|x| = p^m$ for some $m \leq n$.

Solution. If $x^{p^n} = 1$, then **??** says that $|x|$ divides p^n. Since p is prime, then $|x|$ must also be a power of p that is at most n. $\square$

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

Solution. We proceed by induction. For $n = 1$, we have the following:

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

where 1 and p^2 are for $k = 0$ and $k = 1$ respectively. Note that for $k \geq 2$, then $\binom{p}{k}$ is divisible by p because dividing by $p!$ by $(p - k)!$ results in $p(p-1)\cdots(p-k+1)$, and $k!$ must divide all other terms but p because p is prime. Then for terms $k \geq 2$, we result in $p m_k p^k$ for $k \geq 2$ where $p m_k$ denotes the expanded binomial coefficient $\binom{p}{k}$, and p^k denotes the other term in the summation. For $k \geq 2$, this results in $p^{k+1} m_k$ so that each term contains at least p^3 and is divisible by p. Thus, $(1+p)^p \equiv 1 \bmod p$, and the base case is established.

Moreover, we may write $(1+p)^p = 1+p^2 + M_1 p^3 = 1+p^2(1+M_1 p)$, where $M_1 \in \mathbb{Z}$ corresponds to the rest of the summation terms with subscript 1 corresponding to $n=1$. Now suppose it holds for some n, or that

$$(1+p)^{p^{n-1}} = 1 + p^n(1+M_n p)$$

where $M_n \in \mathbb{Z}$ and reduces to 1 mod p^n. Then for $n+1$, we have

$$(1+p)^{p^n} = (1+p^n(1+M_n p))^p$$

where we set each side to the power of p. Using the Binomial Theorem, we have

$$(1+p^n(1+M_n p))^p = \sum_{j=0}^{p}\binom{p}{j}p^{nj}(1+M_n p)^j = 1 + p^{n+1}(1+M_n p) + \sum_{j=2}^{p}\binom{p}{j}p^{nj}(1+M_n p)^j$$

Note that for $j \geq 2$, we will have terms containing at least $p^{2n} = p^{n+1}p^{n-1}$ times some constant, which reduces to 0 mod p^{n+1}. Moreover, the $j=1$ term reduces to 0 mod p^{n+1} so that $(1+p)^{p^n} \equiv 1$ mod p^{n+1} so that by the inductive hypothesis, we have $(1+p)^{p^{n-1}} \equiv 1$ mod p^n. If we put $n-1$, then

$$(1+p)^{p^{n-2}} = 1 + p^{n-1}(1+M_{n-1}p) = 1 + p^{n-1} + M_{n-1}p^n$$

Taking this mod p^n, we have the left over term $1+p^{n-1} \neq 1$. Since any element in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ must have order that divide $p^{n-1}(p-1)$, we must only check powers of p, since $(1+p)^k = 1 + kp + \cdots \equiv 1$ mod p^2 implies that $kp \equiv 0$ mod p^2 so that $p \mid k$. Since p^{n-1} results in 1 and p^{n-2} doesn't, it follows that $|1+p| = p^{n-1}$. $\square$

(22) Let n be an integer ≥ 3. Use the Binomial Theorem to show that $(1+2^2)^{2^{n-2}} \equiv 1$ mod 2^n but $(1+2^2)^{2^{n-3}} \not\equiv 1$ mod 2^n. Deduce that 5 is an element of order 2^{n-2} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Solution. Like Exercise 21, we will proceed by induction, so we analyze the base case $n=3$. We have

$$(1+2^2)^2 = 25 \equiv 1 \bmod 2^2$$

so it holds true. Suppose the relationship holds for some n. Before moving on to $n+1$, we may rewrite $(1+2^2)^{2^{n-2}}$ in a better form using the Binomial Theorem:

$$(1+2^2)^{2^{n-2}} = \sum_{k=0}^{2^{n-2}}\binom{2^{n-2}}{k}2^{2k} = 1 + 2^n + \sum_{k=2}^{2^{n-2}} \frac{2^{n-2}(2^{n-2}-1)\cdots(2^{n-2}-k+1)}{k!}2^{2k}$$

Evaluating the right most expression for each $k \geq 2$, we notice the following. Using the formula obtained in [Section 0.2, Exercise 8](), note that the largest power of 2 that $k!$ divides is $k-1$:

$$\sum_{i=1}^{\lfloor \log_2(k)\rfloor}\left\lfloor \frac{k}{2^i}\right\rfloor \leq \sum_{i=1}^{\lfloor \log_2(k)\rfloor}\frac{k}{2^i} = \frac{k}{2} + \frac{k}{4} + \cdots < k$$

Moreover, this value must be an integer. Then it must be at most $k-1$. The numerator contains at least $n-2$ 2's, as the other terms contribute at most another 2, since they are either odd (such as $2^{n-2}-1$), or even (such as $2^{n-2}-2 = 2(2^{n-3}-1)$). Therefore, there are at least $n-2$ 2's in the numerator. Coupling with the 2^{2k} term, there are $2k$ more 2's in the numerator as well. Counting all of these, we have $n-2+2k-(k-1) = n+k-1$. Since we are considering only $k \geq 2$, then $n+k-1 \geq n+2-1 = n+1 > n$ so that each term for $k \geq 2$ contains at least 2^n. We may then rewrite the binomial expansion as

$$(1+2^2)^{2^{n-2}} = 1 + M_n 2^n$$

where M_n is the associated constant for the case n after factoring out 2^n out of each term in the summation $k=1$ onward. Then for $n+1$, we see that

$$(1+2^2)^{2^{n+1-2}} = (1+M_n 2^n)^2 = 1 + M_n 2^{n+1} + M_n^2 2^{2n} = 1 + 2^n(2M_n + 2^n M_n^2) \equiv 1 \bmod 2^n$$

so that the result holds by the inductive hypothesis. Moreover, if we put $n-1$ in the hypothesis, then

$$(1+2^2)^{2^{n-3}} = 1 + M_n 2^{n-1} \not\equiv 1 \bmod 2^n$$

Using similar reasoning as in Exercise 21, we need only check powers of 2. Moreover, we do not need to check 2^{n-1}, because $5 \equiv 1 \bmod 4$, and if $x \equiv 1 \bmod 4$, this covers half of the order of 2^{n-1}, which is 2^{n-2} (the other half is seen by some $x \equiv 3 \bmod 4$). Since 2^{n-2} results in $1 \bmod 2^n$ and 2^{n-3} does not, it follows that 5 has order 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$.   □

(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.]

Solution. By **??**, we must have one subgroup of order 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ if it were cyclic. However,

$$(2^n - 1)^2 = (-1)^2 \equiv 1 \bmod 2^n$$

and

$$(2^{n-1} + 1)^2 = 2^{2n-2} + 2^n + 1 \equiv 1 \bmod 2^n$$

Since $n \geq 3$, then $2^n - 1 \neq 2^{n-1} + 1$ but both have order 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. Hence, it cannot be cyclic.   □

(24) Let G be a finite group and let $x \in G$.

(a) Prove that if $g \in N_G(\langle x \rangle)$ then $g x g^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Prove conversely that if $g x g^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle x \rangle)$. [Show first that $g x^k g^{-1} = (g x g^{-1})^k = x^{ak}$ for any integer k so that $g \langle x \rangle g^{-1} \leq \langle x \rangle$. If x has order n, show that the elements $g x^i g^{-1}, i = 0, 1, \ldots, n-1$ are distinct, so that $|g \langle x \rangle g^{-1}| = |\langle x \rangle| = n$ and conclude that $g \langle x \rangle g^{-1} = \langle x \rangle$.]

Note that this cuts down some of the work in commuting normalizers of cyclic subgroups since one does not have to check $g h g^{-1} \in \langle x \rangle$ for every $h \in \langle x \rangle$.

Solution.

(a) Since $g \in N_G(\langle x \rangle)$, then $g \langle x \rangle g^{-1} = \langle x \rangle$ so that $g x g^{-1} \in \langle x \rangle$. Then $g x g^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) We first prove $g x^k g^{-1} = (g x g^{-1})^k$ for any $k \in \mathbb{Z}$. $k = 0$ and $k = 1$ is trivial, while $(g x g^{-1})^{-1} = g x^{-1} g^{-1}$ so that proving the result for positive integers will hold true for all integers. To that end, suppose $(g x g^{-1})^k = g x^k g^{-1}$. Then

$$(g x g^{-1})^{k+1} = (g x g^{-1})^k (g x g^{-1}) = g x^{k+1} g^{-1}$$

so that it holds true by induction. Now if $y \in g \langle x \rangle g^{-1}$, then there is some $m \in \mathbb{Z}$ such that $y = g x^m g^{-1} = x^{am}$ so that $g \langle x \rangle g^{-1} \leq \langle x \rangle$. Moreover, we know that conjugation is an isomorphism so that $|g x g^{-1}| = |x|$. Then $|g \langle x \rangle g^{-1}| = |\langle x \rangle|$ so that $g \langle x \rangle g^{-1} = \langle x \rangle$.   □

(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 that the same is true for any finite group of order n. (For such k each element has a kth 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.)

Solution. Fix $k \in \mathbb{Z}$ such that $(k, n) = 1$, where $|G| = n$. Then there exist $a, b \in \mathbb{Z}$ such that $ak + bn = 1$. Pick some $g \in G$, where we note that $g^n = 1$ since G is cyclic with order n. Then

$$\varphi(g^a) = g^{ak} = g^{1-bn} = g(g^n)^{-b} = g$$

so that φ is surjective.   □

(26) Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a : Z_n \to Z_n \quad \text{by} \quad \sigma_a(x) = x^a \text{ for all } x \in Z_n$$

(a) Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime.

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \bmod n$.

(c) Prove that *every* automorphism of Z_n is equal to σ_a for some integer a.

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\bar{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $\mathrm{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$).

Solution.

(a) Suppose $\sigma_a \in \mathrm{Aut}(Z_n)$, and put $d = (n, a)$. Then there are $s, t \in \mathbb{Z}$ such that $n = ds$ and $a = dt$. If $Z_n = \langle x \rangle$, then

$$\sigma_a(x^s) = x^{as} = x^{dst} = x^{nt} = 1 = \sigma_a(1)$$

If $x^s \neq 1$, then $\sigma_a \notin \mathrm{Aut}(Z_n)$ as it would have a non-trivial kernel. It must be that $x^s = 1$, and since $|x| = n$ and $n \mid s$, then $s = n$ so that $d = 1$.

Suppose that $(a, n) = 1$. By the previous exercise, then σ_a is a surjective map. Since Z_n is finite, then σ_a is also bijective. Moreover,

$$\sigma_a(xy) = (xy)^a = x^a y^a = \sigma_a(x)\sigma_a(y)$$

for some $x, y \in Z_n$. Then σ_a is also a homomorphism, hence $\sigma_a \in \mathrm{Aut}(Z_n)$.

(b) Let $Z_n = \langle x \rangle$. If $\sigma_a = \sigma_b$, then $\sigma_a(x) = \sigma_b(x)$. In particular, $x^a = x^b$, or $x^{a-b} = 1$. By **??**, then $n \mid (a - b)$ or $a \equiv b \bmod n$.

If $a \equiv b \bmod n$, then there is some $c \in \mathbb{Z}$ such that $a = b + cn$. Then for any $x^m \in Z_n$, we have

$$\sigma_a(x^m) = x^{am} = x^{(b+cn)m} = x^{bm+cnm} = x^{bm}(x^n)^{cm} = x^{bm} = \sigma_b(x^m)$$

so that $\sigma_a = \sigma_b$.

(c) Let $Z_n = \langle x \rangle$ again, and suppose $\varphi \in \mathrm{Aut}(Z_n)$ where $\varphi(x) = x^k$ for some $k \in \mathbb{Z}$. Then for any $x^m \in Z_n$, we have

$$\varphi(x^m) = \varphi(x)^m = x^{km} = \sigma_k(x^m)$$

so that $\varphi = \sigma_k$.

(d) It is clear for any $x^m \in Z_n$ that

$$\sigma_a(\sigma_b(x^m)) = \sigma_a(x^{bm}) = x^{abm} = \sigma_{ab}(x^m)$$

so that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Part (a) shows that $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $\sigma_a \in Z_n$, so we may define the map

$$\psi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(Z_n) \quad \text{where} \quad \bar{a} \mapsto \sigma_a$$

Moreover, the "only if" direction in part (b) shows that ψ is well-defined, and the "if" direction shows that ψ is injective. Also, part (c) shows that ψ is surjective, hence $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(Z_n)$. □

2.4   Subgroups Generated by Subsets of a Group

(1) Prove that if H is a subgroup of G then $\langle H \rangle = H$.

Solution. It is clear that $H \subseteq \langle H \rangle$ by definition. If $h \in \langle H \rangle$, recall that $\langle H \rangle$ is the intersection of all subgroups that contain H, and H is a subgroup that contains itself. Then $h \in H$ so that $\langle H \rangle \subseteq H$. □

(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 $\langle A \rangle = \langle B \rangle$.

Solution. If $a \in \langle A \rangle$, then $a \in A$ so that $a \in B$. Then $a \in \langle B \rangle$, hence $\langle A \rangle \leq \langle B \rangle$. Moreover, take $\langle A \rangle = \{x\}$ and $B = \{x, x^2\}$ in Z_4. Then $A \subset B$, but $\langle A \rangle = \langle B \rangle = Z_4$. □

(3) Prove that if H is an abelian subgroup of a group G then $\langle H, Z(G) \rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H) \rangle$ is not abelian.

Solution. Let $g, h \in \langle H, Z(G) \rangle$. Using **??**, we may put them as follows:

$$g = g_1^{\varepsilon_1} g_2^{\varepsilon_2} \dots g_m^{\varepsilon_m}, \quad h = h_1^{\delta_1} h_2^{\delta_2} \dots h_n^{\delta_n}$$

where $\varepsilon_i = \delta_i = \pm 1$, and $g_i, h_i \in H \cup Z(G)$ for all i. Since both H and $Z(G)$ are abelian, then elements of H and $Z(G)$ commute with each other. Then

$$g h = g_1^{\varepsilon_1} \dots g_m^{\varepsilon_m} h_1^{\delta_1} \dots h_n^{\delta_n} = h_1^{\delta_1} \dots h_n^{\delta_n} g_1^{\varepsilon_1} \dots g_m^{\varepsilon_m} = h g$$

so that $\langle H, Z(G) \rangle$ is abelian. Moreover, put $G = D_8$ and $H = \{1, r^2\}$. Since $H \subseteq Z(D_8)$, then $C_G(D_8) = D_8$, which is not abelian.   □

(4) Prove that if H is a subgroup of G then H is generated by the set $H - \{1\}$.

Solution. If $H = \{1\}$, then $H - \{1\}$ is empty so that $\langle H - \{1\} \rangle = \{1\}$. Suppose $|H| > 1$, and let $h \in H$ that is not the identity. Then $h^{-1} \in H$ so $1 = h h^{-1} \in \langle H - \{1\} \rangle$ so that $H \le \langle H - \{1\} \rangle$. Moreover, $1 \in \langle H - \{1\} \rangle$ and $\langle H - \{1\} \rangle$ being the minimal set to contain $H - \{1\}$ (now equipped with 1) must also be in H. Then $H = \langle H - \{1\} \rangle$.   □

(5) Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3.

Solution. Consider the 2-cycles $(1\ 2)$ and $(1\ 3)$. Then

$$(1\ 2)(1\ 3) = (1\ 3\ 2)$$
$$(1\ 3)(1\ 2) = (1\ 2\ 3)$$
$$(1\ 3\ 2)(1\ 2) = (2\ 3)$$

so that $\langle (1\ 2), (1\ 3) \rangle = S_3$. One can also do similar calculations to ensure $\langle (1\ 2), (2\ 3) \rangle = \langle (1\ 3), (2\ 3) \rangle = S_3$.   □

(6) Prove that the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 2)(3\ 4)$ is a noncyclic group of order 4.

Solution. Let $a = (1\ 2)$ and $b = (3\ 4)$. Then $\langle a, ab \rangle = \{1, a, b, ab\}$ where $ab = ba$ since they are disjoint cycles. Moreover, $|a| = |b| = |ab| = 2$ so that it is noncyclic.   □

(7) Prove that the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 3)(2\ 4)$ is isomorphic to the dihedral group of order 8.

Solution. Put $\alpha = (1\ 2)$ and $\beta = (1\ 3)(2\ 4)$. Then $\gamma = \alpha\beta = (1\ 3\ 2\ 4)$. Since $|\gamma| = 4$, then $\alpha\beta$ maps to $r \in D_8$. Moreover, for some $\delta \in \langle \alpha, \beta \rangle$ to map to s, it must be that $\alpha\beta\delta = \delta(\alpha\beta)^{-1} = \delta\beta\alpha$, where $\alpha\beta = \beta\alpha$ since $|\alpha| = |\beta| = 2$. By inspection, $\delta = \alpha$, hence α and γ satisfies $r^4 = s^2 = 1$. Then there is a homomorphism $\varphi : D_8 \to \langle \alpha, \beta \rangle$ given by

$$\varphi(s^i r^j) = \alpha^i (\alpha\beta)^j, \quad \text{where } i \in \{0, 1\}, j \in \{0, 1, 2, 3\}$$

Since γ, γ^2, and γ^3 are distinct elements, then φ is injective. Moreover, since $\gamma\alpha = \alpha\gamma^{-1} \in \langle \alpha, \beta \rangle$, then any product of α and β can be reduced to $\alpha^i (\alpha\beta)^j$ so that φ is surective. Since its bijective, then φ is an isomorphism, hence $D_8 = \langle \alpha, \beta \rangle$.   □

(8) Prove that $S_4 = \langle (1\ 2\ 3\ 4), (1\ 2\ 4\ 3) \rangle$.

Solution. Let $A = \langle (1\ 2\ 3\ 4), (1\ 2\ 4\ 3) \rangle$ where $\alpha = (1\ 2\ 3\ 4)$ and $\beta = (1\ 2\ 4\ 3)$. Then $\alpha\beta = (1\ 3\ 2)$, which has order 3. Then $|\langle \alpha\beta \rangle| = 3$ and is a subgroup of A so that 3 and 4 divide $|A|$. Since $A \le S_4$, then $|A|$ divides 24 as well. Then $|A| = 12$ or 24. Note that $\alpha^2 = (1\ 3)(2\ 4)$, and we obtain $(1\ 2)$ as follows: First, note that α^2 is two disjoint 2-cycles, while β is a 4-cycle that "disrupts" the symmetry/order of powers of α. In particular, by disrupting α^2 with β, we will result in a smaller cycle, where our goal is to obtain a 2-cycle. We compute $\beta\alpha^2 = (2\ 3)$. Secondly, recall the process of conjugation. Conujugating a 2-cycle by a permutation sends the elements of the 2-cycle to the corresponding integer in the permutation, i.e., $\alpha(i\ j)\alpha^{-1} = (\alpha(i)\ \alpha(j))$, where this is verified because $(\alpha(i, j)\alpha^{-1})(x)$ for some $x \ne i$ nor j is just the identity map. Our goal is to get $(1\ 2)$, so we need to conjugate $(2\ 3)$ by some permutation such that 2 is sent to 1, and 3 is sent to 2. Observe that the permutation that does this is $\alpha^{-1} = \alpha^3$, so that $\alpha^3(2\ 3)\alpha = (1\ 2)$, i.e., $\alpha^3\beta\alpha^2\alpha = \alpha^3\beta\alpha^3 = (1\ 2)$. Then $(1\ 2) \in \langle \alpha, \beta \rangle$ so that by the previous exercise, A has a subgroup of order 8, hence $|A| = 24$. Then $A = S_4$.   □

(9) Prove that $\mathrm{SL}_2(\mathbb{F}_3)$ is the subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. [Recall from Exercise 9 of Section 1 that $\mathrm{SL}_2(\mathbb{F}_3)$ is the subgroup of matrices of determinant 1 You may assume this subgroup has order 24—this will be an exercise in Section 3.2.]

Solution. Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Since we know that $\mathrm{SL}_2(\mathbb{F}_3)$ has order 24, we need to exhibit at least 13 distinct matrices using A and B, since $\langle A, B \rangle$ divides 24. Since I, A, and B are 3 distinct matrices, we compute 10 more:

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad\qquad B^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

$$AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \qquad\qquad BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

$$(AB)^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \qquad\qquad ABA^2 = \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}$$

$$A^2 B = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix} \qquad\qquad B^2 A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$$

$$ABA = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad\qquad BAB = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Hence $\langle A, B \rangle = 24$ so that $\langle A, B \rangle = \mathrm{SL}_2(\mathbb{F}_3)$. $\qquad\qquad\qquad\square$

(10) Prove that the subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is isomorphic to the quaternion group of order 8. [Use a presentation for Q_8.]

Solution. Let

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Doing some calculations, we see that $A^2 = B^2 = -I$. Moreover, letting $C = AB$, we also see that $C^2 = ABC = -I$. Moreover, I and $-I$ commute with A, B, and C. Since this satisfies the presentation given in Section 1.5, Exercise 3, then there is a surjective homomorphism $\varphi : Q_8 \to \langle A, B \rangle$ given by

$$\varphi(i) = A, \quad \varphi(j) = B, \quad \varphi(k) = AB$$

Moreover, $|\langle A, B \rangle| \le 8$ since $|Q_8| = 8$, and $|Q_8| = |\langle A, B \rangle|$ because $I, -I, A, B, C \in \langle A, B \rangle$ are all distinct so that φ is injective. Then $Q_8 \cong \langle A, B \rangle$. $\qquad\qquad\qquad\square$

(11) Show that $\mathrm{SL}_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.

Solution. Recall that Q_8 and S_4 both have 6 elements of order 4. However, no two elements in Q_8 can generate the entirety of $\mathrm{SL}_2(\mathbb{F}_3)$ since $|Q_8| = 8$, while $S_4 = \langle (1\,2\,3\,4), (1\,2\,4\,3) \rangle$, hence they cannot be isomorphic. $\qquad\square$

(12) Prove that the subgroup of upper triangular matrices in $\mathrm{GL}_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8. (First find the order of this subgroup.)

Solution. Let $\mathrm{UT}_3(\mathbb{F}_2)$ denote the given subgroup. Moreover, refer to each matrix in $\mathrm{UT}_3(\mathbb{F}_2)$ as (a, b, c), where these are the entries above the diagonals of 1 in the matrix (each entry on the diagonal must be 1, for otherwise we would have 0 which would mean determinant of 0, hence uninvertible). Since each of a, b, c can be 0 or 1, then there are $2^3 = 8$ elements in $\mathrm{UT}_3(\mathbb{F}_2)$.

For a matrix $A = (a, b, c) \in \mathrm{UT}_3(\mathbb{F}_2)$ to be mapped to $r \in D_8$, it must be that $A^4 = I$. Note that $A^2 = (2a, ac + 2b, 2c) = (0, ac, 0)$ so that $A^4 = (0, 2ac, 0) = I$. We must then choose a, c such that they are not 0 mod 2 after being multiplied once; the choice is $a = c = 1$, while b can be anything, so set $A = (1, 0, 1)$. Moreover, for $B = (d, e, f) \in \mathrm{UT}_3(\mathbb{F}_2)$ to map to s, it must be that $AB = BA^{-1} = BA^3$, or $(1, 0, 1)(d, e, f) = (d, e, f)(1, 1, 1)$. We find that

$$(1, 0, 1)(d, e, f) = (1 + d, e + f, 1 + f) = (1 + d, 1 + d + e, 1 + f) = (d, e, f)(1, 1, 1)$$

The only relevant equality is $e + f = 1 + d + e$, which implies $f = 1 + d$. Then d and f must be different, while e can be any element, so put $B = (1, 0, 0)$. Since $A^4 = B^2 = I$, then we have a homomorphism $\varphi : D_8 \to \mathrm{UT}_3(\mathbb{F}_2)$ given by

$$\varphi(r) = A, \quad \varphi(s) = B$$

It is easy to see that none of A, A^2, A^3 are distinct nor is equal to B, so $B \notin \langle A \rangle$ and $|\langle A \rangle| = 4$. Then $\langle A, B \rangle = \mathrm{UT}_3(\mathbb{F}_2)$ so that φ is surjective. Moreover, $|\langle A, B \rangle| = |D_8|$, hence φ is injective. Then $D_8 \cong \mathrm{UT}_3(\mathbb{F}_2)$. $\square$

(13) Prove that the multiplicative group of positive rational numbers is generated by the set $\{1/p \mid p \text{ is prime}\}$.

Solution. Let P denote the set in question. Note that for any $1/p \in P$, then $(1/p)^{-1} = p \in P$, and any powers are also in P. Take any $m, n \in \mathbb{Q}$ such that $(m, n) = 1$. Using the Fundamental Theorem of Arithmetic, m and n have prime factorizations so they can be written as a product of primes. Then $m/n \in \langle P \rangle$, so $\langle P \rangle = \mathbb{Q}^+$. $\square$

(14) A group H is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.
   (a) Prove that every finite group is finitely generated.
   (b) Prove that $\mathbb{Z}$ is finitely generated.
   (c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \le \langle 1/k \rangle$, where k is the product of all denominators appearing in a set of generators for H.]
   (d) Prove that $\mathbb{Q}$ is not finitely generated.

Solution.
   (a) Any finite group G is generated by $\langle G \rangle$.
   (b) $\mathbb{Z} = \langle 1 \rangle$.
   (c) Let $H = \langle A \rangle$, where
   $$A = \left\{ \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_n}{q_n} \right\}$$
   where $(p_i, q_i) = 1$ for all $1 \le i \le n$. Then every element $h \in H$ is of the form
   $$h = \sum_{i=1}^{n} a_i \frac{p_i}{q_i}, \quad a_i \in \mathbb{Z}$$
   since $\mathbb{Q}$ is abelian. Define the quantities
   $$k = \prod_{i=1}^{n} q_i, \quad k_j = k/q_j$$
   so that k is the product of all denominators in A, and k_j is the product of all denominators except the denominator in the j-th fraction of A. We may then rewrite h as
   $$h = \frac{1}{k} \sum_{i=1}^{n} a_i p_i k_i$$
   so that $h \in \langle 1/k \rangle$, which is a cyclic subgroup of $\mathbb{Q}$. Then $H \le \langle 1/k \rangle$, hence it is cyclic.
   (d) Suppose $\mathbb{Q}$ was finitely generated. Then $\mathbb{Q} = \langle p/q \rangle$ where $(p, q) = 1$, by the previous part. Let $r \in \mathbb{Z}$ such that r does not divide q. Then there is some $n \in \mathbb{Z}$ such that
   $$n \frac{p}{q} = \frac{1}{r}$$
   Then $q = npr$, contradicting that r doesn't divide q. $\square$

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

Solution. By the previous exercise, such a subgroup cannot be finitely generated. Consider the set
$$A = \left\{ \frac{1}{2^k} \,\middle|\, k \in \mathbb{Z}^+ \cup \{0\} \right\}$$
where $\langle A \rangle \le \mathbb{Q}$. Note that $\langle A \rangle < \mathbb{Q}$ since $1/3 \notin \langle A \rangle$. Moreover, if $\langle A \rangle = \langle p/q \rangle$, then $q = 2^m$ since every element of A has a power of 2. Then $2^{m+1} \notin \langle p/q \rangle$, but $2^{m+1} \in \langle A \rangle$, hence $\langle A \rangle$ cannot be cyclic. $\square$

(16) A subgroup M of a group G is called a *maximal subgroup* if $M \neq G$ and the only subgroups of G which contain M are M and G.

  (a) Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.

  (b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.

  (c) Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup H is maximal if and only if $H = \langle x^p \rangle$ for some prime p dividing n.

  Solution.

  (a) If H is maximal, then we are done. If not, there exists a subgroup $H_1 < G$ such that $H < H_1$. If H_1 is maximal, we are done, but if not, then there must be another subgroup such that $H_1 < H_2$. Continuing on, we can create a chain of subgroups H_i such that $H_i < H_{i+1}$. Since G is finite, the process of creating subgroups must terminate at some k. Then $H_k < G$ is a maximal subgroup that contains H.

  (b) Note that $s \notin \langle r \rangle$ so that $\langle r \rangle$ is a proper subgroup of D_{2n}. If $\langle r \rangle$ was not maximal, there must exist some H such that $\langle r \rangle < H$ so that some reflection $sr^k \in H$ for some $1 \leq k < n$. Note that $r^{n-k} \in H$ so that $sr^k r^{n-k} = s \in H$. But then $H = D_{2n}$, contradicting that $H < D_{2n}$. It must be that $\langle r \rangle$ is maximal.

  (c) Suppose H is maximal, and put $H = \langle x^k \rangle$ and $d = (n, k)$. Note that $d > 1$ for the subgroup to be proper. Let p be a prime that divides n. If $k = p$, then we are done. If $k \neq p$, consider $\langle x^p \rangle$. Then $H < \langle x^p \rangle$ since $p \mid d$. Since H is maximal, then $\langle x^p \rangle = G$. Then $(p, n) = 1$, but this contradicts that $p \mid n$. Then $k = p$.

  Suppose that $H = \langle x^p \rangle$ for prime $p \mid n$. If H is not maximal, there exists $\langle x^d \rangle$ such that $d \mid p$. Since p is prime, then either $d = 1$ or p. If $d = 1$, then $\langle x^d \rangle = G$ which shows that $\langle x^d \rangle$ is not a proper subgroup of G. If $d = p$, then $\langle x^d \rangle = \langle x^p \rangle$ so that H is not a proper subgroup of $\langle x^d \rangle$. It follows that H is maximal. $\square$

(17) This is an exercise involving Zorn's Lemma. Prove that every nontrivial finitely generated group possesses maximal subgroups. Let G be a finitely generated group, say $G = \langle g_1, g_2, \ldots, g_n \rangle$, and let $\mathscr{S}$ be the set of all proper subgroups of G. Then $\mathscr{S}$ is partially ordered by inclusion. Let $\mathscr{C}$ be a chain in $\mathscr{S}$.

  (a) Prove that the union H of all the subgroups in $\mathscr{C}$ is a subgroup of G.

  (b) Prove that H is a proper subgroup.

  (c) Use Zorn's Lemma to show that $\mathscr{S}$ has a maximal element (which is, by definition, a maximal subgroup).

  Solution.

  (a) Let $\mathscr{C} \subseteq \mathscr{S}$ be a chain. Put
  $$H = \bigcup_{K \in \mathscr{C}} K$$
  Since at least one subgroup is in $\mathscr{C}$ and subgroups are nonempty, then $\mathscr{C}$ is nonempty. Suppose $g, h \in H$. Then $g \in K_1$ and $h \in K_2$ for some $K_1, K_2 \in \mathscr{C}$ such that $K_1 \leq K_2$ or $K_2 \leq K_1$, or both. Without loss of generality, suppose $K_1 \leq K_2$. Then $g \in K_2$ as well so that $gh^{-1} \in K_2 \subseteq H$. Then $H \leq G$.

  (b) If H was not a proper subgroup, then H must contain all generators g_i. Associate each generator with a (not necessarily distinct) subgroup K_i so that $g_i \in K_i$ for every $1 \leq i \leq n$. Since $\mathscr{C}$ is a chain, then we may order the subgroups such that $K_j \leq K_{j+1}$ for all $1 \leq j \leq n-1$. It follows that K_n contains every generator g_i so that $K_n = G$, contradicting that $\mathscr{C}$ is a chain of proper subgroups of G.

  (c) Because G is nontrivial, then $\{1\} \in \mathscr{S}$ so that $\mathscr{S}$ is nonempty. Moreover, $H \in \mathscr{S}$ by the previous part, and for any $K \in \mathscr{C}$, we have $K \leq H$ so that H is an upper bound for $\mathscr{C}$. Then every chain in $\mathscr{S}$ has an upper bound, so by Zorn's Lemma, $\mathscr{S}$ must have a maximal element. $\square$

(18) Let p be a prime and let $Z = \{z \in \mathbb{C} \mid z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}^+\}$ (so Z is the multiplicative group of all p-power roots of unity in $\mathbb{C}$). For each $k \in \mathbb{Z}^+$ let $H_k = \{z \in Z \mid z^{p^k} = 1\}$ (the group of p^kth roots of unity). Prove:

  (a) $H_k \leq H_m$ if and only if $k \leq m$.

  (b) H_k is cyclic for all k.

  (c) Every proper subgroup of Z equals H_k for some k. In particular, every proper subgroup of Z is finite and cyclic.

  (d) Z is not finitely generated.

Solution.

(a) Note that $|H_k| = p^k$ for any k as there are exactly p^k roots of unity. Now, if $H_k \leq H_m$, then $p^k \mid p^m$ by Lagrange's Theorem. Then $p^k \leq p^m$, or $k \leq m$ since $p > 0$.

If $k \leq m$, then $p^k \leq p^m$. In particular, $p^k \mid p^m$. Then for any $z \in H_k$, we have

$$z^{p^m} = (z^{p^k})^{p^{m-k}} = 1$$

so that $z \in H_m$. Then $H_k \leq H_m$.

(b) Let $\theta = e^{2\pi i/p^k}$. Note that $\langle \theta \rangle$ has order p^k, and $\langle \theta \rangle \subseteq H_k$. Now for some $z \in H_k$, we have $z = e^{2\pi i x/p^k}$ for some $0 \leq x < p^k$. Then $z = (e^{2\pi i/p^k})^x \in \langle \theta \rangle$ so that $\langle \theta \rangle = H_k$.

(c) Let H be a proper subgroup of Z. Note that every element in Z has order p^i for some $i \in \mathbb{Z}^+$, so elements of H will have similar orders. Define the set

$$S = \{n \in \mathbb{Z}^+ \mid |h| = p^n \text{ for some } h \in H\}$$

so that S is the set of integers n such that H contains a p^n–th root of unity. Moreover, H is trivially nonempty if we define $H_0 = \{z \in Z \mid z^{p^0} = z = 1\}$ so that the trivial proper subgroup $\{1\}$ of Z allows $1 \in H$.

Suppose now that S is infinite. For any $n \in \mathbb{Z}^+$, there exists $h \in H$ and $m \in \mathbb{Z}^+$ such that $|h| = p^m > p^n$, for otherwise it would be that every $h \in H$ has order $|h| \leq p^n$, meaning that n is an upper bound for S. Then $|h| = p^m$ so that $H_m = \langle h \rangle$, and $H_m \leq H$. Since $H_n \leq H_m$ for every $n \in \mathbb{Z}^+$, then

$$Z = \bigcup_{n \in \mathbb{Z}^+} H_n \subseteq H$$

which shows $Z \leq H$. But $H \leq Z$, hence $Z = H$, which contradicts that $Z = H$. It must be that S is finite, so it has some maximal element s. Because $s \in S$, then there is $h_0 \in H$ where $|h_0| = p^s$ so that $H_s = \langle h_0 \rangle \leq H$. Suppose $h \in H$ with $|h| = p^k$ for some $k \in \mathbb{Z}^+$. Then $k \in S$ where $k \leq s$ so that $H_k \leq H_s$. Since $h \in H_k$, then $h \in H_s$ so $H \leq H_s$. Hence, $H = H_s$.

(d) Put $Z = \langle z_1, z_2, \ldots, z_n \rangle$ for some $n \in \mathbb{Z}^+$ such that $|z_i| = p^{x_i}$. Let $x = \max(x_1, x_2, \ldots, x_n)$. Then $z_i \in H_x$ for every $1 \leq i \leq n$ so that $Z \leq H_x$. But recall that Z comprises every p-power roots of unity so that $H_x \leq H_x$, contradicting part (a). It must be that Z is infinitely generated. $\square$

(19) A nontrivial abelian group A (written multiplicatively) is called *divisible* if for each element $a \in A$ and each nonzero integer k there is an element $x \in A$ such that $x^k = a$.

  (a) Prove that the additive group of rational numbers $\mathbb{Q}$ is divisible.

  (b) Prove that no finite abelian group is divisible.

Solution.

  (a) Suppose $p/q \in \mathbb{Q}$. Then $(p/qn)n = p/q$, where $p/qn \in \mathbb{Q}$.

  (b) Suppose we have a finite abelian group G with $|G| = n$. Pick some nonidentity $g \in G$. Then there is no such $h \in$ where $h^n = g$, since $h^n = 1$. $\square$

(20) Prove that if A and B are nontrivial abelian groups, then $A \times B$ is divisible if and only if both A and B are divisible.

Solution. Suppose $A \times B$ is divisible, and let $a \in A$, $b \in B$, and $k \in \mathbb{Z}^+$. Then there exists $(c, d) \in A \times B$ such that $(c, d)^k = (c^k, d^k) = (a, b)$. But then $c^k = a$ and $d^k = b$ so that A and B are divisible.
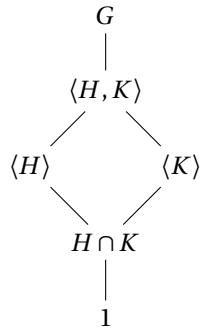
If A and B are both divisible, pick $(a, b) \in A \times B$ and let $k \in \mathbb{Z}^+$. Then there exists $c \in A$ and $d \in B$ such that $c^k = a$ and $d^k = b$. Then $(c, d)^k = (c^k, d^k) = (a, b)$ so that $A \times B$ is divisible. $\square$

2.5   The Lattice of Subgroups of a Group
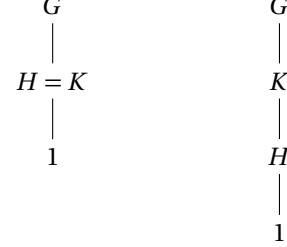
(1) Let H and K be subgroups of G. Exhibit all possible sublattices which show only $G, 1, H, K$ and their joins and intersections. What distinguishes the different drawings?

Solution.

If H and K are distinct with nontrivial intersection and properly contained in their join, then we have the following lattice:

$$
\begin{array}{c}
G \\
| \\
\langle H, K \rangle \\
\diagup \quad \diagdown \\
\langle H \rangle \qquad \langle K \rangle \\
\diagdown \quad \diagup \\
H \cap K \\
| \\
1
\end{array}
$$

Remaining scenarios include if $H = K$ or if $H \leq K$ (or the other way), in which case $\langle H, K \rangle = H \cap K$ or $\langle H, K \rangle = H$ and $H \cap K = K$ respectively:

$$
\begin{array}{ccc}
G & \qquad & G \\
| & & | \\
H = K & & K \\
| & & | \\
1 & & H \\
& & | \\
& & 1
\end{array}
$$

In further scenarios, we may have that some of the groups are trivial.   □

(2) In each of (a) to (d) list all subgroups of D_{16} that satisfy the given condition.

  (a) Subgroups that are contained in $\langle sr^2, r^4 \rangle$
  (b) Subgroups that are contained in $\langle sr^7, r^4 \rangle$
  (c) Subgroups that contain $\langle r^4 \rangle$
  (d) Subgroups that contain $\langle s \rangle$.

Solution.

  (a) $\langle sr^2, r^4 \rangle, \langle sr^6 \rangle, \langle sr^2 \rangle, \langle r^4 \rangle, 1$.
  (b) Note $sr^7 = sr^3$, so $\langle sr^3, r^4 \rangle, \langle r^4 \rangle, \langle sr^3 \rangle, \langle sr^7 \rangle, 1$.
  (c) $\langle r^4 \rangle, \langle sr^2, r^4 \rangle, \langle s, r^4 \rangle, \langle r^2 \rangle, \langle sr^3, r^4 \rangle, \langle sr^5, r^4 \rangle, \langle s, r^2 \rangle, \langle r \rangle, \langle sr, r^2 \rangle, D_{16}$.
  (d) $\langle s \rangle, \langle s, r^4 \rangle, \langle s, r^2 \rangle, D_{16}$.   □

(3) Show that the subgroup $\langle s, r^2 \rangle$ of D_8 is isomorphic to V_4.

Solution. Note $V_4 = \{1, a, b, c\}$ and $\langle s, r^2 \rangle = \{1, s, r^2, sr^2\}$, and that both groups are abelian and of order 4. Define the mapping $\varphi : \langle s, r^2 \rangle \to V_4$ given by

$$
\varphi(1) = 1, \quad \varphi(s) = a, \quad \varphi(r^2) = b, \quad \varphi(sr^2) = c
$$

To check φ is a homomorphism, note that it is sufficient to check the squares of all elements and all pairs of elements:

$$
\begin{aligned}
\varphi(s^2) &= \varphi(1) = 1 = c^2 = \varphi(s)^2 \\
\varphi(sr^2) &= c = ab = \varphi(s)\varphi(r^2) \\
\varphi(r^4) &= \varphi(1) = 1 = b^2 = \varphi(r^2)^2 \\
\varphi(ssr^2) &= \varphi(r^2) = b = ac = \varphi(s)\varphi(sr^2) \\
\varphi((sr^2)^2) &= \varphi(1) = 1 = c^2 = \varphi(sr^2)^2 \\
\varphi(r^2 sr^2) &= \varphi(s) = a = bc = \varphi(r^2)\varphi(sr^2)
\end{aligned}
$$

so that φ is indeed a homomorphism. This is necessarily bijective so that $\langle s, r^2 \rangle \cong V_4$.   □

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

Solution. Note that $D_8 = \langle s, r \rangle$. Moreover, $s \neq rs$, and $r \in \langle s, rs \rangle$ so that $\langle s, rs \rangle = D_8$. Since $r = r^3$, we also have $\langle s, r^3 \rangle = D_8$. We may also replace the reflection s with sr^2, since combinations of a reflection with an odd rotation and a reflection with an even rotation contain r and thus generates D_8. It follows that the pairs of elements that generate D_8 are:

$$
\langle s, r \rangle, \langle s, r^3 \rangle, \langle s, rs \rangle, \langle s, r^3 s \rangle, \langle r^2 s, r \rangle, \langle r^2 s, r^3 \rangle, \langle r^2 s, rs \rangle, \langle r^2 s, r^3 s \rangle, \langle r, rs \rangle, \langle r^3, rs \rangle, \langle r, r^3 s \rangle, \langle r^3, r^3 s \rangle \quad □
$$

(5) Use the given lattice to find all elements $x \in D_{16}$ such that $D_{16} = \langle x, s \rangle$ (there are 8 such elements x).

Solution. Note that $\langle r \rangle = \langle r^3 \rangle = \langle r^5 \rangle = \langle r^7 \rangle$. We then pair each generator with an s so that we obtain just the rotation to then generate D_{16}: $x = r, r^3, r^5, r^7, sr, sr^3, sr^5, sr^7$. □

(6) Use the given lattices to help find the centralizers of every element in the following groups:

   (a) D_8
   (b) Q_8
   (c) S_3
   (d) D_{16}.

   Solution.

   (a) To calculate the centralizer of an element a, start with the cyclic subgroup that contains a and see if any other elements are contained in $\langle a \rangle$. For example, to calculate $C_{D_8}(rs)$, start with $\langle rs \rangle$ in the subgroup lattice. Since $r^4, sr^5 \in C_{D_8}(rs)$, then $C_{D_8}(rs) \leq \langle sr^5, r^4 \rangle$. Checking the next subgroup, it follows that $r^2 \in C_{D_8}(rs)$ so that $C_{D_8}(rs) \leq \langle rs, r^2 \rangle$. Since $r \notin C_{D_8}(rs)$, then $C_{D_8}(rs) \neq D_{16}$ so that $C_{D_8}(rs) = \langle rs, r^2 \rangle$. We use similar reasoning to deduce the other centralizers:

$$
\begin{aligned}
C_{D_8}(1) &= D_8 \\
C_{D_8}(r) &= \langle r \rangle \\
C_{D_8}(r^2) &= D_8 \\
C_{D_8}(r^3) &= \langle r \rangle \\
C_{D_8}(s) &= \langle s, r^2 \rangle \\
C_{D_8}(rs) &= \langle rs, r^2 \rangle \\
C_{D_8}(r^2 s) &= \langle s, r^2 \rangle \\
C_{D_8}(r^3 s) &= \langle sr, r^2 \rangle
\end{aligned}
$$

   (b) Note that $1, -1 \in Z(Q_8)$, while none of i, j, and k commute with anything but themselves. Then:

$$
\begin{aligned}
C_{Q_8}(1) &= C_{Q_8}(-1) = Q_8 \\
C_{Q_8}(i) &= C_{Q_8}(-i) = \langle i \rangle \\
C_{Q_8}(j) &= C_{Q_8}(-j) = \langle j \rangle \\
C_{Q_8}(k) &= C_{Q_8}(-k) = \langle k \rangle
\end{aligned}
$$

   (c) Since no element in S_3 commutes with each other, then $C_{S_3}(a) = \langle a \rangle$ for all $a \in S_3 - \{1\}$, where $C_{S_3}(1) = S_3$.
   (d) Use similar reasoning as in part (a) to obtain the centralizers:

$$
\begin{aligned}
C_{D_{16}}(1) &= C_{D_{16}}(r^4) = D_{16} \\
C_{D_{16}}(r^k) &= \langle r \rangle \text{ for all } k = 1, 2, 3, 5, , 6, \\
C_{D_{16}}(s) &= C_{D_{16}}(sr^4) = \langle s, r^4 \rangle \\
C_{D_{16}}(sr) &= C_{D_{16}}(sr^5) = \langle sr^5, r^4 \rangle \\
C_{D_{16}}(sr^2) &= C_{D_{16}}(sr^6) = \langle sr^2, r^4 \rangle \\
C_{D_{16}}(sr^3) &= C_{D_{16}}(sr^7) = \langle sr^3, r^4 \rangle
\end{aligned}
$$

□

(7) Find the center of D_{16}.

   Solution. $Z(D_{16}) = \{1, r^4\}$ by Section 2.2, Exercise 7. □

(8) In each of the following groups find the normalizer of each subgroup:

   (a) S_3
   (b) Q_8.

   Solution.

(a) Note that every subgroup of S_3 is maximal with the exception of the trivial subgroup, so it follows that $N_{S_3}(\langle \alpha \rangle) = \langle \alpha \rangle$ or S_3 for all $\alpha \in S_3 - \{1\}$. To that end, we have $N_{S_3}(1) = S_3$. Also, for $(1\ 2) \in S_3$, then $(1\ 3)(1\ 2)(1\ 3) \neq (1\ 2)$ so that $(1\ 3) \notin N_{S_3}(\langle (1\ 2) \rangle)$. Then $N_{S_3}(\langle (1\ 2) \rangle) = \langle (1\ 2) \rangle$. Using similar reasoning with the two other 2-cycles, we conclude that $N_{S_3}(\langle \alpha \rangle) = \langle \alpha \rangle$ when α is a 2-cycle. For $\langle (1\ 2\ 3) \rangle$, note that

$$(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2), \quad (1\ 2)(1\ 3\ 2)(1\ 2) = (1\ 2\ 3)$$

so that $(1\ 2) \in N_{S_3}(\langle (1\ 2\ 3) \rangle)$, hence $N_{S_3}(\langle (1\ 2\ 3) \rangle) = S_3$.

(b) Like S_3, the subgroups of Q_8 are maximal except for $\langle -1 \rangle$ and the trivial subgroup, so $N_{Q_8}(1) = N_{Q_8}(-1) = Q_8$ since $-1 \in Z(Q_8)$. Taking i, we see that

$$j\,i(-j) = (-k)(-j) = -i, \quad k\,i(-k) = (-j)(-k) = i$$
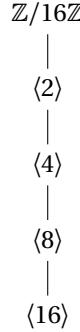
so that $j, k \in N_{Q_8}(\langle i \rangle)$. Then $N_{Q_8}(\langle i \rangle) = Q_8$. We deduce similarly that $N_{Q_8}(\langle j \rangle) = N_{Q_8}(\langle k \rangle) = Q_8$. $\square$

(9) Draw the lattices of subgroups of the following groups:
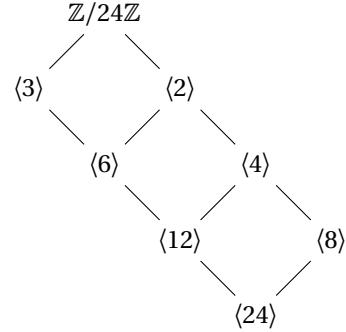
   (a) $\mathbb{Z}/16\mathbb{Z}$

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

   (c) $\mathbb{Z}/48\mathbb{Z}$.

Solution.
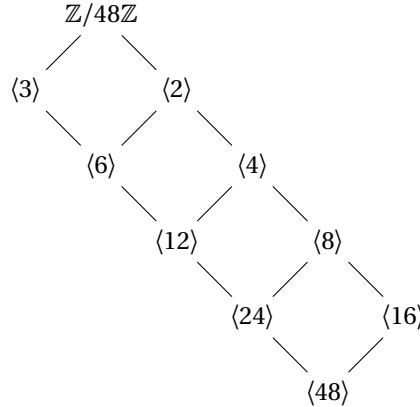
   (a) $\mathbb{Z}/16\mathbb{Z}$ (b) $\mathbb{Z}/24\mathbb{Z}$

   (c) $\mathbb{Z}/48\mathbb{Z}$

                                                                                                          $\square$

(10) Classify groups of order 4 by proving that if $|G| = 4$, then $G \cong Z_4$ or $G \cong V_4$. [See Section 1.1, Exercise 36]
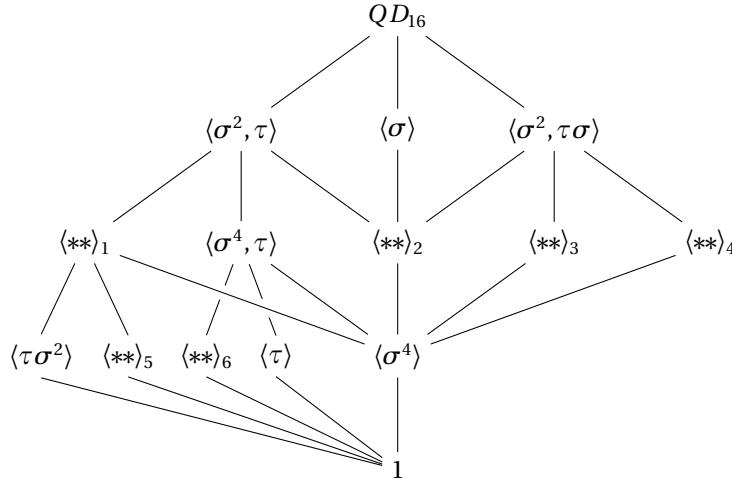
   Solution. Let $G = \{1, g, h, k\}$. Certainly, $G \cong Z_4$ if G contains an element of order 4 (so is then cyclic), since **??** says that cyclic groups of the same order are isomorphic. Suppose that G is not cyclic. It must be that

$|g| = |h| = |k| = 2$. If $gh = 1$, then $h = g$ so that g and h are not distinct. If $gh = g$ or h, we may cancel to deduce either $h = 1$ or $g = 1$ respectively, contradicting the order of G. Hence, $gh = k$. We may use similar reasoning to deduce that $gk = h$ and $hk = g$ so that $G \cong V_4$. $\qquad\qquad\square$

(11)   Consider the group of order 16 with the following presentation:

$$QD_{16} = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$
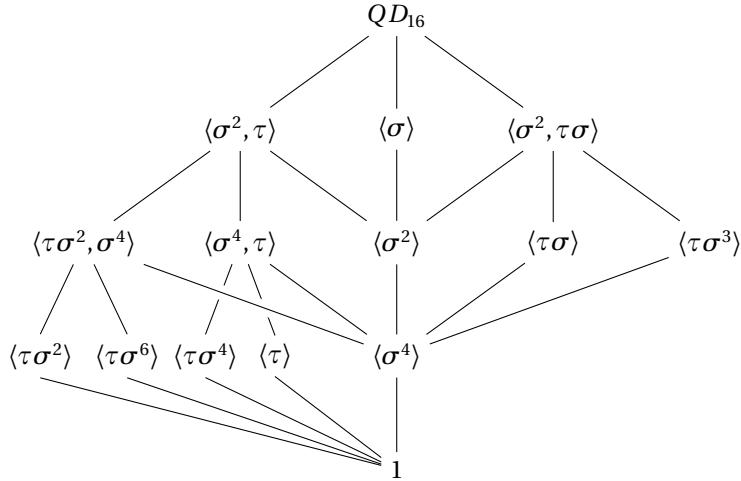
(called the *quasidihedral* or *semidihedral* group of order 16). This group has three subgroups of order 8: $\langle \tau, \sigma^2 \rangle \cong D_8, \langle \sigma \rangle \cong Z_8$, and $\langle \sigma^2, \sigma\tau \rangle \cong Q_8$, and every proper subgroup is contained in one of these three subgroups. Fill in the missing subgroups in the lattice of all subgroups of the quasidihedral group, exhibiting each subgroup with at most two generators.

Solution. Note that the above has been assigned subscripts to the unknown subgroups so that we may refer to them by name in the solution. To that end, note that 2 is $\langle \sigma^2 \rangle$. To fill in the rest, we examine the cyclic subgroups for the rest of the elements. Since the structure of the subgroups generated by σ^k are clear, we must then look to elements of the form $\tau\sigma^k$. We have

$$\langle \tau\sigma \rangle = \{1, \tau\sigma, \sigma^4, \tau\sigma^5\}$$
$$\langle \tau\sigma^3 \rangle = \{1, \tau\sigma^3, \sigma^4, \tau\sigma^7\}$$
$$\langle \tau\sigma^4 \rangle = \{1, \tau\sigma^4\}$$
$$\langle \tau\sigma^6 \rangle = \{1, \tau\sigma^6\}$$

It becomes clear that 6 must be $\langle \tau\sigma^4 \rangle$, since the subgroup above contains both τ and σ^4. 3 and 4 must be $\langle \tau\sigma \rangle$ and $\langle \tau\sigma^3 \rangle$ respectively, since $\langle \sigma^2, \tau\sigma \rangle$ both contain $\tau\sigma$ and σ^2 which multiply to $\tau\sigma^3$. Certainly, 1 cannot be $\langle \tau\sigma^6 \rangle$ as it does not contain $\langle \tau\sigma^2 \rangle$, so it must be 5. Then 1 must be $\langle \tau\sigma^2, \sigma^4 \rangle$ as it contains both subgroups. Hence, the completed diagram is

$$QD_{16}$$

The diagram shows the lattice of subgroups of QD_{16}, with top element QD_{16}, maximal subgroups $\langle \sigma^2, \tau \rangle$, $\langle \sigma \rangle$, $\langle \sigma^2, \tau\sigma \rangle$; next level $\langle \tau\sigma^2, \sigma^4 \rangle$, $\langle \sigma^4, \tau \rangle$, $\langle \sigma^2 \rangle$, $\langle \tau\sigma \rangle$, $\langle \tau\sigma^3 \rangle$; then $\langle \tau\sigma^2 \rangle$, $\langle \tau\sigma^6 \rangle$, $\langle \tau\sigma^4 \rangle$, $\langle \tau \rangle$, $\langle \sigma^4 \rangle$; and bottom element 1.

□
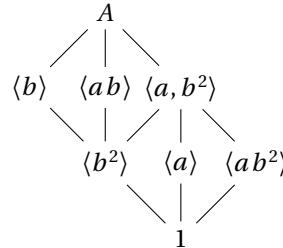
The next three examples lead to two nonisomorphic groups that have the same lattice of subgroups.

(12) The group $A = Z_2 \times Z_4 = \langle a, b \mid a^2 = b^4 = 1, ab = ba \rangle$ has order 8 and has three subgroups of order 4: $\langle a, b^2 \rangle \cong V_4, \langle b \rangle \cong Z_4$, and $\langle ab \rangle \cong Z_4$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of A, giving each subgroup in terms of at most two generators.

Solution. First, A is abelian, so we may write out the elements of A as

$$A = \{1, b, b^2, b^3, a, ab, ab^2, ab^3\}$$
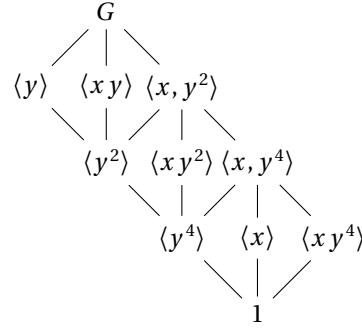
Moreover, we know that $\langle a, b^2 \rangle$ must have 3 subgroups of order 2, namely $\langle a \rangle, \langle b^2 \rangle$, and $\langle ab^2 \rangle$. $\langle b \rangle$ has one subgroup of order 2, $\langle b^2 \rangle$, and $\langle ab \rangle$ has one subgroup of order 2, $\langle b^2 \rangle$. We may then form the lattice:

The diagram shows the lattice of subgroups of A, with top element A; middle-upper level $\langle b \rangle$, $\langle ab \rangle$, $\langle a, b^2 \rangle$; middle-lower level $\langle b^2 \rangle$, $\langle a \rangle$, $\langle ab^2 \rangle$; and bottom element 1.

□

(13) The group $G = Z_2 \times Z_8 = \langle x, y \mid x^2 = y^8 = 1, xy = yx \rangle$ has order 16 and has three subgroups of order 8: $\langle x, y^2 \rangle \cong Z_2 \times Z_4, \langle y \rangle \cong Z_8$, and $\langle xy \rangle \cong Z_8$, and every proper subgroup is contained in one of those three. Draw the lattice of all subgroups of G, giving each subgroups in terms of at most two generators (cf. Exercise 12).

Solution. Using $a = x$ and $b = y^2$ in the previous exercise, the subgroup lattice of G contains a copy of the previous lattice as well as the maximal subgroups $\langle y \rangle$ and $\langle xy \rangle$. We then have the lattice

$$G$$

$$\langle y\rangle \quad \langle xy\rangle \ \langle x,y^2\rangle$$

$$\langle y^2\rangle \ \langle xy^2\rangle \ \langle x,y^4\rangle$$

$$\langle y^4\rangle \quad \langle x\rangle \quad \langle xy^4\rangle$$

$$1$$

$\square$

(14) Let M be the group of order 16 with the following presentation:
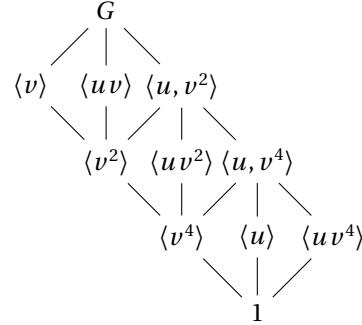
$$\langle u,v \mid u^2 = v^8 = 1, vu = uv^5\rangle$$

(sometimes called the *modular* group of order 16). It has three subgroups of order 8: $\langle u,v^2\rangle, \langle v\rangle$, and $\langle uv\rangle$, and every proper subgroup is contained in one of those three. Prove that $\langle u,v^2\rangle \cong Z_2 \times Z_4, \langle v\rangle \cong Z_8$, and $\langle uv\rangle \cong Z_8$. Show that the lattice of subgroups of M is the same as the lattice of subgroups of $Z_2 \times Z_8$ (cf. Exercise 13) but that these two groups are not isomorphic.

Solution. Using the presentation for $Z_2 \times Z_4$ in Exercise 12, note that $u^2 = (v^2)^4 = 1$, and $v^2 u = vuv^5 = uv^{10} = uv^2$, then $\langle u,v^2\rangle$ is an abelian subgroup of M, and the map $\varphi : Z_2 \times Z_4 \to \langle u,v^2\rangle$ defined by

$$\varphi(a) = u, \quad \varphi(b) = v^2$$

is a homomorphism. Moreover, φ is surjective by construction as $\langle u,v^2\rangle = \langle \varphi(a), \varphi(b)\rangle$. Since $|Z_2 \times Z_4| = |\langle u,v^2\rangle|$, then φ is bijective so that $Z_2 \times Z_4 \cong \langle u,v^2\rangle$. Now, $\langle v\rangle$ has order 8, and $\langle uv\rangle = \{1,, uv, uv^3, uv^5, uv^7, v^2, v^4, v^6\}$ so that $\langle uv\rangle$ also has order 8. Then $\langle v\rangle \cong Z_8$ and $\langle uv\rangle \cong 8$ since cyclic groups of the same order are isomorphic. Then the lattice of subgroups of M is the same as the lattice of $Z_2 \times Z_8$, where $x = u$ and $y = v$:

$$G$$

$$\langle v\rangle \quad \langle uv\rangle \ \langle u,v^2\rangle$$

$$\langle v^2\rangle \ \langle uv^2\rangle \ \langle u,v^4\rangle$$

$$\langle v^4\rangle \quad \langle u\rangle \quad \langle uv^4\rangle$$

$$1$$

Lastly, these two subgroups are not isomorphic since M is not abelian, but $Z_2 \times Z_8$ is: if it were, then $uv = vu$, but $vu = uv^5 = uv$ would imply that $v^4 = 1$, contradicting that $|v| = 8$. $\square$

(15) Describe the isomorphism type of each of the three subgroups of D_{16} of order 8.

Solution. Since $|r| = 8$, then $\langle r\rangle \cong Z_8$. For the remaining subgroups, note that the lattice for D_{16} shows a striking similarity to the lattice for D_8; in fact, these subgroups *are* isomorphic to D_8 as follows:
    For the subgroup $\langle s,r^2\rangle$, observe that $(r^2)4 = s^2 = 1$, and $sr^2 = r^6 s = (r^2)^{-1}s$. Then the mapping $\varphi : D_8 \to \langle s,r^2\rangle$ given by

$$\varphi(r) = r^2, \quad \varphi(s) = s$$

extends to a homomorphism. Moreover, this mapping is surjective by construction. Since $\langle s,r^2\rangle$ contains a subgroup of order 4 and is a subgroup of D_{16}, it must be 8 so that φ is an isomorphism, and $D_8 \cong \langle s,r^2\rangle$.

For the subgroup $\langle sr, r^2 \rangle$, we again observe that $(r^2)^4 = (sr)^2 = 1$, and $(sr)r^2 = sr^3 = r^5s = r^6r^7s = (r^2)^{-1}(sr)$. The mapping $\psi : D_8 \to \langle sr, r^2 \rangle$ given by

$$\varphi(r) = r^2, \varphi(s) = sr$$

extends to a homomorphism, surjective by construction, and is an isomorphism because $\langle sr, r^2 \rangle$ has order 8. Then $D_8 \cong \langle sr, r^2 \rangle$. □

(16) Use the lattice of subgroups of the quasidihedral of order 16 to show that every element of order 2 is contained in the proper subgroup $\langle \tau, \sigma^2 \rangle$ (cf. Exercise 11).

Solution. Every element of order 2 generates a cyclic subgroup of order 2. Using the lattice, $\langle \tau, \sigma^2 \rangle$ properly contains all cyclic subgroups, except $\langle \tau\sigma \rangle$ and $\langle \tau\sigma^3 \rangle$, both of which are order 4. Then $\langle \tau, \sigma^2 \rangle$ contains all cyclic subgroups of order 2, hence contain all elements of order 2. □

(17) Use the lattice of subgroups of the modular group M of order 16 to show that the set $\{x \in M \mid x^2 = 1\}$ is a subgroup of M isomorphic to the Klein 4-group (cf. Exercise 14).

Solution. Using the lattice in Exercise 14, we see that we have 3 candidates to be isomorphic to V_4, namely $\langle v^2 \rangle, \langle uv^2 \rangle$, and $\langle u, v^4 \rangle$. The first and second subgroups are cyclic, while $\langle u, v^4 \rangle = \{1, u, v^4, uv^4\}$. Since it is not generated by one element, each of these elements are of order 2, and $v^4u = v^3uv^5 = \cdots = uv^{20} = uv^4$ so that it is abelian, then $\langle u, v^4 \rangle \cong V_4$. □

(18) Use the lattice to help find the centralizer of every element of QD_{16} (cf. Exercise 11).

Solution. Note that $\sigma^4\tau = \sigma^3\tau\sigma^3 = \cdots = \tau\sigma^{12} = \tau\sigma^4$ so that $\sigma^4 \in Z(QD_{16})$ as σ^4 already commutes with powers of σ. Moreover, any power of σ does not commute with τ except for σ^4. The elements $\tau\sigma$ and $\tau\sigma^3$ do not commute with σ^2 as $(\tau\sigma)\sigma^2 = \tau\sigma^3 = \sigma\tau \neq \sigma^2(\tau\sigma) = \tau\sigma^2$, and $(\tau\sigma^3)\sigma^2 = \sigma^7\tau \neq \sigma^3\tau = \sigma^2(\tau\sigma^3)$. Next, $(\tau\sigma^2)\sigma^2 = \tau\sigma^4 \neq \tau = \sigma^2(\tau\sigma^2)$ so that σ^2 does not commute with $\tau\sigma^2$. Moreover, $(\tau\sigma^6)(\tau\sigma^2) = \tau\sigma^2\sigma^4\tau\sigma^2 = (\tau\sigma^2)(\tau\sigma^6)$ so that $\tau\sigma^2$ commutes with $\tau\sigma^6$, but $\sigma^2\tau\sigma^6 = \tau\sigma^4 \neq \tau = (\tau\sigma^6)\sigma^2$ so σ^2 does not commute with $\tau\sigma^6$. Lastly, $\sigma^2(\tau\sigma^4) = \tau\sigma^2 \neq (\tau\sigma^4)\sigma^2$, and $\sigma^2\tau = \tau\sigma^6 \neq \tau\sigma^2$ so that σ^2 does not commute with $\tau\sigma^4$ nor with τ. It follows that the centralizers of the elements of QD_{16} are

$$C_{QD_{16}}(1) = C_{QD_{16}}(\sigma^4) = QD_{16}$$
$$C_{QD_{16}}(\langle \sigma^k \rangle) = \langle \sigma \rangle \text{ for } k = 1, 2, 3, 5, 6, 7$$
$$C_{QD_{16}}(\langle \tau\sigma \rangle) = C_{QD_{16}}(\langle \tau\sigma^5 \rangle) = \langle \tau\sigma \rangle$$
$$C_{QD_{16}}(\langle \tau\sigma^3 \rangle) = C_{QD_{16}}(\langle \tau\sigma^7 \rangle) = \langle \tau\sigma^3 \rangle$$
$$C_{QD_{16}}(\langle \tau \rangle) = C_{QD_{16}}(\langle \tau\sigma^4 \rangle) = \langle \sigma^4, \tau \rangle$$
$$C_{QD_{16}}(\langle \tau\sigma^2 \rangle) = C_{QD_{16}}(\langle \tau\sigma^6 \rangle) = \langle \tau\sigma^2, \sigma^4 \rangle$$

□

(19) Use the lattice to help find $N_{D_{16}}(\langle s, r^4 \rangle)$.

Solution. Based on the placement of $\langle s, r^4 \rangle$, its normalizer may be itself, $\langle s, r^2 \rangle$, or D_{16}. Note that $\langle s, r^4 \rangle = \{1, s, r^4, sr^4\}$, and taking r^2 and $(r^2)^{-1} = r^6$, we have

$$r^2 \langle s, r^4 \rangle r^6 = \{1, sr^4, r^4, s\} = \langle s, r^4 \rangle$$

so that $r^2 \in N_{D_{16}}(\langle s, r^4 \rangle)$, and $\langle s, r^2 \rangle \leq N_{D_{16}}(\langle s, r^4 \rangle)$. Since $rsr^{-1} = r^2s \neq r$, then $r \notin N_{D_{16}}(\langle s, r^4 \rangle)$ so that $N_{D_{16}}(\langle s, r^4 \rangle) = \langle s, r^2 \rangle$. □

(20) Use the lattice of subgroups of QD_{16} (cf. Exercise 11) to help find the normalizers

   (a) $N_{QD_{16}}(\langle \tau\sigma \rangle)$
   (b) $N_{QD_{16}}(\langle \tau, \sigma^4 \rangle)$.

Solution.

(a) Note that $\langle \tau\sigma \rangle = \{1, \tau\sigma, \sigma^4, \tau\sigma^5\}$. Moreover, $(\sigma^2)^{-1} = \sigma^6$ so that

$$\sigma^2 \langle \tau\sigma \rangle \sigma^6 = \{1, \tau\sigma^4, \sigma^4, \tau\sigma\} = \langle \tau\sigma \rangle$$

and $\sigma(\tau\sigma)\sigma^7 = \tau\sigma^3 \neq \tau\sigma$ so that $\sigma \notin N_{QD_{16}}(\langle \tau\sigma \rangle)$ so that $N_{QD_{16}}(\langle \tau\sigma \rangle) = \langle \sigma^2, \tau\sigma \rangle$.

(b) $\langle \tau, \sigma^4 \rangle = \{1, \tau, \sigma^4, \tau\sigma^4\}$, and

$$z\sigma^2 \langle \tau, \sigma^4 \rangle \sigma^6 = \{1, \tau\sigma^4, \sigma^4, \tau\}$$

while $\sigma\tau\sigma^7 = \tau\sigma^2 \neq \tau$ so that $\sigma \notin N_{QD_{16}}(\langle \tau, \sigma^4 \rangle)$. Then $N_{QD_{16}}(\langle \tau, \sigma^4 \rangle) = \langle \sigma^2, \tau \rangle$.   □

3   Quotient Groups and Homomorphisms

3.1   Definitions and Examples

Let G and H be groups.

(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 $\ker(\varphi) \trianglelefteq G$.

Solution. Since $E \leq H$, then $1_H \in E$. Since $\varphi(1_G) = 1_H \in E$, then $1_G \in \varphi^{-1}(E)$ so that it is nonempty. Suppose $x, y \in \varphi^{-1}(E)$. Then $\varphi(x), \varphi(y) \in E$ so that $\varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1}) \in E$. Then $xy^{-1} \in \varphi^{-1}(E)$, hence $\varphi^{-1}(E) \leq G$.

If $E \trianglelefteq H$, then $heh^{-1} \in E$ for every $e \in E$ and $h \in H$. Let $x \in \varphi^{-1}(E)$ and $g \in G$. Note that $\varphi(g) \in H$. Then

$$\varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(gxg^{-1}) \in E$$

so that $gxg^{-1} \in \varphi^{-1}(E)$. Then $\varphi^{-1}(E) \trianglelefteq G$, and since $\ker(\varphi) = \varphi^{-1}(1_H)$, then $\ker(\varphi) \trianglelefteq G$ as well.   □

(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 $u \in X$ (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 $u^{-1}w \in Y$.]

Solution. To show that $v = u^{-1}w \in Y$, then

$$\varphi(v) = \varphi(u^{-1}w) = \varphi(u)^{-1}\varphi(w) = a^{-1}(ab) = b \in Y$$ □

(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.

Solution. Let $aB, a'B \in A/B$. Then

$$(aB)(a'B) = (aa')B = (a'a)B = (a'B)(aB)$$

so that A/B is abelian.

To produce an abelian quotient group from a non-abelian group, a good thought is to consider the centers of non-abelian groups. In this case, we may choose $G = D_8$ with $Z(D_8) = \langle r^2 \rangle \trianglelefteq D_8$. Since $D_8/\langle r^2 \rangle \cong V_4$, then the quotient group is abelian.   □

(4) Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

Solution. Note that $(gN)^0 = 1N = g^0 N$, and $(gN)^{-1} = g^{-1}N$ by **??**. It suffices to show that the relationship holds for $\alpha \in \mathbb{Z}^+$. To that end, note that $\alpha = 1$ holds. Supposing it holds for some α, then

$$(gN)^{\alpha+1} = (gN)^\alpha(gN) = (g^\alpha N)(gN) = g^{\alpha+1}N$$

so that the result is true by induction.   □

(5) Use the preceding exercise 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 integer 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.

Solution. Let $gN \in G/N$. If possible, let $n \in \mathbb{Z}^+$ be the smallest integer such that $g^n \in N$. Then $g^n N = (gN)^n = 1N$ so that $|gN| \leq n$. Moreover, if $m \in \mathbb{Z}^+$ is an integer such that $(gN)^m = 1N$, then $g^m N = 1N$ so that $g^m \in N$. By minimality of n, then $|gN| \geq n$ so that $|gN| = n$.

If there is no such n, then $g^k \notin N$ for every $k \in \mathbb{Z}^+$. Suppose for contradiction that gN has infinite order x. Then $(gN)^x = g^x N = 1N$, or that $g^x \in N$, contradicting our previous assumption. It follows that gN has infinite order. Moreover, let G be a nontrivial group with nonidentity $g \in G$. Noting that $G \trianglelefteq G$, then $gG \in G/N$ has order 1, but $|g| > 1$.   □

(6) Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x. Describe the fibers of φ and prove that φ is a homomorphism.

Solution. The fibers of φ are as follows: the positive reals map to 1, and the negative reals map to -1. Moreover, for any $x, y \in \mathbb{R}^\times$, then

$$\varphi(xy) = \frac{xy}{|xy|} = \frac{x}{|x|} \cdot \frac{y}{|y|} = \varphi(x)\varphi(y) \qquad\qquad \square$$

(7) Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernel and fibers of π geometrically.

Solution. Let $(x, y),(a, b) \in \mathbb{R}^2$. Then

$$
\begin{aligned}
\pi((x, y)+(a, b)) &= \pi((x + a, y + b)) \\
&= (x + a)+(y + b) \\
&= (x + y)+(a + b) \\
&= \pi((x, y))+\pi((a, b))
\end{aligned}
$$

so that π is a homomorphism. Moreover, for any $a \in \mathbb{R}$, then $\pi((a,0)) = a$ so that π is surjective. $\ker(\pi)$ is the diagonal line in $\mathbb{R}$ with equation $y = -x$, and the fiber $\varphi^{-1}(a)$ for any $a \in \mathbb{R}$ is the diagonal line $y = -x + a$, or just a vertical translation of the kernel. $\qquad\qquad \square$

(8) Let $\varphi : \mathbb{R}^\times \to \mathbb{R}^\times$ be the map sending x to the absolute value of x. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ.

Solution. Let $x, y \in \mathbb{R}^\times$. Then
$$\varphi(xy) = |xy| = |x||y| = \varphi(x)\pi(y)$$

so that φ is a homomorphism. Moreover, $\varphi(\pm a) = a$ for any $a \in \mathbb{R}^+$ so that $\mathrm{im}(\varphi)$ is the positive reals. $\ker(\varphi) = \{1, -1\}$ since no other real number has an absolute value of 1, and the fiber of φ over a is the pair of reals $\{a, -a\}$. $\qquad\qquad \square$

(9) Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ by $\varphi(a + bi) = a^2 + b^2$. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ geometrically (as subsets of the plane).

Solution. Let $a + bi, c + di \in \mathbb{C}^\times$. Then

$$
\begin{aligned}
\varphi((a + bi)(c + di)) &= \varphi((ac - bd)+(ad + bc)i) \\
&= (ac - bd)^2 +(ad + bc)^2 \\
&= a^2 c^2 - 2abcd + b^2 d^2 + a^2 d^2 + 2abcd + b^2 c^2 \\
&= c^2(a^2 + b^2)+d^2(a^2 + b^2) \\
&= (a^2 + b^2)(c^2 + d^2) \\
&= \varphi(a + bi)\varphi(c + di)
\end{aligned}
$$

and φ is a homomorphism. Note that $a^2 + b^2 > 0$ for any a, b where at least one of them is nonzero, so $\mathrm{im}(\varphi) \subseteq \mathbb{R}^+$. Also, $\varphi(\sqrt{a} + 0i) = a$ for any $a \in \mathbb{R}^+$, so $\mathrm{im}(\varphi) = \mathbb{R}^+$. $\ker(\varphi) = \{a + bi \in \mathbb{C}^\times \mid a^2 + b^2 = 1\}$ is simply the circle of radius 1, and the fiber of φ over some $a \in \mathbb{R}^\times$ is the circle with radius $\sqrt{a}$. $\qquad\qquad \square$

(10) Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\overline{a}) = \overline{a}$. 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 $\overline{a}$ has a different meaning in the domain and range of φ).

Solution. Suppose $\overline{a} = \overline{b}$ for $\overline{a}, \overline{b} \in \mathbb{Z}/8\mathbb{Z}$. Then $a = b + 8k$ for $k \in \mathbb{Z}$, and

$$\varphi(\overline{a}) = \overline{a} = \overline{b + 8k} = \overline{b + 4(2k)} = \overline{b} = \varphi(\overline{b})$$

Moreover, this is a homomorphism as

$$\varphi(\overline{a}+\overline{b}) = \varphi(\overline{a + b}) = \overline{a + b} = \overline{a}+\overline{b} = \varphi(\overline{a})+\varphi(\overline{b})$$

and is clearly surjective as $\varphi(\overline{a}) = \overline{a}$ for any $\overline{a} \in \mathbb{Z}/4\mathbb{Z}$. The fibers are the following, noting that $\ker(\varphi) = \varphi^{-1}(\overline{0})$:

$$\varphi^{-1}(\overline{0}) = \{\overline{0}, \overline{4}\}$$
$$\varphi^{-1}(\overline{1}) = \{\overline{1}, \overline{5}\}$$
$$\varphi^{-1}(\overline{2}) = \{\overline{2}, \overline{6}\}$$
$$\varphi^{-1}(\overline{3}) = \{\overline{3}, \overline{7}\}$$ $\square$

(11) Let F be a field and let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in F, ac \neq 0 \right\} \leq \mathrm{GL}_2(F)$$

(a) Prove that the map

$$\varphi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$$

is a surjective homomorphism from G onto $F^\times$ (recall that $F^\times$ is the multiplicative group of nonzero elements in F). Describe the fibers and kernel of φ.

(b) Prove that the map

$$\psi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

is a surjective homomorphism from G onto $F^\times \times F^\times$. Describe the fibers and kernel of ψ.

(c) Let

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in F \right\}$$

Prove that H is isomorphic to the additive group F.

Solution.

(a) Note that

$$\varphi \left(\begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix} \right) = a$$

so that φ is surjective. Moreover, for any $a, b, c, d, e, f \in F$ with $ac \neq 0$ and $df \neq 0$, we have

$$\varphi \left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} \right) = \varphi \left(\begin{pmatrix} ad & ae + bf \\ 0 & cf \end{pmatrix} \right) = ad = \varphi \left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) \varphi \left(\begin{pmatrix} d & e \\ 0 & f \end{pmatrix} \right)$$

and φ is then a homomorphism. The fiber of $a \in F^\times$ over φ is

$$\varphi^{-1}(a) = \left\{ \begin{pmatrix} a & s \\ 0 & t \end{pmatrix} \middle| s, t \in F, t \neq 0 \right\}$$

with $\ker(\varphi) = \varphi^{-1}(1)$.

(b) Showing that ψ is a surjective homomorphism is very similar to the previous part. The fiber of any $(a, c) \in F^\times \times F^\times$ is

$$\psi^{-1}((a, c)) = \left\{ \begin{pmatrix} a & s \\ 0 & c \end{pmatrix} \middle| s \in F \right\}$$

with $\ker(\psi) = \psi^{-1}((1, 1))$.

(c) Define the mapping $\pi : H \to F$ given by

$$\pi \left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right) = b$$

Then its inverse $\pi^{-1} : F \to H$ given by

$$\pi^{-1}(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$
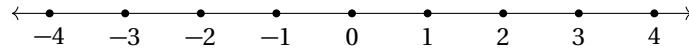
is a two-sided inverse of π so that π is a bijection. Moreover, for $b, c \in F$, then

$$\pi\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right) = \pi\left(\begin{pmatrix} 1 & b+c \\ 0 & 1 \end{pmatrix}\right) = b + c = \pi\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right) + \pi\left(\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right)$$

so that π is a homomorphism. Then π is an isomorphism, and $H \cong F$. □

(12) Let G be the additive group of real numbers, let H be the multiplicative 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 a 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.

Solution. Since $e^{2\pi i r} = 1$ if and only if r is an integer, then $\ker(\varphi) = \mathbb{Z}$. On a number line, this is shown as
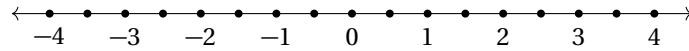

Moreover, note that $-1 = e^{-2\pi i/2}$ and $i = e^{2\pi i/4}$. Then the fibers of these elements are just the integral differences of $1/2, 1/4$, and $2/3$ respectively, since $4\pi i/3 = 2/3(2\pi i)$:

$$\varphi^{-1}(-1) = \frac{1}{2} + \mathbb{Z} = \left\{ \frac{1}{2} + n \;\middle|\; n \in \mathbb{Z} \right\}$$

$$\varphi^{-1}(i) = \frac{1}{4} + \mathbb{Z} = \left\{ \frac{1}{4} + n \;\middle|\; n \in \mathbb{Z} \right\}$$

$$\varphi^{-1}(e^{4\pi i/3}) = \frac{2}{3} + \mathbb{Z} = \left\{ \frac{2}{3} + n \;\middle|\; n \in \mathbb{Z} \right\}$$
□

(13) Repeat the preceding exercise with the map φ replaced by the map $\varphi : r \mapsto e^{4\pi i r}$.

Solution. The kernel of φ is $\frac{1}{2}\mathbb{Z}$, or

Moreover, the fibers are just all halved, so

$$\varphi^{-1}(-1) = \frac{1}{4} + \frac{1}{2}\mathbb{Z} = \left\{ \frac{1}{4} + \frac{n}{2} \;\middle|\; n \in \mathbb{Z} \right\}$$

$$\varphi^{-1}(-i) = \frac{1}{8} + \frac{1}{2}\mathbb{Z} = \left\{ \frac{1}{8} + \frac{n}{2} \;\middle|\; n \in \mathbb{Z} \right\}$$

$$\varphi^{-1}(e^{4\pi i/3}) = \frac{1}{3} + \frac{1}{2}\mathbb{Z} = \left\{ \frac{1}{3} + \frac{n}{2} \;\middle|\; n \in \mathbb{Z} \right\}$$
□

(14) Consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.

(a) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \le q < 1$.

(b) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elements of arbitrarily large order.

(c) Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$ (cf. Exercise 6, Section 2.1).

(d) Prove that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the multiplicative group of roots of unity in $\mathbb{C}^\times$.

Solution.

(a) Suppose $t \in \mathbb{Q}$, and put $t = a/b$ in lowest terms. Then there exists unique q, r such that $a = bq + r$, or that $t = q + r/b$, where $0 \le r < 1$. Then $t + \mathbb{Z} = q + r/b + \mathbb{Z} = r/b + \mathbb{Z}$. Since r is unique, then r/b is the representative of $t + \mathbb{Z}$ such that $0 \le r < 1$.

(b) Suppose $t = p/q \in \mathbb{Q}$. Then $|t + \mathbb{Z}| \le q$, since $q(t + \mathbb{Z}) = qt + \mathbb{Z} = \mathbb{Z}$ so that $t + \mathbb{Z}$ has finite order. Moreover, $1/k + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ has order k, but because $k \in \mathbb{Z}$ can be made arbitrarily large, then $1/k + \mathbb{Z}$ has arbitrarily large order.

(c) Note that $\mathbb{Q}/\mathbb{Z} \subseteq \text{Tor}(\mathbb{R}/\mathbb{Z})$ by the previous exercise, so it remains to show that cosets with irrational representatives do not have finite order. If $x + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ with finite order n, and $x \in \mathbb{R} - \mathbb{Q}$, then $n(x+\mathbb{Z}) = nx + \mathbb{Z} = \mathbb{Z}$ implies that $nx \in \mathbb{Z}$. But since $n \in \mathbb{Z}^{+}$, this implies that $x \in \mathbb{Z}$, contradicting that it was irrational. Hence, $\text{Tor}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.

(d) By Exercise 3.1.12, we have $\mathbb{R}/\mathbb{Z} \cong S^1$. Note that $\text{Tor}(S^1)$ consists of $z \in \mathbb{C}^{\times}$ such that $z^n = 1$, which is precisely the set of roots of unity. Since $\text{Tor}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$, then $\mathbb{Q}/\mathbb{Z}$ is isomorphic to the set of roots of unity. $\square$

(15) Prove that a quotient of a divisible abelian group by any proper subgroup is also divisible. Deduce that $\mathbb{Q}/\mathbb{Z}$ is divisible (cf. Exercise 19, Section 2.4).

Solution. Let A be a divisible abelian group, and let B be a proper subgroup of A. Pick $aB \in A/B$. Since A is divisible, there exists $x \in A$ such that $x^n = a$ for $x \in A$ and $n \in \mathbb{Z}$. Then $(xB)^n = x^n B = aB$ so that A/B is divisible. Since $\mathbb{Q}$ is divisible, and $\mathbb{Z} < \mathbb{Q}$ is proper, then $\mathbb{Q}/\mathbb{Z}$ is also divisible. $\square$

(16) Let G be a group, let N be a normal subgroup of G, and let $\overline{G} = G/N$. Prove that if $G = \langle x, y \rangle$ then $\overline{G} = \langle \overline{x}, \overline{y} \rangle$. Prove more generally that if $G = \langle S \rangle$ for any subset S of G, then $\overline{G} = \langle \overline{S} \rangle$.

Solution. If $G = \langle S \rangle$, then for every $g \in G$, we have

$$g = s_1 s_2 \dots s_n \quad \text{where } s_i \in S \text{ for } 1 \le i \le n$$

Let $\overline{S} = \{sN \mid s \in S\}$. Then for any $\overline{g} \in \overline{G}$, we have

$$gN = (s_1 s_2 \dots s_n)N = (s_1 N)(s_2 N) \dots (s_n N)$$

so that $\overline{g} \in \overline{S}$. Hence, $\overline{G} = \langle \overline{S} \rangle$. The case where $\overline{G} = \langle \overline{x}, \overline{y} \rangle$ is similar, where every element $g \in G$ is of the form $g = w(x, y)$, where $w(x, y)$ denotes a word in $\langle x, y \rangle$. $\square$

(17) Let G be the dihedral group of order 16 (whose lattice appears in Section 2.5): $G = \langle r, s \mid r^8 = s^2 = 1, \ rs = sr^{-1} \rangle$, and let $\overline{G} = G/\langle r^4 \rangle$ be the quotient of G by the subgroup generated by r^4 (this subgroup is the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.
(b) Exhibit each element of $\overline{G}$ in the form $\overline{s}^a \overline{r}^b$, for some integers a and b.
(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).
(d) Write each of the following elements of $\overline{G}$ in the form $\overline{s}^a \overline{r}^b$, for some integers a and b as in (b): $\overline{rs}$, $\overline{sr^{-2}s}$, $\overline{s^{-1}r^{-1}sr}$.
(e) Prove that $\overline{H} = \langle \overline{s}, \overline{r}^2 \rangle$ is a normal subgroup of $\overline{G}$ and $\overline{H}$ is isomorphic to the Klein 4-group. Describe the isomorphism type of the complete preimage of $\overline{H}$ in G.
(f) Find the center of $\overline{G}$ and describe the isomorphism type of $\overline{G}/Z(\overline{G})$.

Solution.

(a) Since $\langle r^4 \rangle = \{1, r^4\}$, each coset in $\overline{G}$ has 2 elements and partitions G into 8 sets. Hence, $|\overline{G}| = 8$.
(b) The elements of $\overline{G}$ are

$$\begin{aligned}
\overline{1} &= \{1, r^4\}, & \overline{s} &= \{s, sr^4\} \\
\overline{r} &= \{r, r^5\}, & \overline{sr} &= \{sr, sr^5\} \\
\overline{r}^2 &= \{r^2, r^6\}, & \overline{sr^2} &= \{sr^2, sr^6\} \\
\overline{r}^3 &= \{r^3, r^7\}, & \overline{sr^3} &= \{sr^3, sr^7\}
\end{aligned}$$

(c) The orders of the elements of $\overline{G}$ are

$\overline{x}$	$\overline{1}$	$\overline{r}$	$\overline{r}^2$	$\overline{r}^3$	$\overline{s}$	$\overline{sr}$	$\overline{sr^2}$	$\overline{sr^3}$
$|x|$	1	4	2	4	2	2	2	2

(d) $\overline{rs} = \overline{sr^3}, \overline{sr^{-2}s} = \overline{r}^2, \overline{s^{-1}r^{-1}sr} = \overline{r}^2$.

(e) We first note that $\overline{H} = \{1, \overline{r}^2, \overline{s}, \overline{s}\overline{r}^2\}$. To show that $\overline{H} \trianglelefteq \overline{G}$, we simplify the process by noting that elements of $\overline{G}$ are of the form $\overline{r}^k$ or $\overline{s}\overline{r}^k$. If an element is of the former, we have

$$\overline{r^k r^2 r^{-k}} = \overline{r}^2 \in \overline{H}$$
$$\overline{r^k s r^{-k}} = \overline{s(r^2)^{-k}} \in \overline{H}$$

If it is of the latter, then

$$\overline{(sr^k)r^2(r^{-k}s)} = \overline{r^{-2}} \in H$$
$$\overline{(sr^k)s(r^{-k}s)} = \overline{s(r^2)^k} \in H$$

where $\overline{sr^{k-1}} = \overline{r^{-k}s}$. The above calculations show that for every $\overline{g} \in \overline{G}$, then $\overline{g r^2 g^{-1}}, \overline{g s g^{-1}} \in H$ so that $\overline{gHg^{-1}} = \overline{H}$, hence $\overline{H} \trianglelefteq \overline{G}$. Moreover, it is easy to see that every element of $\overline{H}$ is of order 2 so that $\overline{H} \cong V_4$.

Let $\pi : G \to \overline{G}$ be the natural projection of G onto $\overline{G}$. Then $\pi^{-1}(\overline{H})$ is the complete preimage of $\overline{H}$, or the set of elements that map to a coset in $\overline{H}$. Using part (b), we see that

$$\pi^{-1}(\overline{H}) = \{1, r^2, r^4, r^6, s, sr^2, sr^4, sr^6\}$$

Note that $|\pi^{-1}(\overline{H})| = 8$, and the elements of $\overline{H}$ satisfy the relations $(r^2)^4 = s^2 = 1$. Then the mapping $\varphi : D_8 \to \pi^{-1}(\overline{H})$ given by $\varphi(r) = r^2$ and $\varphi(s) = s$ extends to a homomorphism that is clearly surjective. Then φ is an isomorphism, and $\pi^{-1}(\overline{H}) \cong D_8$.

(f) From the previous exercise, we have that $\overline{G} = \langle \overline{r}, \overline{s} \rangle$. Since $\overline{r}^2$ commutes with both $\overline{r}$ and $\overline{s}$, then $\overline{r}^2 \in Z(\overline{G})$. However, $\overline{r}\overline{s} \neq \overline{s}\overline{r}$ and $\overline{r}^3\overline{s} \neq \overline{s}\overline{r}^3$. Additionally, none of $\overline{s}\overline{r}, \overline{s}\overline{r}^2$, nor $\overline{s}\overline{r}^3$ commute with $\overline{r}$ so that $Z(\overline{G}) = \{\overline{1}, \overline{r}^2\}$. The elements of $\widehat{G} = \overline{G}/Z(\overline{G})$ are as follows:

$$\hat{1} = \{\overline{1}, \overline{r}^2\} \qquad\qquad \hat{s} = \{\overline{s}, \overline{s}\overline{r}^2\}$$
$$\hat{r} = \{\overline{r}, \overline{r}^3\} \qquad\qquad \widehat{sr} = \{\overline{s}\overline{r}, \overline{s}\overline{r}^3\}$$

One can see that each nonidentity element of $\widehat{G}$ has order 2 so that $\widehat{G} \cong V_4$. $\square$

(18) Let G be the quasidihedral group of order 16 (whose lattice was computed in Exercise 11 of Section 2.5): $G = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \ \sigma\tau = \tau\sigma^3 \rangle$, and let $\overline{G} = G/\langle \sigma^4 \rangle$ be the quotient of G by the subgroup generated by σ^4 (this subgroup is the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.
(b) Exhibit each element of $\overline{G}$ in the form $\overline{\tau}^a \overline{\sigma}^b$, for some integers a and b.
(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).
(d) Write each of the following elements of $\overline{G}$ in the form $\overline{\tau}^a \overline{\sigma}^b$, for some integers a and b as in (b): $\overline{\sigma\tau}$, $\overline{\tau\sigma^{-2}\tau}$, $\overline{\tau^{-1}\sigma^{-1}\tau\sigma}$.
(e) Prove that $\overline{G} \cong D_8$.

Solution.

(a) $\langle \sigma^4 \rangle$ has 2 elements, so each coset has 2 elements which subsequently split G into 8 cosets. Hence, $|\overline{G}| = 8$.

(b) The elements are

$$\overline{1} = \{1, \sigma^4\} \qquad\qquad \overline{\tau} = \{\tau, \tau\sigma^4\}$$
$$\overline{\sigma} = \{\sigma, \sigma^5\} \qquad\qquad \overline{\tau\sigma} = \{\tau\sigma, \tau\sigma^5\}$$
$$\overline{\sigma}^2 = \{\sigma^2, \sigma^6\} \qquad\qquad \overline{\tau\sigma^2} = \{\tau\sigma^2, \tau\sigma^6\}$$
$$\overline{\sigma}^3 = \{\sigma^3, \sigma^7\} \qquad\qquad \overline{\tau\sigma^3} = \{\tau\sigma^3, \tau\sigma^7\}$$

(c) The orders are

$\overline{x}$	$\overline{1}$	$\overline{\sigma}$	$\overline{\sigma}^2$	$\overline{\sigma}^3$	$\overline{\tau}$	$\overline{\tau\sigma}$	$\overline{\tau\sigma^2}$	$\overline{\tau\sigma^3}$
$|\overline{x}|$	1	4	2	4	2	2	2	2

(d) $\overline{\sigma\tau} = \overline{\tau\sigma^3}, \overline{\tau\sigma^{-2}\tau} = \overline{\sigma}^2, \overline{\tau^{-1}\sigma^{-1}\tau\sigma} = \overline{\sigma}^2$.

(e) Note that $\overline{\sigma}^4 = \overline{\tau}^2 = \overline{1}$, and $\overline{\sigma}\overline{\tau} = \overline{\tau\sigma^3} = \overline{\tau\sigma^7} = \overline{\tau\sigma}$ so that $\overline{G}$ satisfies the same relations in D_8. Then the mapping $\varphi : \overline{G} \to D_8$ given by $\varphi(\overline{\sigma}) = r$ and $\varphi(\overline{\tau}) = s$ extends to a surjective homomorphism, hence $\overline{G} \cong D_8$. $\qquad\square$

(19) Let G be the modular group of order 16 (whose lattice was computed in Exercise 14 of Section 2.5): $G = \langle u, v \mid u^2 = v^8 = 1,\ v u = u v^5 \rangle$, and let $\overline{G} = G/\langle v^4 \rangle$ be the quotient of G by the subgroup generated by v^4 (this subgroup is contained in the center of G, hence is normal).

   (a) Show that the order of $\overline{G}$ is 8.
   (b) Exhibit each element of $\overline{G}$ in the form $\overline{u}^a \overline{v}^b$, for some integers a and b.
   (c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).
   (d) Write each of the following elements of $\overline{G}$ in the form $\overline{u}^a \overline{v}^b$, for some integers a and b as in (b): $\overline{v u}$, $\overline{u v^{-2} u}$, $\overline{u^{-1} v^{-1} u v}$.
   (e) Prove that $\overline{G}$ is abelian and is isomorphic to $Z_2 \times Z_4$.

Solution.

   (a) $\langle v^4 \rangle$ has 2 elements, so each coset has 2 elements. Then G is split into 8 cosets, hence $|\overline{G}| = 8$.
   (b) The elements are

$$\overline{1} = \{1, v^4\} \qquad\qquad \overline{u} = \{u, u v^4\}$$
$$\overline{v} = \{v, v^5\} \qquad\qquad \overline{u v} = \{u v, u v^5\}$$
$$\overline{v}^2 = \{v^2, v^6\} \qquad\qquad \overline{u v^2} = \{u v^2, u v^6\}$$
$$\overline{v}^3 = \{v^3, v^7\} \qquad\qquad \overline{u v^3} = \{u v^3, u v^7\}$$

   (c) The orders are

$\overline{x}$	$\overline{1}$	$\overline{v}$	$\overline{v}^2$	$\overline{v}^3$	$\overline{u}$	$\overline{u v}$	$\overline{u v^2}$	$\overline{u v^3}$
$\lvert \overline{x} \rvert$	1	4	2	4	2	2	2	2

   (d) $\overline{v u} = \overline{u v^5}, \overline{u v^{-2} u} = \overline{u}^2, \overline{u^{-1} v^{-1} u v} = \overline{1}$.
   (e) Since $\overline{v u} = \overline{u v^5} = \overline{u v}$, $\overline{G}$ is abelian. Moreover, using the presentation of $Z_2 \times Z_4$ in Section 2.5, Exercise 12, we see that $\overline{u}^2 = \overline{v}^4 = 1$ so that $\overline{G}$ satisfies the same relations. Then $\varphi : \overline{G} \to Z_2 \times Z_4$ given by $\varphi(\overline{u}) = a$ and $\varphi(\overline{v}) = b$ is a surjective homomorphism, hence $\overline{G} \cong Z_2 \times Z_4$. $\qquad\square$

(20) Let $G = \mathbb{Z}/24\mathbb{Z}$ and let $\widetilde{G} = G/\langle \overline{12} \rangle$, where for each integer a we simplify notation by writing $\widetilde{\overline{a}} a$ as $\widetilde{a}$.

   (a) Show that $\widetilde{G} = \{\widetilde{0}, \widetilde{1}, \ldots, \widetilde{11}\}$.
   (b) Find the order of each element of $\overline{G}$.
   (c) Prove that $\widetilde{G} \cong \mathbb{Z}/12\mathbb{Z}$ (thus $(\mathbb{Z}/24\mathbb{Z})/(12\mathbb{Z}/24\mathbb{Z}) \cong \mathbb{Z}/12\mathbb{Z}$, just as if we inverted and canceled the $24\mathbb{Z}$'s).

Solution.

   (a) Note that for some $\widetilde{x} \in \widetilde{G}$, we have $\widetilde{x} = \overline{x}\langle 12 \rangle = \{\overline{x}, \overline{x+12}\}$. It follows that $x = 0, 1, 2, \ldots, 11$ produces distinct cosets.
   (b) The orders are

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

   (c) Define the mapping $\varphi : \widetilde{G} \to \mathbb{Z}/12\mathbb{Z}$ given by $\varphi(\widetilde{x}) = \overline{x}$. This map is trivially a bijection, and for any $\widetilde{x}, \widetilde{y} \in \widetilde{G}$, then

$$\varphi(\widetilde{x} + \widetilde{y}) = \varphi(\widetilde{x+y}) = \overline{x+y} = \overline{x} + \overline{y} = \varphi(\widetilde{x}) + \varphi(\widetilde{y})$$

   so that φ is a homomorphism. Then $\widetilde{G} \cong \mathbb{Z}/12\mathbb{Z}$. $\qquad\square$

(21) Let $G = Z_4 \times Z_4$ be given in terms of the following generators and relations:

$$G = \langle x, y \mid x^4 = y^4 = 1, x y = y x \rangle$$

Let $\overline{G} = G/\langle x^2 y^2 \rangle$ (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 elements of $\overline{G}$ exhibited in (b).

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

Solution.

(a) Note that $(x^2 y^2)^2 = x^4 y^4 = 1$ so that $\langle x^2 y^2 \rangle = \{1, x^2 y^2\}$. Then each coset of $\overline{G}$ has 2 elements, hence its order is 8.

(b) Noting that $\overline{x}^2 \overline{y}^2 = \overline{1}$ in $\overline{G}$, we have $\overline{x}^2 = \overline{y}^2$. Then we have the elements

$$\overline{1} = \{1, x^2 y^2\} \qquad\qquad \overline{y} = \{y, x^2 y^3\}$$
$$\overline{x} = \{x, x^3 y^2\} \qquad\qquad \overline{xy} = \{xy, x^3 y^3\}$$
$$\overline{x}^2 = \{x^2, y^2\} \qquad\qquad \overline{x^2 y} = \{x^2 y, y^3\}$$
$$\overline{x}^3 = \{x^3, xy^2\} \qquad\qquad \overline{x^3 y} = \{x^3 y, xy^3\}$$

(c) The orders are

$\overline{g}$	$\overline{1}$	$\overline{x}$	$\overline{x}^2$	$\overline{x}^3$	$\overline{y}$	$\overline{xy}$	$\overline{x^2 y}$	$\overline{x^3 y}$
$|\overline{g}|$	1	4	2	4	4	2	4	2

(d) Using the presentation of $Z_2 \times Z_4$ in [Section 2.5, Exercise 12](), and noting that $\overline{xy}^2 = \overline{x}^4 = 1$ then the mapping $\varphi : Z_2 \times Z_4 \to \overline{G}$ given by

$$\varphi(a) = \overline{xy}, \quad \varphi(b) = \overline{x}$$

extends to a unique homomorphism. Now suppose $\varphi(a^s b^t) = \varphi(a^u b^v)$. Then $\overline{xy}^s \overline{x}^t = \overline{xy}^u \overline{x}^v$. Since $\langle \overline{xy} \rangle \cap \langle \overline{x} \rangle$ is trivial, then $\overline{xy}^{s-u} = \overline{x}^{v-t}$ imply that both quantities must be one. Then $\overline{xy}^s = \overline{xy}^u$ and $\overline{x}^v = \overline{x}^t$. Then $s \equiv u \bmod 2$ and $v \equiv t \bmod 4$, so that $a^s b^t = a^u b^t$ since $|a| = 2$ and $|b| = 4$. Then φ is injective. Because $|Z_2 \times Z_4| = |\overline{G}| = 8$, then φ is an isomorphism, hence $\overline{G} \cong Z_2 \times Z_4 \cong Z_4 \times Z_2$. □

(22) (a) 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.

(b) Prove that the intersection of an arbitrary nonempty collection of normal subgroups of a group is a normal subgroup (do not assume the collection is countable).

Solution.

(a) Observe that $H \cap K \leq G$ since $H \leq G$ and $K \leq G$. Let $g \in G$ and $x \in H \cap K$. Since $H \trianglelefteq G$ and $K \trianglelefteq G$, then $gxg^{-1} \in H$ and $gxg^{-1} \in K$, hence $gxg^{-1} \in H \cap K$. Then $g(H \cap K)g^{-1} \subseteq H \cap K$. By **??**, then $H \cap K \trianglelefteq G$.

(b) Let G be a group and I be a nonempty set of indices, possibly not countable. Consider the collection of subgroups $\{N_i \mid i \in I\}$ of G, where $N_i \trianglelefteq G$ for every $i \in I$. Consider their intersection

$$N = \bigcap_{i \in I} N_i$$

Since $N \leq G$, what remains to be shown is that $gNg^{-1} \subseteq N$ for some $g \in G$. To that end, let $n \in N$. Then $gng^{-1} \in N_i$ for each $i \in I$ because $N_i \trianglelefteq G$. It follows that $gng^{-1} \in N$ so that $gNg^{-1} \subseteq N$. □

(23) Prove that the join (cf. Section 2.5) of any nonempty collection of normal subgroups of a group is a normal subgroup.

Solution. Let G be a group and I be a nonempty set of indices. Let $\{N_i \mid i \in I\}$ be a collection of normal subgroups of G, and let $N = \langle N_i \mid i \in I \rangle$ be the join of the collection. Let $g \in G$ and $n \in N$. Then

$$n = n_1 n_2 \dots n_k \quad \text{where } n_i \in N_i \text{ for some } i \in I$$

Since $N_i \trianglelefteq G$, then $gn_i g^{-1} \in N_i$ for each $1 \leq i \leq k$. Then

$$gng^{-1} = g(n_1 n_2 \dots n_k)g^{-1} = (gn_1 g^{-1})(gn_2 g^{-1}) \cdots (gn_k g^{-1})$$

Because gng^{-1} is written as a product of elements where each one belongs to some N_i, it follows that it is in the join N, hence $gNg^{-1} \subseteq N$. Then $N \trianglelefteq G$. □

(24) Prove that if $N \trianglelefteq G$ and H is any subgroup of G then $N \cap H \trianglelefteq H$.

Solution. We know $N \cap H \leq G$, so pick $h \in H$ and $x \in N \cap H$. Since $N \trianglelefteq G$, then $hxh^{-1} \in N$. Since $H \leq G$, then $hxh^{-1} \in H$ so that $hxh^{-1} \in N \cap H$. Then $N \cap H \trianglelefteq H$. □

(25) (a) Prove that a subgroup N of G is normal if and only if $gNg^{-1} \subseteq N$ for all $g \in G$.
   (b) Let $G = \mathrm{GL}_2(\mathbb{Q})$, let N be the subgroup of upper triangular matrices with integer entries and 1's on the diagonal, and let g be the diagonal matrix with entries $2, 1$. Show that $gNg^{-1} \subseteq N$ but g does not normalize N.

Solution.

   (a) ($\Rightarrow$) If $N \trianglelefteq G$, then $gNg^{-1} \subseteq N$ holds true for all $g \in G$.

   ($\Leftarrow$) Suppose $gNg^{-1} \subseteq N$ for every $g \in G$, and let $n \in N$. To show that $N \subseteq gNg^{-1}$, note for some $g \in G$, then $g^{-1}Ng \subseteq N$ so that $g^{-1}ng \in N$. It follows that $n = g(g^{-1}ng)g^{-1} \in gNg^{-1}$ so that $N = gNg^{-1}$, hence $N \trianglelefteq G$.

   (b) Let
   $$n = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N$$

   where $x \in \mathbb{Z}$. Then
   $$gng^{-1} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix} \in N$$

   since $2x \in \mathbb{Z}$. Notice that the upper right entry of gng^{-1} for any $n \in N$ will be even, so any matrix with an odd integer in the upper right entry will have no such $n \in N$ such that gng^{-1} is that matrix. □

(26) Let $a, b \in G$.
   (a) Prove that the conjugate of the product of a and b is the product of the conjugate of a and the conjugate of b. Prove that the order of a and the order of any conjugate of a are the same.
   (b) Prove that the conjugate of a^{-1} is the inverse of the conjugate of a.
   (c) Let $N = \langle S \rangle$ for some subset S of G. Prove that $N \trianglelefteq G$ if $gSg^{-1} \subseteq N$ for all $g \in G$.
   (d) Deduce that if N is the cyclic group $\langle x \rangle$, then N is normal in G if and only if for each $g \in G$, $gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$.
   (e) Let n be a positive integer. Prove that the subgroup N of G generated by all the elements of G of order n is a normal subgroup of G.

Solution.
   (a) Note that $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$. The second result follows by [Exercise 1.1.22].
   (b) For any $g \in G$, then
   $$(ga^{-1}g^{-1})(gag^{-1}) = ga^{-1}(g^{-1}g)ag^{-1} = g(a^{-1}a)g^{-1} = gg^{-1} = 1$$

   so that $(gag^{-1})^{-1} = ga^{-1}g^{-1}$.
   (c) If S is empty, then N is trivial, so the result follows. Suppose S is not empty, and pick $n \in N$. Because $N = \langle S \rangle$, then we have $n = s_1 s_2 \ldots s_k$, where $s_i \in S$ for each $i = 1, 2, \ldots, k$. Since
   $$gng^{-1} = (gs_1g^{-1})(gs_2g^{-1})\cdots(gs_kg^{-1})$$

   for every $g \in G$, and $gSg^{-1} \subseteq N$, then the right hand side is also in N, hence $gNg^{-1} \subseteq N$ so that $N \trianglelefteq G$.
   (d) ($\Rightarrow$) Immediate from the definition of a normal subgroup.
   ($\Leftarrow$) Put $S = \{x\}$ and use the previous part.
   (e) Let $S = \{g \in G \mid |g| = n\}$, and put $N = \langle S \rangle$. If S is empty, then N is trivial, hence is normal. If S is nonempty, note that part (a) shows that for any $g \in G$ and $s \in S$, then $|gsg^{-1}| = |s| = n$ so that $gsg^{-1} \in S \subseteq N$. Then $gSg^{-1} \subseteq N$, hence $N \trianglelefteq G$ by part (c). □

(27) Let N be a *finite* subgroup of a group G. Show that $gNg^{-1} \subseteq N$ if and only if $gNg^{-1} = N$. Deduce that $N_G(N) = \{g \in G \mid gNg^{-1} \subseteq N\}$.

Solution. ($\Rightarrow$) Suppose $gNg^{-1} \subseteq N$. For any $g \in G$, define a mapping $\varphi : N \to gNg^{-1}$ given by $\varphi(n) = gng^{-1}$. If $\varphi(m) = \varphi(n)$, then $gmg^{-1} = gng^{-1}$ so that φ is injective by cancellation. Moreover, if $m \in gNg^{-1}$, there exists $n \in N$ such that $m = gng^{-1} = \varphi(n)$ so that φ is surjective. It follows that φ is a bijection, and $|N| = |gNg^{-1}|$. Since $gNg^{-1} \subseteq N$, and N is finite, it follows that $gNg^{-1} = N$.
($\Leftarrow$) Immediate.
   Note that $N_G(N) = \{g \in G \mid gNg^{-1} = N\}$. We may replace the condition that $gNg^{-1} = N$ with $gNg^{-1} \subseteq N$ by the implication showed above. $\square$

(28) Let N be a *finite* subgroup of a group G and assume $N = \langle S \rangle$ for some subset S of G. Prove that an element $g \in G$ normalizes N if and only if $gSg^{-1} \subseteq N$.

Solution. ($\Rightarrow$) Immediate, since $gSg^{-1} \subseteq gNg^{-1} = N$ because $g \in N_G(N)$.
($\Leftarrow$) If S is empty, then N is trivial hence the conclusion follows. Suppose S is not empty, and pick $n \in N$. Then $n = s_1 s_2 \ldots s_k$, where $s_i \in S$ for every $i = 1, 2, \ldots, k$. Then $gng^{-1} = gs_1 g^{-1} gs_2 g^{-1} \ldots gs_k g^{-1} \in N$ because $gs_i g^{-1} \in gSg^{-1} \subseteq N$. Then $gNg^{-1} \subseteq N$, and by the previous exercise, $g \in N_G(N)$. $\square$

(29) Let N be a *finite* subgroup of G and suppose $G = \langle T \rangle$ and $N = \langle S \rangle$ for some subsets S and T of G. Prove that N is normal in G if and only if $tSt^{-1} \subseteq N$ for all $t \in T$.

Solution. ($\Rightarrow$) Immediate, since $gNg^{-1} = N$ for every $g \in G$, so $tSt^{-1} \subseteq N$.
($\Leftarrow$) Suppose S and T are nonempty subsets of G, and let $g \in G$. Since $g \in \langle T \rangle$, then $g = t_1 t_2 \ldots t_k$, where $t_i \in T$ for each $i = 1, 2, \ldots, k$. Since we need to show this for every $g \in G$, we must proceed by inducting on the word length of $g \in \langle T \rangle$. To that end, $t_1 S t_1^{-1} \subseteq N$, so the base case is satisfied. Assume now that $gSg^{-1} \subseteq N$ when g is some k-length word made up of elements from T. Consider the $k+1$-length word $g = t_1 t_2 \ldots t_k t_{k+1}$, where $t_i \in T$ for each $i = 1, 2, \ldots, k+1$. For notation, set $\hat{t} = t_1 t_2 \ldots t_k$ so that $g = \hat{t} t_{k+1}$. The induction assumption shows that $\hat{t} S \hat{t}^{-1} \subseteq N$. For any $s \in S$, then

$$gsg^{-1} = \hat{t} t_{k+1} s t_{k+1}^{-1} h^{-1} = \hat{t}(t_{k+1} s t_{k+1}^{-1}) \hat{t}^{-1}$$

where $t_{k+1} s t_{k+1}^{-1} \in N$ because $tSt^{-1} \subseteq N$ for every $t \in T$. Since $N = \langle S \rangle$, then we may set $t_{k+1} s t_{k+1}^{-1} = s_1 s_2 \ldots s_m$, where $s_i \in S$ for every $i = 1, 2, \ldots, m$. Then

$$\hat{t}(t_{k+1} s t_{k+1}^{-1}) \hat{t}^{-1} = (\hat{t} s_1 \hat{t}^{-1})(\hat{t} s_2 \hat{t}^{-1}) \cdots (\hat{t} s_m \hat{t}^{-1}) \in N$$

Hence, $gsg^{-1} \in N$ so that $gSg^{-1} \subseteq N$. Induction shows that this is true for every $g \in G$, and by finiteness of N, we use the result from the previous exercise to conclude that $N \trianglelefteq G$. $\square$

(30) Let $N \leq G$ and let $g \in G$. Prove that $gN = Ng$ if and only if $g \in N_G(N)$.

Solution. ($\Rightarrow$) Suppose $gN = Ng$. For some $n \in N$, there exists $n' \in N$ such that $ng = gn'$, or $n = gn'g^{-1}$. Then $n \in gNg^{-1}$ so that $N \subseteq gNg^{-1}$. Moreover, if $n \in N$, then for some $n' \in N$ we have $gn = n'g$ so that $gng^{-1} = n'$, hence $gNg^{-1} \subseteq N$, hence $g \in N_G(N)$.
($\Leftarrow$) Suppose $g \in N_G(N)$ and $n \in N$. Since $n \in gNg^{-1}$, there exists $n' \in N$ such that $n = gn'g^{-1}$ so that $ng = gn'$, hence $n \in gN$, and $Ng \subseteq gN$. By symmetry, we have $gN \subseteq Ng$, hence $gN = Ng$. $\square$

(31) Prove that if $H \leq G$ and N is a normal subgroup of H then $H \leq N_G(N)$. Deduce that $N_G(N)$ is the largest subgroup of G in which N is normal (i.e. is the join of all subgroups H for which $N \trianglelefteq H$).

Solution. If $h \in H$, then $hNh^{-1} = N$ because $N \trianglelefteq H$, hence $h \in N_G(N)$. Because $N_G(N) \leq G$, then $H \subseteq N_G(N)$ implies $H \leq N_G(N)$. Moreover, since every subgroup such that N is normal in is a subgroup of $N_G(N)$, then $N_G(N)$ is the largest subgroup in which N is normal. $\square$

(32) Prove that every subgroup of Q_8 is normal. For each subgroup find the isomorphism type of its corresponding quotient. [You may use the lattice of subgroups for Q_8 in Section 2.5.]

Solution. By the lattice, the subgroups of Q_8 are 1, $\langle -1 \rangle, \langle i \rangle, \langle j \rangle, \langle k \rangle$, and Q_8. It is clear that $Q_8/1 \cong Q_8$, and $Q_8/Q_8 \cong 1$. Now, the lattice shows that $\langle i \rangle, \langle j \rangle$, and $\langle k \rangle$ are all maximal subgroups, so their normalizers must either be themselves, or Q_8. Since $j\langle i \rangle(-j) = \langle i \rangle$, then $j \in N_{Q_8}(\langle i \rangle)$ so that $N_{Q_8}(\langle i \rangle) = Q_8$. We may similarly argue that $N_{Q_8}(\langle j \rangle) = N_{Q_8}(\langle k \rangle) = Q_8$. Moreover, $Z(Q_8) = \langle -1 \rangle$, and every center of a group is normal. It follows that every subgroup of Q_8 is normal.

Let us first examine $Q_8/\langle -1 \rangle = \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\}$. Since $\bar{i}^2 = \overline{-1} = \bar{1}$, then $|\bar{i}| = 2$. We can argue that $|\bar{j}| = |\bar{k}| = 2$ so that $Q_8/\langle -1 \rangle \cong V_4$. The quotient group $Q_8/\langle i \rangle = \{\bar{1}, \bar{j}\}$ has order 2 so $Q_8/\langle i \rangle \cong Z_2$. By symmetry, $Q_8/\langle j \rangle \cong Q_8/\langle k \rangle \cong Z_2$. $\qquad\square$

(33) Find all normal subgroups of D_8 and for each of these find the isomorphism type of its corresponding quotient. [You may use the lattice of subgroups for D_8 in Section 2.5.]

Solution. Again, $D_8/1 \cong D_8$ and $D_8/D_8 \cong 1$. Examining the three maximal subgroups $\langle s, r^2 \rangle, \langle r \rangle$, and $\langle rs, r^2 \rangle$, observe the following:

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

so that the normalizers of each of the subgroups contain r and s, hence $N_{D_8}(\langle s, r^2 \rangle) = N_{D_8}(\langle r \rangle) = N_{D_8}(\langle rs, r^2 \rangle) = Q_8$. Moreover, each of these maximal subgroups are of order 4, which means their corresponding quotient groups will have order 2, hence $Q_8/\langle s, r^2 \rangle \cong Q_8/\langle r \rangle \cong Q_8/\langle rs, r^2 \rangle \cong Z_2$.

Now we examine $\langle r^2 \rangle = Z(D_8)$ so it is clearly normal. Then $D_8/\langle r^2 \rangle = \{\bar{1}, \bar{r}, \bar{s}, \overline{sr}\}$. Note that the nonidentity elements have order 2, and so $D_8/\langle r^2 \rangle \cong V_4$.

For the remaining subgroups of order 2, observe that

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

so that none of the subgroups of order 2 contain r, hence none of them are normal. $\qquad\square$

(34) Let $D_{2n} = \langle r, s \mid r^n = s^2 = 1, \ rs = sr^{-1} \rangle$ be the usual presentation of the dihedral group of order $2n$ and let k be a positive integer dividing n.

  (a) Prove that $\langle r^k \rangle$ is a normal subgroup of D_{2n}.

  (b) Prove that $D_{2n}/\langle r^k \rangle \cong D_{2k}$.

Solution.

  (a) Observe that $\langle r^k \rangle = \{1, r^k, r^{2k}, \dots, r^{n-k}\}$. It is clear that $r\langle r^k \rangle r^{-1} = \langle r^k \rangle$, and observe that $sr^ks^{-1} = r^{-k} = r^{n-k}$ so that $s\langle r^k \rangle s^{-1} = \langle r^k \rangle$. Since $r, s \in N_{D_{2n}}(\langle r^k \rangle)$, then $\langle r^k \rangle \trianglelefteq D_{2n}$.

  (b) Consider $D_{2n}/\langle r^k \rangle$. Since $k \mid n$, then the order of $\langle r^k \rangle$ is n/k, and the number of cosets in the quotient group is $2n/(n/k) = 2k$. Now consider the cosets $\bar{r}$ and $\bar{s}$:

$$\bar{r} = \{r, r^{k+1}, r^{2k+1}, \dots, r^{n-k+1}\} \quad \text{and} \quad \bar{s} = \{s, sr^k, sr^{2k}, \dots, sr^{n-k}\}$$

It is clear that $\bar{s} \neq \bar{1}$, and $\bar{s}^2 = \bar{1}$ so that $|\bar{s}| = 2$. Moreover, $\bar{r}^k = \bar{1}$, hence $|\bar{r}| \leq k$. However, note that $\bar{r}^i = \bar{1}$ when $i \mid k$ so that $|\bar{r}| = k$. This clearly satisfies the relations for D_{2k}, hence $D_{2n}/\langle r^k \rangle \cong D_{2k}$. $\qquad\square$

(35) Prove that $\mathrm{SL}_n(F) \trianglelefteq \mathrm{GL}_n(F)$ and describe the isomorphism type of the quotient group (cf. Exercise 9, Section 2.1).

Solution. We know that $\mathrm{SL}_n(F) \leq \mathrm{GL}_n(F)$, so we just need to show that $A\,\mathrm{SL}_n(F)A^{-1} = \mathrm{SL}_n(F)$ for all $A \in \mathrm{GL}_n(F)$. To that end, note that for any $S \in \mathrm{SL}_n(F)$ and $X \in \mathrm{GL}_n(F)$, we have $\det(XSX^{-1}) = \det(X)\det(S)\det(X^{-1}) = 1$, hence $X\,\mathrm{SL}_n(F)X^{-1} \subseteq \mathrm{SL}_n(F)$, and $\mathrm{SL}_n(F) \trianglelefteq \mathrm{GL}_n(F)$.

Recall that when a subgroup is normal, it is actually the kernel of some homomorphism. Observe that every element of $\mathrm{SL}_n(F)$ has determinant 1, so if we consider the mapping $A \mapsto \det(A)$ for some $A \in \mathrm{GL}_n(F)$, then the kernel of this homomorphism is clearly $\mathrm{SL}_n(F)$. We may then consider the mapping $\varphi : \mathrm{GL}_n(F)/\mathrm{SL}_n(F) \to F^\times$ given by $\varphi(\overline{X}) = \det(X)$.

We now show that this mapping is well defined. To that end, suppose $\overline{A} = \overline{B}$ for some $\overline{A}, \overline{B} \in \mathrm{GL}_n(F)/\mathrm{SL}_n(F)$. Recall that the elements of $\overline{A}$ are of the form AS for $A \in \mathrm{GL}_n(F)$ and some $S \in \mathrm{SL}_n(F)$. Since $\overline{A} = \overline{B}$, then for $AS \in \overline{A}$ there exists $S' \in \mathrm{SL}_n(F)$ such that $AS = BS_0$. Then

$$\varphi(\overline{A}) = \det(A) = \det(AS) = \det(BS') = \det(B) = \varphi(\overline{B})$$

so that φ is well defined.

To show that φ is injective, suppose $\varphi(\overline{A}) = \varphi(\overline{B})$. Then $\det(A) = \det(B)$. Pick some $AS \in \overline{A}$, where $S \in \mathrm{SL}_n(F)$. Observe that $B^{-1}AS \in \mathrm{SL}_n(F)$, since $\det(B^{-1}AS) = \det(B^{-1})\det(A)\det(S) = \det(A)^{-1}\det(A)\det(S) = 1$, hence $B^{-1}AS = S'$ for some $S' \in \mathrm{SL}_n(F)$. Then $AS = BS'$, and $AS \in \overline{B}$ so that $\overline{A} \subseteq \overline{B}$. A similar argument shows that $\overline{B} \subseteq \overline{A}$ so that $\overline{A} = \overline{B}$, and φ is injective. Moreover, for some $f \in F^\times$, then $\det(fI_n) = f\det(I_n) = f$ so that φ is surjective. Lastly, for $\overline{A}, \overline{B} \in \mathrm{SL}_n(F)$, then

$$\varphi(\overline{AB}) = \det(AB) = \det(A)\det(B) = \varphi(\overline{A})\varphi(\overline{B})$$

so that φ is a homomorphism. Then φ is a bijective homomorphism, and $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^\times$.   □

(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 $x^a z$ for some integer $a \in \mathbb{Z}$ and some element $z \in Z(G)$.]

Solution. Suppose $G/Z(G) = \langle xZ(G) \rangle$ for some $x \in G$. Then cosets are of the form $x^a Z(G)$ for some $a \in \mathbb{Z}$. Suppose $g, h \in G$. Since both g and h belong to some coset in $G/Z(G)$, then $g = x^m z$ and $h = x^n z'$ for some $m, n \in \mathbb{Z}$ and $z, z' \in Z(G)$. Then

$$ab = (x^m z)(x^n z') = (x^n z')(x^m z) = ba$$

so that G is abelian.   □

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

Solution. Let C be the the given set. It is clear that $C \leq A \times B$. Suppose $(a,b) \in A \times B$. Then for any $(a',1) \in C$, we have

$$(a,b)(a',1)(a,b)^{-1} = (aa'a^{-1}, b1b^{-1}) = (aa'a^{-1}, 1) \in C$$

so that $C \trianglelefteq A \times B$.

Consider the mapping $\varphi : A \times B/C \to B$ given by $\varphi(\overline{(a,b)}) = b$. To show that this is well-defined, suppose $\overline{(a,b)} = \overline{(a',b')}$. Then $(a,b)C = (a',b')C$, which implies that $C = (a^{-1}, b^{-1})(a',b')C$, or that $(a^{-1}a', b^{-1}b') \in C$. Then $b^{-1}b' = 1$, or $b = b'$ so that φ is well-defined.

Now suppose $\varphi(\overline{(a,b)}) = \varphi(\overline{(a',b')})$. Then $b = b'$ so that $(a,b)C = (a',b')C$, hence φ is injective. Moreover, $\varphi(\overline{(1,b)}) = b$ so that φ is surjective. Lastly, for $\overline{(a,b)}, \overline{(a',b')} \in A \times B/C$, then

$$\varphi(\overline{(a,b)(a',b')}) = \varphi(\overline{(aa',bb')}) = bb' = \varphi(\overline{(a,b)})\varphi(\overline{(a',b')})$$

so that φ is a bijective homomorphism. Hence, $A \times B/C \cong B$.   □

(38) Let A be an abelian group and let D be the (diagonal) subgroup $\{(a,a) \mid a \in A\}$ of $A \times A$. Prove that D is a normal subgroup of $A \times A$ and $(A \times A)/D \cong A$.

Solution. Since A is abelian, then $A \times A$ is abelian, hence any subgroup is normal so that $D \trianglelefteq A \times A$.

Now consider two cosets $\overline{(a_1, a_2)}, \overline{(a_3, a_4)} \in (A \times A)/D$. Then $\overline{(a_1, a_2)} = \overline{(a_3, a_4)}$ when $(a_1, a_2)^{-1}(a_3, a_4) \in D$, which implies that $a_1^{-1}a_3 = a_2^{-1}a_4$, or $a_3 a_4^{-1} = a_1 a_2^{-1}$. We can construct a well-defined, injective homomorphism $\varphi : (A \times A)/D \to A$ given by $\varphi(\overline{(a,b)}) = ab^{-1}$. Moreover, this is surjective, since $\varphi(\overline{(a,1)}) = a$ for any

$a \in A$. Lastly, it is a homomorphism, because

$$\begin{aligned}
\varphi(\overline{(a_1, b_1)(a_2, b_2)}) &= \varphi(\overline{(a_1 a_2, b_1 b_2)}) \\
&= (a_1 a_2)(b_1 b_2)^{-1} \\
&= (a_1 b_1^{-1})(a_2 b_2^{-1}) \\
&= \varphi(\overline{(a_1, b_1)})\varphi(\overline{(a_2, b_2)})
\end{aligned}$$

Hence, φ is a bijective homomorphism, and $(A \times A)/D \cong A$. $\qquad\square$

(39) Suppose A is the non-abelian group S_3 and D is the diagonal subgroup $\{(a, a) \mid a \in A\}$ of $A \times A$. Prove that D is not normal in $A \times A$.

Solution. Let $\alpha, \beta \in S_3$, where $\alpha = 1$ and $\beta = (1\ 2\ 3)$ so that $\alpha^{-1} = \alpha$ and $\beta^{-1} \neq \beta$. For $\gamma = (1\ 2) \in S_3$, consider $\alpha\gamma\alpha^{-1}$ and $\beta\gamma\beta^{-1}$. Observe that $\alpha\gamma\alpha^{-1} = \gamma$, while $\beta\gamma\beta^{-1} = (1\ 2\ 3)(1\ 2)(3\ 2\ 1) = (2\ 3) \neq (1\ 2) = \gamma$. Then $(\alpha, \beta)(\gamma, \gamma)(\alpha^{-1}, \beta^{-1}) = (\gamma, (2\ 3))$, hence D is not a normal subgroup of $S_3 \times S_3$. $\qquad\square$

(40) Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$. (The element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y and is denoted by $[x, y]$.)

Solution. ($\Rightarrow$) Suppose $\overline{xy} = \overline{yx}$. Then $xyN = yxN$. Then there exists $n, n' \in N$ such that $xyn = yxn'$, or $x^{-1}y^{-1}xy = n'n^{-1}$ so that $x^{-1}y^{-1}xy \in N$.
($\Leftarrow$) Suppose $x^{-1}y^{-1}xy \in N$. Then there is $n \in N$ such that $x^{-1}y^{-1}xy = n$, or $xy = yxn$. Then $a \in xyN$ if and only if $a = xyn'$ for some $n' \in N$ if and only if $a = yxnn'$ if and only if $a \in yxN$. Hence, $\overline{xy} = \overline{yx}$. $\qquad\square$

(41) Let G be a group. Prove that $N = \langle x^{-1}y^{-1}xy \mid x, y \in G \rangle$ is a normal subgroup of G and G/N is abelian (N is called the *commutator* subgroup of G).

Solution. Let $g \in G$ and $x^{-1}y^{-1}xy \in N$. Then

$$g(x^{-1}y^{-1}xy)g^{-1} = (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) = (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \in N$$

so that $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}] \in N$. Then $gNg^{-1} \subseteq N$, hence $N \trianglelefteq G$.
$\quad$ G/N is abelian, since the previous exercise shows that $\overline{x}$ and $\overline{y}$ in G/N commute when $[x, y] \in N$. $\qquad\square$

(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 $x^{-1}y^{-1}xy \in H \cap K$.]

Solution. Let $x \in H$ and $y \in K$. Since $H \trianglelefteq G$, then $y^{-1}xy \in H$, hence $[x, y] \in H$. Since $K \trianglelefteq G$, then $x^{-1}y^{-1}x \in K$, hence $[x, y] \in K$. Then $[x, y] \in H \cap K = 1$ so that $[x, y] = 1$. It follows that $x^{-1}y^{-1}xy = 1$, or $xy = yx$. $\qquad\square$

(43) Assume $\mathscr{P} = \{A_i \mid i \in I\}$ is any partition of G with the property that $\mathscr{P}$ is a group under the "quotient operation" defined as follows: to compute the product of A_i with A_j take any element a_i of A_i and any element a_j of A_j and let $A_i A_j$ be the element of $\mathscr{P}$ containing $a_i a_j$ (this operation is assumed to be well defined). Prove that the element of $\mathscr{P}$ that contains the identity of G is a normal subgroup of G and the elements of $\mathscr{P}$ are the cosets of this subgroup (so $\mathscr{P}$ is just a quotient group of G in the usual sense).

Solution. For any $g \in G$, let $\overline{g} \in \mathscr{P}$ be the element such that $g \in \overline{g}$. Now, $\overline{1} \in \mathscr{P}$ is the set such that $1 \in \overline{1}$ so that $\overline{1}$ is nonempty. Moreover, for any $g, h \in \overline{1}$, we have $\overline{gh} = \overline{g} \cdot \overline{h} = \overline{1} \cdot \overline{1} = \overline{1}$ so that $\overline{1}$ is closed under the operation. Lastly, we have that $\overline{g^{-1}} = \overline{g^{-1}} \cdot \overline{1} = \overline{g^{-1}} \cdot \overline{g} = \overline{g^{-1}g} = \overline{1}$ so that $\overline{1}$ is closed under inverses, hence $\overline{1} \leq G$.
$\quad$ To show that $\overline{1} \trianglelefteq G$, let $g \in G$ and $x \in \overline{1}$. Then $\overline{gxg^{-1}} = \overline{g} \cdot \overline{x} \cdot \overline{g^{-1}} = \overline{g} \cdot \overline{1} \cdot \overline{g^{-1}} = \overline{gg^{-1}} = \overline{1}$, hence $gxg^{-1} \in \overline{1}$ so that $\overline{1} \trianglelefteq G$.
$\quad$ Consider some $g\overline{1} \in G/\overline{1}$, and let $\overline{g} \in \mathscr{P}$. For some $gy \in g\overline{1}$ where $y \in \overline{1}$, then $\overline{gy} = \overline{g} \cdot \overline{y} = \overline{g} \cdot \overline{1} = \overline{g}$ so that $gy \in \overline{g}$, hence $g\overline{1} \subseteq \overline{g}$. If $x \in \overline{g}$, then $\overline{x} = \overline{g}$ so that $\overline{g^{-1}x} = \overline{g^{-1}g} = \overline{1}$, hence $g^{-1}x \in \overline{1}$. Then $x = gg^{-1}x = g(g^{-1}x) \in g\overline{1}$, hence $\overline{g} \subseteq g\overline{1}$. It follows that $\overline{g} = g\overline{1}$. $\qquad\square$

3.2   More on Cosets and Lagrange's Theorem