Section 0.2

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

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

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

Proof. (Bastille) Let $t \in \mathbb{Z}$. Assume $ax_0 + by_0 = N$ (with $x_0, y_0 \in \mathbb{Z}$). Define

$$x = x_0 + \frac{b}{d}t \quad , \quad y = y_0 - \frac{a}{d}t.$$

First we verify that $x, y \in \mathbb{Z}$: since $d = (a, b)$, $d|b$, $d|a$, $d \neq 0$. Therefore since also $a, b \neq 0$

$$\exists\, k_1, k_2 \in \mathbb{Z}^* : \quad b = k_1 d \quad , \quad a = k_2 d$$

and so $k_1 = \dfrac{b}{d} \in \mathbb{Z}$ and $k_2 = \dfrac{a}{d} \in \mathbb{Z}$. Hence $x, y \in \mathbb{Z}$. Now we have:

$$\begin{aligned} ax + by = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ba}{d}t \\ = \underbrace{ax_0 + by_0}_{=N \text{ by assumption}} + \underbrace{\left(\frac{ab}{d} - \frac{ba}{d}\right)}_{=0} t &= N. \end{aligned}$$

□

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

(Bastille) We present the formulae used to compile the table below. By definition,

$$\varphi(n) = |\{a : (a, n) = 1\ , 1 \leq a \leq n\}|\,. \tag{1}$$

We also have for p a prime and $\alpha \geq 1$

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1). \tag{2}$$

And for any a, b such that $(a, b) = 1$ we have

$$\varphi(ab) = \varphi(a)\varphi(b). \tag{3}$$

Hence we used (1) to compute $\varphi(1)$, (2) to compute φ for $2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29,$ and (3) for $6 = 3 \cdot 2,\ 10 = 2 \cdot 5,\ 12 = 3 \cdot 4,\ 14 = 2 \cdot 7,\ 15 = 3 \cdot 5,\ 18 = 2 \cdot 9,\ 20 = 4 \cdot 5,\ 21 = 3 \cdot 7,\ 22 = 2 \cdot 11,\ 24 = 3 \cdot 8,\ 26 = 2 \cdot 13,\ 28 = 4 \cdot 7,\ 30 = 5 \cdot 6.$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

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

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

Proof. (Bastille) We assume $0 < d \leq n$ to be able to define $\varphi(d), \varphi(n)$. Let $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the prime factorization of d. If $d|n$ with $0 < d \leq n$ then there exists $\ell \in \mathbb{Z}^+$ such that

$$n = \ell d.$$

We can always write ℓ in the following way:

$$\ell = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} m$$

such that $(m, p_i) = 1 \quad \forall i \in \{1, \dots k\}$ with the stipulation that $\beta_i \geq 0$. Hence,

$$n = \ell d = p_1^{\alpha_1+\beta_1} \cdots p_k^{\alpha_k+\beta_k} m,$$

and

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{\alpha_1+\beta_1} \cdots p_k^{\alpha_k+\beta_k}) \cdot \varphi(m) \quad \text{ since } \left(m, p_1^{\alpha_1+\beta_1} \cdots p_k^{\alpha_k+\beta_k}\right) = 1 \\
&= p_1^{\alpha_1+\beta_1-1}(p_1 - 1) \cdots p_k^{\alpha_k+\beta_k-1}(p_k - 1) \cdot \varphi(m) \\
&= \underbrace{p_1^{\alpha_1-1}(p_1 - 1) \cdots p_k^{\alpha_k-1}(p_k - 1)}_{=\varphi(d)} \cdot \underbrace{p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta^k} \cdot \varphi(m)}_{=:r\in\mathbb{Z}^+}.
\end{aligned}$$

Thus, there exists $r \in \mathbb{Z}$ such that $\varphi(n) = r\varphi(d)$. Therefore,

$$\varphi(d)|\varphi(n).$$

□

Section 0.3

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

Proof. (Gillispie) Let $n \in \mathbb{Z}$ be an odd positive integer, and there exists a $k \in \mathbb{Z}$ s.t. $n = 2k + 1$. We will proceed by induction on k.

Supposing $k = 0$, we have then that $n^2 \mod 8 \equiv (0 + 1)^2 \mod 8 \equiv 1 \mod 8$.

Now suppose the theorem holds for $k \geq 0$. Consider the odd integer $2(k + 1) + 1$, and note then that

$$\begin{aligned}
(2(k+1)+1)^2 \mod 8 &\equiv (2k+3)^2] \mod 8 \\
&\equiv (4k^2 + 12k + 9) \mod 8 \\
&\equiv (4k^2 + 4k + 1) \mod 8 \\
&\equiv (2k+1)^2 \mod 8 \\
&\equiv 1 \mod 8 \text{ by induction.}
\end{aligned}$$

Thus, the theorem holds for all of the positive odd integers.

Suppose $n = 2k + 1$ is an odd negative integer. Note then that $(2k + 1)(-1) > 0$

$$\begin{aligned}
n \mod 8 &= (2k+1) \mod 8 \\
&= (2k+1)(-1)(-1) \mod 8 \\
&\equiv ((2k+1)(-1) \mod 8)(-1 \mod 8) \\
&\equiv 1 \cdot 7 \mod 8 \\
&\equiv 1 \mod 8.
\end{aligned}$$

Hence the remainder of any odd integer when divided by 8 is 1.

□

13. Let $n \in \mathbb{Z}$, $n > 1$ and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. If $(a, n) = 1$ then there is an integer c s.t. $ac \equiv 1(mod n)$.

Proof. (Gillispie) Since $(a, n) = 1$, by 0.2.7 we know there are $x, y \in \mathbb{Z}$ s.t.

$$ax + ny = 1.$$

Using cancellation, we establish

$$ax = -ny + 1 = (-y)n + 1 \equiv 1(mod n).$$

□

Section 1.1

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

Proof. (Schamel) Since n is the order of an element, $n \geq 1$. Since n is also odd, there is an integer $r \geq 0$ so that $2r + 1 = n$. Since $|x| = n$ in G then $x = x^{n+1} = x^{(2r+1)+1} = x^{2(r+1)} = (x^2)^{r+1}$. Since $r + 1 \geq 1$, our claim is proven. □

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

Proof. (Schamel) Note first that, by hypothesis, each non-identity element is its own inverse. Let $x, y \in G$. Since $xy \in G$, we have $(xy)^2 = 1$ and thus

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

□

27 Prove that if x is an element of the group G then $\{x^n | n \in \mathbb{Z}\}$ is a subgroup of G.

Proof. (Buchholz) Let $H = \{x^n | n \in \mathbb{Z}\}$. Since $H \subseteq G$ we must show is that H is a group. First note that H inherits associativity from G. Then since G is a group $e \in G$ and $e^n = e$ so $e \in H$. Lastly since $x^{-1} \in G$ we we have $(x^{-1})^n = x^{-n}$ and $-n \in \mathbb{Z}$ we know that $x^{-1} \in H$. Hence $H \leq G$.

□

31 Prove that any finite group G of even order contains an element of order 2.

Proof. (Buchholz) Let $t(G) = \{g \in G | g \neq g^{-1}\}$. Note that if $a \in t(G)$ then $a^{-1} \in t(G)$ because $a \neq a^{-1}$. So $e \notin t(G)$ since the inverse of e is not in $t(G)$. Since $e \notin t(G)$ then $|t(G)|$ is even because each element and its inverse are contained in $t(G)$. We also know that G is of even order. Thus there exists some element $b \in G$, where $b \neq e$, such that $b^2 = e$. Hence G contains an element of order 2.

□

Section 1.3

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

   Proof. (Lawless)

   (a) S_3 ={1, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)}.
   elements with order 1: 1.
   elements with order 2: (1 2), (1 3), (2 3).
   elements with order 3: (1 2 3), (1 3 2).

   (b) S_4 = {1, (1 2), (1 3), (1 4), (2 3), (2 4), (3 4), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3), (1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3), (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2),}
   elements with order 1: 1.
   elements with order 2: (1 2), (1 3), (1 4), (2 3), (2 4), (3 4), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3).
   elements with order 3: (1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3).
   elements with order 4: (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2).

   □

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

   Proof. (Lawless) Since disjoint cycles commute, and since each of the cycles of σ are disjoint, then the order of σ is the least common multiple of the orders of the cycles. Since σ has a cycle of length 5, 3, and 2, then the order of σ is 30. □

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

   Proof. (Lawless) The elements of order 4 in S_4 are:

   $$(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,2\,4), (1\,3\,4\,2), (1\,4\,2\,3), (1\,4\,3\,2).$$

   This is a complete list since only four cycles can have order 4 in S_4 and there are $3! = 6$ four cycles. □

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

   Proof. (Lawless) The elements of order 2 in S_4 are:

   $$(1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3).$$

   □

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.

    Proof (Granade). Let p be prime, and let $x \in S_n$ have a disjoint cycle decomposition given by:

    $$x = x_1 x_2 \cdots x_m$$

    for some $x_i \in S_n$ being cycles. We shall then show each direction of the theorem in turn.

    $\Leftarrow$ Suppose that each x_i is a p-cycle. Then, since the order of x is given by $\operatorname{lcm}(p, p, \ldots, p)$, we have that $|x| = p$ as required.

$\Rightarrow$ We shall proceed here to show the contrapositive. Suppose x is not a product of p-cycles. That is, that there exists $k \in \{1, 2, \ldots, m\}$ such that $|x_k| = r \neq p$ for some $r \in \mathbb{N}$. Then, since p is prime, $r \nmid p$, and the order of x must include a factor of r. We conclude that $|x| \neq p$.

$\square$

Note that the theorem proved above does *not* hold if x is a product of non-commuting r-cycles for some composite r. To see this, consider that in S_5, $|(12)(345)| = \operatorname{lcm}(2, 3) = 6$, but that $(12)(345)$ is not a product of commuting 6-cycles.

19. Find all numbers n such that S_7 contains an element of order n.

Solution (Granade). Note that each element in S_7 can be written as the product of disjoint cycles. This decomposition can each number in $\{1, 2, 3, 4, 5, 6, 7\}$ at most once, limiting the possible decompositions available. For instance, we know that no element in S_7 has a disjoint cycle decomposition into two 4-cycles, since this would require that some number appear in two different cycles.

We can use this insight, along with the fact that the order of a permutation is completely determined by the lengths of the cycles in its disjoint cycle decomposition. Thus, to figure out the possible orders of elements in S_7, we start by listing the ways in which we can add the integers $\{2, 3, 4, 5, 6, 7\}$ and obtain a sum no greater than 7:

$$2,\ 2+2,\ 2+2+2,\ 3,\ 3+3,\ 4,\ 5,\ 6,\ 7,\ 2+3,\ 2+4,\ 2+5,\ 2+2+3,\ 3+4$$

Each sum listed corresponds to a possible order for an element in S_7, with some orders duplicated, as can be seen if we view each term as the length of a cycle in the decomposition of an element in S_7. Taking the least common multiple of the terms in each sum listed above, we find the possible orders (omitting 1):

$$\begin{aligned}
2 &= \operatorname{lcm}(2) = \operatorname{lcm}(2,2) = \operatorname{lcm}(2,2,2) \\
3 &= \operatorname{lcm}(3) = \operatorname{lcm}(3,3) \\
4 &= \operatorname{lcm}(4) = \operatorname{lcm}(2,4) \\
5 &= \operatorname{lcm}(5) \\
6 &= \operatorname{lcm}(6) = \operatorname{lcm}(2,3) = \operatorname{lcm}(2,2,3) \\
7 &= \operatorname{lcm}(7) \\
10 &= \operatorname{lcm}(2,5) \\
12 &= \operatorname{lcm}(3,4)
\end{aligned}$$

Thus, elements in S_7 can have orders in $\{1, 2, 3, 4, 5, 6, 7, 10, 12\}$.

Chapter 1.4

2. Write out all the elements of $GL_2(\mathbb{F}_2)$ and compute the order of each element.

(Baggett) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ order $= 1$

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ order $= 2$

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ order $= 2$

$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ order $= 2$

$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ order $= 3$

$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ order $= 3$

10. Let $G = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} | a, b, c \in \mathbb{R}; a \neq 0, c \neq 0\}$

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.
(Baggett)

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$$

Since $a_1 \neq 0$ and $a_2 \neq 0$, $a_1a_2 \neq 0$; similarly, since $c_1 \neq 0$ and $c_2 \neq 0$, $c_1c_2 \neq 0$. Thus, $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \in G$, and 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.

(Baggett) Since $\det \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = ac \neq 0$ because $a \neq 0$ and $c \neq 0$, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1}$ exists. Furthermore, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & \frac{-b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix}$ since

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} \frac{1}{a} & \frac{-b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} \frac{1}{a} & \frac{-b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Note that since $a \neq 0$ and $c \neq 0$, $\frac{1}{a}$, $\frac{-b}{ac}$, $\frac{1}{c} \in \mathbb{R}$. Also, $\frac{1}{a} \neq 0$ and $\frac{1}{c} \neq 0$. Hence, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} \in G$ and G is closed under inverses.

c. Deduce that G is a subgroup of $GL_2(\mathbb{R})$.

(Baggett) Firstly, $\varnothing \neq G \subseteq GL_2(\mathbb{R})$, since $\det \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = ac \neq 0$ because $a \neq 0$ and $c \neq 0$. Secondly, G is closed under inverses and matrix multiplication. This is enough to show that G is a subgroup of $GL_2(\mathbb{R})$. (If $A \in G$, then $A^{-1} \in G$, and $AA^{-1} = I_2 \in G$ since G is closed under multiplication. Since matrix multiplication is associative in $GL_2(\mathbb{R})$, matrix multiplication is associative in G.) Therefore, G is a subgroup of $GL_2(\mathbb{R})$.

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

Proof. (Baggett) First, we will show that $H = \{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} | a, b \in \mathbb{R}; a \neq 0\}$ is closed under matrix multiplication. Take any two matrices $\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} \in H$. Then

$$\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1a_2 \\ 0 & a_1a_2 \end{pmatrix}$$

Since $a_1 \neq 0$ and $a_2 \neq 0$, $a_1a_2 \neq 0$. Thus, $\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} \in H$ and H is closed under matrix multiplication. Second, we will show that H is closed under inverses. Take any matrix $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in H$. Then $\det \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a^2 \neq 0$ because $a \neq 0$, so $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1}$ exists. Furthermore, $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a^2} \\ 0 & \frac{1}{a} \end{pmatrix}$ since

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

and

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

Because $a \neq 0$, $\frac{1}{a}, -\frac{b}{a^2} \in \mathbb{R}$ and $\frac{1}{a} \neq 0$. Hence, $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} \in H$ and H is closed under inverses. Lastly, $H \subseteq GL_2(\mathbb{R})$ since for any $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in H$, $\det \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a^2 \neq 0$ because $a \neq 0$. As before, this is enough to conclude that H is a subgroup of $GL_2(\mathbb{R})$.

□

Chapter 1.5

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

   (Baggett)
   $|\ 1| = 1$
   $|-1| = 2$
   $|\ i| = 4$
   $|-i| = 4$
   $|\ j| = 4$
   $|-j| = 4$
   $|\ k| = 4$
   $|-k| = 4$

Section 1.6

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

   Lemma: The identity element of G maps to the identity element of H.

   Let e_G be the identity element in G. Then we know that $ae_G = e_G a = a$ where $a \in G$. Further, it is true that $\varphi(ae_G) = \varphi(e_G a) = \varphi(a) = \varphi(a)\varphi(e_G) = \varphi(e_G)\varphi(a)$. Let $\varphi(a) = b$ where $b \in H$. Then $b\varphi(e_G) = \varphi(e_G)b = b$ and $\varphi(e_G)$ is the identity element in H or $\varphi(e_G) = e_H$. Thus, the identity element of G maps to the identity element of H.

   Proof. (Mobley) If $x \in G$ has order n, it follows that $x^n = e_G$. Then $\varphi(x^n) = [\varphi(x)]^n = \varphi(e_G)$. From the lemma, we can state that $[\varphi(x)]^n = \varphi(e_G) = e_H$, and therefore $|\varphi(x)| \Big| n$. However, if $|\varphi(x)| = k < n$, then $e_H = \varphi(x)^k = \varphi(x^k) = \varphi(e_G)$ and since φ is an isomorphism, we have $x^k = e_G$. It follows that $|x| \Big| k < n$ which contradicts that n is the *smallest* positive integer for which $|x^n| = e_G$. Thus, $|\varphi(x)| = |x|$ in the finite case.

   Let $y \in G$ have infinite order. Suppose $|\varphi(y)| = m$. Then $[\varphi(y)]^m = \varphi(y^m) = e_H$. We have shown in the lemma that $\varphi(e_G) = e_H$. Then $\varphi(y^m) = \varphi(e_G)$. It must follow that $y^m = e_G$ and that y has a finite order. But this is a contradiction. Thus, if the order of $y \in G$ is infinite, the order of $\varphi(y)$ is also infinite.

   □

Since $|\varphi(x)| = |x|$ for all $x \in G$, it must be the case that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. If the case existed that one group had more elements of order n than the other group, it would not be true that $|\varphi(x)| = |x|$ for all $x \in G$.

The result is not true if φ is only assumed to be a homomophism. As an example we have the homomorphism of $\varphi : \mathbb{C} \to \mathbb{C}$ defined by $\varphi(z) = z^2$. Here the order of i is 4. The order of $\varphi(i)$ is 2.

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

Proof. (Mobley) If it were true that $\mathbb{R} - \{0\} \cong \mathbb{C} - \{0\}$, then for all $x \in G$, $|x| = |\varphi(x)|$. However, in $R - \{0\}$, $|e| = 1$, $|-1| = 2$ and all other elements have infinite order. In the case of $\mathbb{C} - \{0\}$, $|e| = 1$, $|-1| = 2$, but $|i| = 4$. Since there is no element in $\mathbb{R} - \{0\}$ with order 4, $\mathbb{R} - \{0\} \ncong \mathbb{C} - \{0\}$.

□

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

Proof. (Mobley) If it were true that $\mathbb{R} \cong \mathbb{Q}$, then $|\mathbb{R}|$ would have to be equal to $|\mathbb{Q}|$. But $\mathbb{R}$ is an uncountable set whereas $\mathbb{Q}$ is a countable set. Therefore $|\mathbb{R}| \neq |\mathbb{Q}|$ and the two additive groups are not isomorphic.

□

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

Proof. (Mobley) If it were true that $\mathbb{Z} \cong \mathbb{Q}$, then a group isomorphism φ would have to exist between the two groups. However, since φ sends $1_{\mathbb{Z}}$ to $1_{\mathbb{Q}}$ and preserves sums, we have that $\varphi(z) = z \in \mathbb{Q}$ for all $z \in \mathbb{Z}$. We can see however that this mapping is not surjective. □

14. (Hazlett) Let G and H be groups and let $\phi : G \to H$ be a homomorphism. 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

Proof. First, notice that $e_G \in \ker(\phi)$ so the kernel is non-empty. Now choose $x, y \in \ker(\phi)$. Then $\phi(xy) = \phi(x)\phi(y) = 1_H 1_H = 1_H$. So $xy \in \ker(\phi)$ and the kernel is closed under products. Note $\phi(x^{-1}) = 1_H\phi(x^{-1}) = \phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1_G) = 1_H$. Consequently $x^{-1} \in \ker(\phi)$. Since $\ker(\phi)$ is non-empty, closed under products and inverses, $\ker(\phi) \leq G$.

Suppose $\ker(\phi) = \{1_G\}$ and $\phi(x) = \phi(y)$. Thus $\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(y)\phi(y^{-1}) = \phi(yy^{-1}) = \phi(1_G) = 1_H$. So $xy^{-1} \in \ker(\phi)$. This implies that $xy^{-1} = 1_G$. Hence $x = y$ and ϕ is an injection. Assume instead then that ϕ is an injection. Let $x \in \ker(\phi)$. Then $\phi(x) = \phi(1_G)$. Therefore $x = 1_G$ and $\ker(\phi) = \{1_G\}$. □

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

Proof. Let $\phi : G \to G$ such that $\phi(x) = x^k$ for some fixed integer k. Note $\phi(xy) = (xy)^k = x^k y^k = \phi(x)\phi(y)$. Thus ϕ is a homomorphism. Choose $z \in G$. Then for some $n \in \mathbb{Z}^+$ we have $z^n = 1$. Note further that if we write $z = e^{i\theta}$ then, z has a kth root, $w = e^{i\frac{\theta}{k}}$. Moreover, $(w)^{nk} = z^n = 1$. Hence $w \in G$. Also, $\phi(w) = z$. Consequently ϕ is a surjection. Note, there are exactly k kth-roots of unity. Thus there are $w_1, w_2, \ldots, w_k \in \mathbb{C}$ where $w_i^k = 1$. Then $w_i \in G$ for $1 \leq i \leq k$. However, $\phi(w_i) = w_i^k = 1$ for all $1 \leq i \leq k$. Thus ϕ is not an injection. Therefore ϕ is not an isomorphism. □