Algebra Homework

Benji Altman

May 27, 2018

Contents

1 Chapter 1

1.1 Section 1

1.1.1 Question 1

Choose $a, b \in S$. We find

$$a = a * b = b * a = b$$

, and thus all elements in S must be the same element, so there is most one element of S.

1.1.2 Question 2

Let us choose $a, b, c \in S$.

(a) We have

$$a * b = a - b = -(b - a) = -(b * a)$$

, thus iff $0 = a * b = a - b$ we have $a * b = b * a$ as $0 = -0$, however for any other value of $a * b$, $a * b \neq b * a$. We also may notice that iff $a = b$, then $a * b = a - b = 0$. Thus for all $a \neq b$, $a * b \neq b * a$.

(b) We have

$$\begin{aligned} a * (b * c) &= a - (b - c) \\ &= a + (c - b) \\ &= a + c - b \\ &= a - b + c \\ &= a - b - (-c) \\ &= (a - b) - (-c) \\ &= (a * b) * -c \end{aligned}$$

so $a * (b * c) = (a * b) * c$ iff $c = -c$ which is only true if $c = 0$.

(c) We have $a * 0 = a - 0 = a$.

(d) We have $a * a = a - a = 0$.

1.2 Section 2

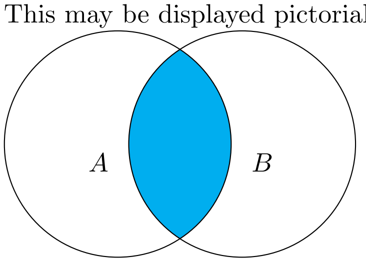
1.2.1 Question 8

Let $x \in (A - B) \cup (B - A)$ then either $x \in A - B$ or $x \in B - A$. If $x \in A - B$ then we get that $x \in A$ and $x \notin B$, thus $x \in A \cup B$ and $x \notin A \cap B$, which would mean $x \in (A \cup B) - (A \cap B)$. If $x \in B - A$ then we get that $x \in B$ and $x \notin A$, thus $x \in A \cup B$ and $x \notin A \cap B$, which would mean $x \in (A \cup B) - (A \cap B)$. It has now been demonstrated that $(A - B) \cup (B - A) \subset (A \cup B) - (B \cap A)$.

Now let $x \in (A \cup B) - (A \cap B)$. We have that $x \in A \cup B$ and $x \notin A \cap B$. It follows that either $x \in A$ or $x \in B$, however, x is not in both A and B. This may be written as: $x \in A$ and $x \notin B$, or $x \in B$ and $x \notin A$. This then translates to $x \in A - B$ or $x \in B - A$, therefore, $x \in (A - B) \cup (B - A)$. It has now been demonstrated that $(A \cup B) - (B \cap A) \subset (A - B) \cup (B - A)$.

Now it has been shown that both sets are subsets of each-other, thus $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$.

This may be displayed pictorially as follows:



1.2.2 Question 9

Let $x \in A \cap (B \cup C)$, thus $x \in A$ and $x \in B \cup C$. We then have that $x \in B$ or $x \in C$. Now as we already know that $x \in A$ then we get that either $x \in B \cap A$ or $x \in C \cap A$ and therefore $x \in (A \cap B) \cup (A \cap C)$. Thus it has been shown that $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$.

Let $x \in (A \cap B) \cup (A \cap C)$, thus $x \in (A \cap B)$ or $x \in (A \cap C)$. We then get that either $x \in A$ and $x \in B$ or that $x \in A$ and $x \in C$, either way $x \in A$, thus we may write that $x \in A$ and either $x \in B$ or $x \in C$. This would be the same as $x \in A$ and $x \in B \cup C$, which then translates to $x \in A \cap (B \cup C)$. Thus it has been shown that $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$.

We have now shown that both sets are subsets of each-other, thus $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

1.2.3 Question 10

Let $x \in A \cup (B \cap C)$, assume then for the sake of contradiction that $x \notin (A \cup B) \cap (A \cup C)$. Because $x \in A \cup (B \cap C)$ we have that $x \in A$ or $x \in B \cap C$. Because $x \notin (A \cup B) \cap (A \cup C)$ we have that $x \notin A \cup B$ or $x \notin A \cup C$. We then get that either $x \notin A$ and $x \notin B$ or $x \notin A$ and $x \notin C$, either way $x \notin A$, so we have $x \in B \cap C$. We know that $x \notin B$ or $x \notin C$, however we also have that $x \in B$ and $x \in C$ due to $x \in B \cap C$, thus we have a contradiction. Thus $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$.

Let $x \in (A \cup B) \cap (A \cup C)$ and assume for the sake of contradiction that $x \notin A \cup (B \cap C)$. We then get that $x \notin A$ and $x \notin B \cap C$. We also have that $x \in A \cup B$ and $x \in A \cup C$, so if $x \notin A$ then we get $x \in B$ and $x \in C$. This is then translated to $x \in B \cap C$ which is a direct contradiction with $x \notin B \cap C$ and again we have a contradiction. Thus $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$.

We have now shown that both sets are subsets of each other, thus $A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$.

1.2.4 Question 12

(a)

$$\begin{aligned}(A \cup B)' &= \{x \in S \,|\, x \notin A \cup B\} \\ &= \{x \in S \,|\, x \notin A \textit{ and } x \notin B\} \\ &= \{x \in S \,|\, x \in A' \textit{ and } x \in B'\} \\ &= A' \cap B'\end{aligned}$$

(b)

$$\begin{aligned}(A \cap B)' &= \{x \in S \,|\, x \notin A \cap B\} \\ &= \{x \in S \,|\, x \notin A \textit{ or } x \notin B\} \\ &= \{x \in S \,|\, x \in A' \textit{ or } x \in B'\} \\ &= A' \cup B'\end{aligned}$$

1.2.5 Question 13

(a)

$$\begin{aligned}A + B &= (A - B) \cup (B - A) \\ &= (B - A) \cup (A - B) \\ &= B + A\end{aligned}$$

(b) First notice that for any set X, $X - \varnothing = A$ and that $\varnothing - X = \varnothing$.

$$\begin{aligned}A + \varnothing &= (A - \varnothing) \cup (\varnothing - A) \\ &= A \cup \varnothing \\ &= A\end{aligned}$$

(c)

$$\begin{aligned}A \cdot A &= A \cap A \\ &= A\end{aligned}$$

(d)

$$\begin{aligned}A + A &= (A - A) \cup (A - A) \\ &= \varnothing \cup \varnothing \\ &= \varnothing\end{aligned}$$

(e) To simplify this question let me introduce the logical operation, $a \oplus b$ which is defined as either a or b but not both, and we will show that $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ using truth tables.

a	b	c	$a \oplus b$	$b \oplus c$	$a \oplus (b \oplus c)$	$(a \oplus b) \oplus c$
False	False	False	False	False	False	False
False	False	True	False	True	True	True
False	True	False	True	True	True	True
False	True	True	True	False	False	False
True	False	False	True	False	True	True
True	False	True	True	True	False	False
True	True	False	False	True	False	False
True	True	True	False	False	True	True

Now we wish to show that $A + B = \{x \in S \,|\, x \in A \oplus x \in B\}$. To do this we will first show that $a \oplus b = (a \wedge \neg b) \vee (b \wedge \neg a)$, where $\neg$ is a logical not, $\wedge$ is a logical and, and $\vee$ is a logical or. We again show this by the following truth table:

a	b	$\neg b$	$a \wedge \neg b$	$\neg a$	$b \wedge \neg a$	$(a \wedge \neg b) \vee (b \wedge \neg a)$	$a \oplus b$
False	False	True	False	True	False	False	False
False	True	False	False	True	True	True	True
True	False	True	True	False	False	True	True
True	True	False	False	False	False	False	False

Now we find

$$\begin{aligned} A + B &= \{x \in S \,|\, x \in A + B\} \\ &= \{x \in S \,|\, x \in (A - B) \cup (B - A)\} \\ &= \{x \in S \,|\, x \in (A - B) \vee x \in (B - A)\} \\ &= \{x \in S \,|\, (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\} \\ &= \{x \in S \,|\, x \in A \oplus x \in B\} \end{aligned}$$

so we then have

$$\begin{aligned} A + (B + C) &= \{x \in S \,|\, x \in A \oplus x \in B + C\} \\ &= \{x \in S \,|\, x \in A \oplus (x \in B \oplus x \in C)\} \\ &= \{x \in S \,|\, (x \in A \oplus x \in B) \oplus x \in C\} \\ &= \{x \in S \,|\, x \in A + B \oplus x \in C\} \\ &= (A + B) + C \end{aligned}$$

(f) Suppose $B \neq C$. Because $B \neq C$ there exists some $x \in S$ such that either $x \in B$ and $x \notin C$ or $x \in C$ and $x \notin B$, we will assume without loss of generality that $x \in B$ and $x \notin C$. Now if $x \in A$ then we would find $x \notin A + B$ and $x \in A + C$. If $x \notin A$ we would find that $x \in A + B$ and $x \notin A + C$. We now have shown that $B \neq C \implies A + B \neq A + C$, thus by contrapositive we have $A + B = A + C \implies B = C$.

(g) First we will want to show logical equivalence between the statement $a \wedge (b \oplus c)$ and $(a \wedge b) \oplus (a \wedge c)$.

a	b	c	$b \oplus c$	$a \wedge b$	$a \wedge c$	$a \wedge (b \oplus c)$	$(a \wedge b) \oplus (a \wedge c)$
False	False	False	False	False	False	False	False
False	False	True	True	False	False	False	False
False	True	False	True	False	False	False	False
False	True	True	False	False	False	False	False
True	False	False	False	False	False	False	False
True	False	True	True	False	True	True	True
True	True	False	True	True	False	True	True
True	True	True	False	True	True	False	False

now we may show

$$\begin{aligned}
A \cdot (B + C) &= A \cap (B + C) \\
&= \{x \in S \,|\, x \in A \cap (B + C)\} \\
&= \{x \in S \,|\, x \in A \wedge x \in (B + C)\} \\
&= \{x \in S \,|\, x \in A \wedge (x \in B \oplus x \in C)\} \\
&= \{x \in S \,|\, (x \in A \wedge x \in B) \oplus (x \in A \wedge x \in C)\} \\
&= \{x \in S \,|\, x \in A \cap B \oplus x \in A \cap C\} \\
&= \{x \in S \,|\, x \in (A \cap B) + (A \cap C)\} \\
&= (A \cap B) + (A \cap C) \\
&= (A \cdot B) + (A \cdot C)
\end{aligned}$$

1.2.6 Question 14

First notice that if A and B are disjoint then $m(A \cup B) = m(A) + m(B)$. So now we get the three disjoint sets $A - B$, $A \cap B$, and $B - A$, notice that $A = (A - B) \cup (A \cap B)$, that $B = (B - A) \cup (A \cap B)$, and $A \cup B = (A - B) \cup (A \cap B) \cup (B - A)$. Now we get $m(A) = m(A - B) + m(A \cap B)$, $m(B) = m(B - A) + m(A \cap B)$, and $m(A \cup B) = m(A - B) + (A \cap B) + m(B - A)$. We then get

$$\begin{aligned}
m(A) + m(B) &= m(A - B) + m(A \cap B) + m(B - A) + m(A \cap B) \\
&= m(A \cup B) + m(A \cap B) \\
m(A) + m(B) - m(A \cap B) &= m(A \cup B)
\end{aligned}$$

1.2.7 Question 22

(a) To construct a subset of any set we go through each element and choose to include it or not to, this gives us two possibilities per element. For a set of size n then there are n independent choices to be made in constructing a subset, thus 2^n subsets.

(b) There are exactly $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ subsets of a set with n elements that have m elements.

Proof. Let us start by defining $\binom{n}{m}$ as the number of ways to choose a subset with m elements from a set with n elements. Now we must recognize that $k!$ is the number of ways to order a set with k elements. Then we get that $\binom{n}{m} m!(n - m)! = n!$ as we may order our set with n elements by choosing the first m elements in our order ($\binom{n}{m}$ possible ways), then ordering those elements ($m!$ ways), and finally ordering the rest of the elements ($(m - n!)$ ways). This gives us $\binom{n}{m} m!(n - m)! = n!$ and from there we divide and get $\binom{n}{m} = \frac{n!}{m!(n-m)!}$. □

1.3 Section 3

1.3.1 Question 7

Let $g : S \to T$, $h : S \to T$ and $f : T \to U$ be functions such that f is 1-1 and $f \circ g = f \circ h$. Assume for the sake of contradiction that $g \neq h$, then there exists some $s \in S$ such that $g(s) \neq h(s)$. We know that $f \circ g(s) = f \circ h(s)$, thus $f(g(s)) = f(h(s))$ so $g(s) = h(s)$ by f being 1-1. Thus we have a contradiction and we know that $g = h$.

1.3.2 Question 8

(a) Yes, as all integers are either even or odd and none are both even and odd.

(b) Let us break this into cases:

- If s_1 and s_2 are even, then there exists $k_1 \in \mathbb{Z}$ and $k_2 \in \mathbb{Z}$ such that $2k_1 = s_1$ and $2k_2 = s_1$. Thus $s_1 + s_2 = 2k_1 + 2k_2 = 2(k_1 + k_2)$, thus $f(s_1 + s_2) = 1$. We also find that $f(s_1) \cdot f(s_2) = 1 \cdot 1 = 1$.

- If s_1 is even and s_2 is odd, then there exists $k_1 \in \mathbb{Z}$ and $k_2 \in \mathbb{Z}$ such that $s_1 = 2k_1$ and $s_2 = 2k_2+1$. Thus $s_1+s_2 = 2k_1+2k_2+1 = 2(k_1+k_2)+1$ so $f(s_1+s_2) = -1$. We also find that $f(s_1)f(s_2) = 1 \cdot -1 = -1$.
- If s_1 is odd and s_2 is even we may write that $f(s_1+s_2) = f(s_2+s_1)$ and that $f(s_1)f(s_2) = f(s_2)f(s_1)$ because both addition and multiplication are commutative. Now we see that we have reproduced our previous case and thus in this case the equality holds.
- If s_1 and s_2 are odd, then there exists $k_1 \in \mathbb{Z}$ and $k_2 \in \mathbb{Z}$ such that $2k_1+1 = s_1$ and $2k_2+1 = s_2$, thus $s_1+s_2 = 2k_1+1+2k_2+1 = 2(k_1+k_2+1)$ so $f(s_1+s_2) = 1$. We also find that $f(s_1)f(s_2) = -1 \cdot -1 = 1$.

Thus for all possible integers s_1 and s_2, we have $f(s_1+s_2) = f(s_1)f(s_2)$.

This tells us that even integers are closed under addition. that odd integers added together always are even, and finally that an odd added to an even is odd.

(c) No, as $f(1 \cdot 2) = f(2) = 1$ and $f(1)f(2) = -1 \cdot 1 = -1$.

1.3.3 Question 12

(a) No f is not a function as $2/3 = 4/6$ and $f(2/3) = 2^2 3^3 \neq 2^4 3^6 = f(4/6)$.

(b) We may define $f(m/n) = 2^m 3^n$ iff m and n are coprime.

1.3.4 Question 19

Let $f(x) = x^2 + ax + b$, thus $f'(x) = 2x + a$. $f'(x)$ is linear so there exists only one $x \in \mathbb{R}$ for which $f'(x) = 0$, and thus this x is a global extrema for f, so f can not be surjective. Now consider $x_1 = -\frac{a}{2} - 1$ and $x_2 = -\frac{a}{2} + 1$, thus

$$\begin{aligned} f(x_1) &= \left(-\frac{a}{2} - 1\right)^2 + a\left(-\frac{a}{2} - 1\right) + b \\ &= \frac{a^2}{4} + 2\frac{a}{2} + 1 - \frac{a^2}{2} - a + b \\ &= \frac{a^2}{4} + 1 + b \\ f(x_2) &= \left(-\frac{a}{2} + 1\right)^2 + a\left(-\frac{a}{2} + 1\right) + b \\ &= \frac{a^2}{4} - 2\frac{a}{2} + 1 - \frac{a^2}{2} + a + b \\ &= \frac{a^2}{4} + 1 + b \end{aligned}$$

so f must be 1-1.

1.3.5 Question 23

Ugly proof: First let us show that there exists some bijection from $\mathbb{N}$ to ${\mathbb{Z}_{\geq 0}}^2$. Consider the 1 norm on ${\mathbb{Z}_{\geq 0}}^2$, defined as $||(a,b)||_1 = a+b$. Then we may partition ${\mathbb{Z}_{\geq 0}}^2$ into subsets $P_n = \left\{x \in {\mathbb{Z}_{\geq 0}}^2 \,\middle|\, ||x||_1 = n\right\}$, for any $n \in \mathbb{Z}_{\geq 0}$. Notice that for $(a,b) \in P_n$ then $a \leq n$ and $b \leq n$, thus forcing P_n to be finite. Now we can construct a function mapping from $\mathbb{N}$ to ${\mathbb{Z}_{\geq 0}}^2$ by giving each element of P_1 a number from 1 to $|P_0|$ (inclusive), then the next $|P_1|$ will be given to elements of P_1 and so on infinitely. Notice that by construction $x \neq y \implies f(x) \neq f(y)$, so we get this being 1-1, additionally for any $(a,b) \in {\mathbb{Z}_{\geq 0}}^2$, $(a,b) \in P_{a+b}$ and thus receives a number greater than $\sum_{n=0}^{a+b-1} |P_n|$ and less than or equal to $\sum_{n=0}^{a+b} |P_n|$. This means that we can label each element of $\mathbb{Z}_{\geq 0}$ with a single natural number and thus have a bijection.

Now we can also construct a trivial bijection, $h : {\mathbb{Z}_{\geq 0}}^2 \to S$ as $h(a,b) = 2^a 3^b$. Now we may compose the bijections to get a 1-1 correspondence $\mathbb{N} = S$ onto T.

Nice proof: First notice that $T \subset S$ so there exists the trivial injective function from T to S. Second notice that $f : S \to T$ defined as $f(s) = 2^s$ is both well defined as injective. By the Schröder-Bernstein theorem there must be some bijection from S to T.

1.3.6 Question 28

Let S be a finite set, with $f : S \to S$. Now let $f(x) = f(y)$, for some $x \neq y$, then there remain $|S| - 2$ elements in $S - \{x, y\}$ and $|S| - 1$ elements in $S - \{f(x)\}$. This means that for any definition of f on $S - \{x, y\}$ it can not possibly be onto $S - \{f(x)\}$. We have now shown f not being 1-1 implies f not being onto, by contrapositive f being onto implies f is 1-1.

1.3.7 Question 29

Let S be a finite set, with $f : S \to S$ injective. Now as f is 1-1 each $s \in S$ has a unique $f(s) \in S$, so $f(S)$ must have exactly $|S|$ unique elements, thus $f(S) \subset S$ with exactly $|S|$ elements.[1] Because S is finite, this implies $f(S) = S$.

1.4 Section 4

1.4.1 Question 5

(a) First identity:

$$\begin{aligned} f^2 g^2 &= ffgg \\ &= f(fg)g \\ &= f(gf)f \\ &= (fg)^2 \end{aligned}$$

(b) Second Identity: Let i be the identity function.

$$\begin{aligned} f^{-1}g^{-1}gf &= i \\ f^{-1}g^{-1}gf(gf)^{-1} &= i(gf)^{-1} \\ = f^{-1}g^{-1}i &= i(fg)^{-1} \\ = f^{-1}g^{-1} &= (fg)^{-1} \end{aligned}$$

1.4.2 Question 9

(a)

$$\begin{aligned} f^2 &: x_1 \to x_3, x_2 \to x_4, x_3 \to x_1, x_4 \to x_2 \\ f^3 &: x_1 \to x_4, x_2 \to x_1, x_3 \to x_2, x_4 \to x_1 \\ f^4 &: x_1 \to x_1, x_2 \to x_2, x_3 \to x_3, x_4 \to x_4 \end{aligned}$$

(b)

$$\begin{aligned} g^2 &: x_1 \to x_1, x_2 \to x_2, x_3 \to x_3, x_4 \to x_4 \\ g^3 &: x_1 \to x_2, x_2 \to x_1, x_3 \to x_3, x_4 \to x_4 \end{aligned}$$

(c)

$$fg : x_1 \to x_3, x_2 \to x_2, x_3 \to x_4, x_4 \to x_1$$

(d)

$$gf : x_1 \to x_1, x_2 \to x_3, x_3 \to x_4, x_4 \to x_2$$

(e)

$$\begin{aligned} (fg)^3 &: x_1 \to x_1, x_2 \to x_2, x_3 \to x_3, x_4 \to x_4 \\ (gf)^3 &: x_1 \to x_1, x_2 \to x_2, x_3 \to x_3, x_4 \to x_4 \end{aligned}$$

(f) No, $fg(x_1) \neq gf(x_1)$ as can be seen above, thus $fg \neq gf$.

[1] $f(A)$ is defined as $\{y \in \boldsymbol{Rng}(f) \mid \exists_{x \in \boldsymbol{Dom}(f)} f(x) = y\}$ when $A \subset \boldsymbol{Dom}(f)$ and $A \notin \boldsymbol{Dom}(f)$.

1.4.3 Question 10

Consider the cycle structure of a permutation f. It is obvious that $f^k = i$ if k is the greatest common divisor among all the cycle lengths in f. Now for any $f \in S_3$, cycles must be of length one, two, or three. Therefore, as $6 = \gcd(1, 2, 3)$ for any $f \in S_3$, $f^6 = i$.

1.4.4 Question 14

Let F be the mapping from $S_m \to S_n$ such that $F(f)$ is defined to be the same as f where f is defined, and acts as the identity elsewhere. Now F is trivially 1-1, so let us show that it satisfies $F(fg) = F(f)F(g)$ for all $f, g \in S_m$. To start let us choose x in the domain of g, then $F(g)$ takes $x \to g(x)$ and $F(f)$ takes $g(x) \to fg(x)$, which is obviously the same as what $F(fg)$ does. If x is not in the domain of g then $F(g)$ takes $x \to x$ and $F(f)$ takes $x \to x$ as does $F(fg)$, we can thus conclude that $F(fg) = F(f)F(g)$.

1.4.5 Question 21

Let g_j swap x_1 and x_{j+1}. Now when $n = 1$ this is trivially true as we have $f = i$ which satisfies the definition of f. Let us now try and do an induction on this statement. Assume that $g_1 g_2 g_3 \cdots g_{n-1} = f$ when n is some specific fixed constant. Then it follows that for $f' \in S_{n+1}$ where f' is defined just as f was, that is $f' : x_1 \to x_2, x_2 \to x_3, \ldots, x_n \to x_{n+1}, x_{n+1} \to x_1$, then consider $g_1 g_2 g_3 \ldots g_n = f g_n$ and this will obviously give us f', so by induction we have shown that this may be done for any n.

1.4.6 Question 27

For every b in the domain of f there must be exactly one a and c such that $f(a) = b$ and $f(b) = c$. As the domain of f is finite then there must be some $n \in \mathbb{N}$ such that $f^n(b) = b$. It follows then that if there is some n such that $f^n(s) = t$ then there must also be some k such that $f^k(t) = s$. By symmetry we also know that the converse is true. This means that either $O(s) = O(t)$ or the two are disjoint.

1.4.7 Question 30

Each orbit must be exactly of size 1. This is because otherwise all n such that $f^n = i$, would have to be a multiple of a number that is not 1, and thus could not be any prime number.

1.4.8 Question 32

$g \in A(S)$ commutes with f iff g is closed on the set $\{x_1, x_2\}$.

Proof. First we will show by cases that any g that is closed on $\{x_1, x_2\}$ commutes with f, then we will show that no other set does so.

- Let $s, t \in \{x_1, x_2\}$ with $s \neq t$
  - If $g(s) = s$, then $fg(s) = g(t) = t$ and $gf(s) = f(s) = t$.
  - If $g(s) = t$, then $fg(s) = g(t) = s$ and $gf(s) = f(t) = s$.
- Let $s \notin \{x_1, x_2\}$, then $fg(s) = gf(s)$ as f acts as the identity.

Now if g is not closed on $\{x_1, x_2\}$ then lets say without loss of generality that $g(x_1) = s \notin \{x_1, x_2\}$ it follows that $fg(x_1) = g(x_2)$ and $gf(x_1) = f(s) = s$. Now $g(x_2) \neq s$ as otherwise both x_1 and x_2 would map to the same element which is not possible. $\square$

1.5 Section 5

1.5.1 Question 1

For this we use the Euclidean algorithm, rather then do the somewhat tedious math, I will simply employ a program I have written in Python.

(a) $(116, -84) = 4 = 8 \cdot 116 + 11 \cdot -84$.

(b) $(85, 65) = 5 = -3 \cdot 85 + 4 \cdot 65$.

(c) $(72, 26) = 2 = 4 \cdot 72 - 11 \cdot 26$.

(d) $(72, 25) = 1, 8 \cdot 72 - 23 \cdot 25$.

1.5.2 Question 4

This shall be nothing but some simple arithmetic, most of these numbers are factorials making them particularly easy to compute.

(a) $36 = 2^2 3^2$.

(b) $120 = 2^3 3^1 5^1$.

(c) $720 = 2^4 3^2 5^1$.

(d) $5040 = 2^4 3^2 5^1 7^1$.

1.5.3 Question 7

(a) First, we write $m = k_1(m, n)$ and $n = k_2(m, n)$ for some $k_1, k_2 \in \mathbb{Z}$. It follows

$$\frac{mn}{(m,n)} = k_1 k_2 (m, n) = m k_2 = n k_1$$

so this satisfies $m|v$ and $n|v$.

Lemma 1.1. *For $n = \prod_{i \in \mathbb{N}} {p_i}^{n_i}$ and $m = \prod_{i \in \mathbb{N}} {p_i}^{m_i}$, if $c_i = \min(n_i, m_i)$ then*

$$(n, m) = \prod_{i \in \mathbb{N}} {p_i}^{c_i}$$

where p_i is the i^{th} prime number.

Proof. For convention we will let p_i be the i^{th} prime unless otherwise stated. We will also adopt the convention that for any natural number x, the sequence x_i will be it's prime factorization, that is $\prod_{i \in \mathbb{N}} {p_i}^{x_i} = x$ unless otherwise stated. Furthermore we will also by convention assume that if a sequence of natural numbers x_i has been defined then $x = \prod_{i \in \mathbb{N}} {p_i}^{x_i}$, unless otherwise stated. As a last note, we will define $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $2 = p_0$.

Let n and m be natural numbers, and then let $c_i = \min n_i, m_i$ for all $i \in \mathbb{N}$. We would like to show $c = (n, m)$. First it is trivial that $c > 0$.

Second we must show $c|n$ and $c|m$. To do this let $k_i = n_i - c_i$, notice that $n_i \geq c_i$ for all i, therefore k_i is an integer for all i.

$$\begin{aligned}
kc &= \prod_{i \in \mathbb{N}} {p_i}^{k_i} \prod_{i \in \mathbb{N}} {p_i}^{c_i} \\
&= \prod_{i \in \mathbb{N}} {p_i}^{n_i - c_i} \prod_{i \in \mathbb{N}} {p_i}^{c_i} \\
&= \prod_{i \in \mathbb{N}} {p_i}^{n_i} \\
&= n
\end{aligned}$$

The same argument can be made to show that $c|m$.

Lastly we must show that if $d|n$ and $d|m$ then $d|c$, we will do this by contrapositive, so assume $d \nmid c$, therefore there does not exist any k st. $dk = c$. Further there exists no sequence of natural numbers k_i st. $d \prod_{i\in\mathbb{N}} {p_i}^{k_i} = c$. We know have

$$\begin{aligned}\prod_{i\in\mathbb{N}} {p_i}^{k_i} \prod_{i\in\mathbb{N}} {p_i}^{d_i} &= \prod_{i\in\mathbb{N}} {p_i}^{d_i+k_i} \\ &\neq \prod_{i\in\mathbb{N}} {p_i}^{c_i}\end{aligned}$$

for any sequence k_i, therefore there must exists some $i \in \mathbb{N}$ st. $d_i > c_i$. It follows then that either $d_i > n_i$ or $d_i > m_i$. $\square$

Now note that $\min(a, b) + \max(a, b) = a + b$ for any a, b. Therefore if we define $v_i = \max(n_i, m_i)$ and $c_i = \min(n_i, m_i)$ we get

$$\begin{aligned}\frac{mn}{(m,n)} &= \frac{\prod_{i\in\mathbb{N}} {p_i}^{m_i} \prod_{i\in\mathbb{N}} {p_i}^{n_i}}{\prod_{i\in\mathbb{N}} {p_i}^{c_i}} \\ &= \prod_{i\in\mathbb{N}} {p_i}^{m_i+n_i-c_i} \\ &= \prod_{i\in\mathbb{N}} {p_i}^{v_i} \\ &= v\end{aligned}$$

Now we just need to show that v is the least common multiple. If $r < v$ and $\prod_{i\in\mathbb{N}} {p_i}^{r_i} = r$, it follows that is some i for which $r_i < v_i$, therefore either m or n can not possibly divide r as either $m_i > r_i$ or $n_i > r_i$.

We now know that $mn/(m, n)$ is the least common multiple of m and n.

(b) As we have already shown $v = \prod_{i\in\mathbb{N}} {p_n}^{\max(n_i,m_i)}$.

1.5.4 Question 13

(a) If $p = 4n$ then p is divisible by four an not prime. If $p = 4n + 2 = 2(2n + 1)$ then p is divisible by two and not odd. Therefore either $p = 4n + 1$ or $p = 4n + 3$.

(b) If $p = 6n$ then p is divisible by six and not prime. If $p = 6n+2 = 2(3n+1)$ then p is divisible by two and not odd. If $p = 6n + 3 = 3(2n + 1)$ then p is divisible by three and is either the number 3 or is not prime. If $p = 6n + 4 = 2(3n + 2)$ then p is divisible by two. Therefore if p is an odd prime that is not 3, then either $p = 6n + 1$ or $p = 6n + 5$.

1.5.5 Question 17

Let p be the n^{th} prime. Assume for the sake of contradiction that there is some $a, b \in \mathbb{N}$ st. $a^2 = pb^2$, and let $\prod_{i\in\mathbb{N}} {p_i}^{a_i} = a$ and $\prod_{i\in\mathbb{N}} {p_i}^{b_i} = b$. It follows that $\prod_{i\in\mathbb{N}} {p_i}^{2a_i} = p \prod_{i\in\mathbb{N}} {p_i}^{2b_i}$. As p is the n^{th} prime then

$$p^{2a_n} \prod_{i\in\mathbb{N}-\{n\}} {p_i}^{2a_i} = p^{2b_n+1} \prod_{i\in\mathbb{N}-\{n\}} {p_i}^{2a_i}$$

so the prime factorizations can not possibly be the same, so we have a contradiction.

1.6 Section 6

1.6.1 Question 1

Proof. Base case, we have $\frac{1}{6}1(1+1)(2\cdot 1+1) = \frac{1}{6}6 = 1 = 1^2$, when $n = 1$. Inductive case we get

$$\begin{aligned}
\frac{1}{6}(n-1)((n-1)+1)(2(n-1)+1)+n^2 &= \frac{1}{6}(n-1)n(2n-1)+n^2 \\
&= \frac{1}{6}\left(2n^3-3n^2+n\right)+n^2 \\
&= \frac{1}{6}\left(2n^3+3n^2+n\right) \\
&= \frac{1}{6}n(2n^2+3n+1) \\
&= \frac{1}{6}n(n+1)(2n+1)
\end{aligned}$$

□

1.6.2 Question 2

Proof. Base case, we have $\frac{1}{4}1^2(1+1)^2 = \frac{1}{4}4 = 1 = 1^3$, when $n = 1$. Inductive case we get

$$\begin{aligned}
\frac{1}{4}(n-1)^2((n-1)+1)^2+n^3 &= \frac{1}{4}n^2(n-1)^2+n^3 \\
&= \frac{1}{4}\left(n^4-2n^3+n^2\right)+n^3 \\
&= \frac{1}{4}\left(n^4+2n^3+n^2\right) \\
&= \frac{1}{4}n^2(n+1)^2
\end{aligned}$$

□

1.6.3 Question 8

Proof. Our base case is trivial when $n = 1$. In our inductive case we get

$$\begin{aligned}
\frac{(n-1)}{n}+\frac{1}{n(n+1)} &= \frac{(n-1)(n+1)+1}{n(n+1)} \\
&= \frac{n^2}{n(n+1)} \\
&= \frac{n}{n+1}
\end{aligned}$$

□

1.6.4 Question 14

Let $n = 0$, then it is trivial that $n^p - n$ is divisible by p for any prime p.

Now let n be a fixed non-negative integer, and assume that $n^p - n$ is divisible by p for any prime p. By the binomial theorem we have

$$\begin{aligned}
(n+1)^p - (n+1) &= \sum_{i=0}^{p} \binom{p}{i} n^i - n - 1 \\
&= \sum_{i=1}^{p-1} \binom{p}{i} n^i + n^p + 1 - n - 1 \\
&= \sum_{i=1}^{p-1} \binom{p}{i} n^i + (n^p - n)
\end{aligned}$$

By our assumption we have $n^p - n$ is divisible by p. Additionally $\binom{p}{i}$ must be divisible by p for all $0 < i < p$ because $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ and p is prime.

By induction we then know that $n^p - n$ is divisible by p for any prime p.

1.7 Section 7

1.7.1 Question 1

(a) $(6-7i)(8+i) = 48 - 56i + 6i + 7 = 55 - 50i$

(b) $(\frac{2}{3} + \frac{3}{2}i)(\frac{2}{3} - \frac{3}{2}i) = \frac{4}{9} + \frac{9}{4} = \frac{16+81}{36} = \frac{97}{36}$

(c) $(6-7i)(8-i) = 48 - 56i - 6i - 7 = 41 - 62i$

1.7.2 Question 2

In general $z^{-1} = \frac{\bar{z}}{|z|^2}$

(a) $z^{-1} = \frac{6}{6^2+8^2} - \frac{8}{6^2+8^2}i$

(b) $z^{-1} = \frac{6}{6^2+8^2} + \frac{8}{6^2+8^2}i$

(c) $z^{-1} = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$

1.7.3 Question 3

Using Lemma 1.7.1, the fact that $\overline{1} = 1$, and some group axioms, we get.

$$\begin{aligned}
1 &= (\overline{z})^{-1}\overline{z} \\
\therefore \overline{1} &= \overline{(\overline{z})^{-1}\overline{z}} \\
&= \overline{(\overline{z})^{-1}} \cdot \overline{(\overline{z})} \\
&= \overline{(\overline{z})^{-1}} \cdot z \\
\therefore z^{-1} &= \overline{(\overline{z})^{-1}} \\
\therefore \overline{z^{-1}} &= \overline{\left(\overline{(\overline{z})^{-1}}\right)} \\
&= (\overline{z})^{-1}
\end{aligned}$$

1.7.4 Question 6

For any $z \in \mathbb{C}$, there exists $a, b \in \mathbb{R}$ such that $z = a + bi$. Now $\overline{z} = a - bi$ by definition. Therefore $z = \overline{z}$ iff $b = 0$ as $a - bi = a + bi$ iff $b = 0$. Finally if $b = 0$ then $z = a$ and therefore z is real, if $b \neq 0$ then $z = a + bi$ for some non-zero $b \in \mathbb{R}$ so z has an imaginary part and is not real. Therefore we have shown that $z = \overline{z}$ iff $z \in \mathbb{R}$.

Now if $a = 0$ the we say that z is purely imaginary as there is no real part to z. So if z is purely imaginary then $z = bi$ and $\overline{z} = -bi = -z$. If we start with $\overline{z} = -z$ then we get

$$\begin{aligned} -(a+bi) &= a - bi \\ -a - bi &= a - bi \\ -a &= a \\ a &= 0 \end{aligned}$$

so z must be purely imaginary. Putting this all together we get that $-z = \overline{z}$ iff z is purely imaginary.

1.7.5 Question 11

(a) $z = \cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}$
(b) $z = 4\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)$
(c) $z = 36\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$
(d) $z = 13\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)$

1.7.6 Question 13

$$\begin{aligned} \left(\frac{1}{2} + \frac{1}{2}\sqrt{3}i\right)^3 &= \left(\frac{1}{2}\left(1 + \sqrt{3}i\right)\right)^3 \\ &= \frac{1}{8}\left(1 + \sqrt{3}i\right)^3 \\ &= \frac{1}{8}\left(1 + 3\sqrt{3}i + 3\left(\sqrt{3}i\right)^2 + \left(\sqrt{3}i\right)^3\right) \\ &= \frac{1}{8}\left(1 + 3\sqrt{3}i - 9 - 3\sqrt{3}i\right) \\ &= \frac{1}{8}(-8) \\ &= -1 \end{aligned}$$

1.7.7 Question 20

Let us adopt the notation that for any $c \in \mathbb{C}$,

$$c = c_a + c_b i$$

where $c_a, c_b \in \mathbb{R}$.

$$\begin{aligned} |z+w|^2 + |z-w|^2 &= |z_a + z_b i + w_a + w_b i|^2 + |z_a + z_b i - w_a - w_b i|^2 \\ &= (z_a + w_a)^2 + (z_b + w_b)^2 + (z_a - w_a)^2 + (z_b - w_b)^2 \\ &= {z_a}^2 + 2z_a w_a + {w_a}^2 + {z_b}^2 + 2z_b w_b + {w_b}^2 + {z_a}^2 - 2z_a w_a + {w_a}^2 + {z_b}^2 - 2z_b w_b + {w_b}^2 \\ &= 2\left({z_a}^2 + {a_b}^2 + {w_a}^2 + {w_b}^2\right) \\ &= 2\left(|z|^2 + |w|^2\right) \end{aligned}$$

1.7.8 Question 21

Our approach here is to partition A into countably many finite sets, this will show that there is a 1-1 and onto correspondence from A to $\mathbb{N}$ as they are both countably infinite. We define $|a+bi|_1 = |a| + |b|$. Now we define the set $Z_k = \{z \in A \,|\, |z| = k\}$ for $k \in \mathbb{N} \cup \{0\}$. Now for all $z \in A$, there exists some $k \in \mathbb{N} \cup \{0\}$ such that $z \in Z_k$ as for any $z \in A$, $z = a + bi$ for $a, b \in \mathbb{Z}$ and therefore $|z| = |a| + |b| \in \mathbb{N} \cup \{0\}$ so there is some $k \in \mathbb{N} \cup \{0\}$ such that $z \in Z_k$. For any $k \in \mathbb{N} \cup \{0\}$ we also have Z_k is finite as for all $a + bi \in Z_k$, $|a| \leq k$ and $|b| \leq k$, therefore there are only finitely many possibilities for a and b. Now we have $\bigcup\limits_{k \in \mathbb{N} \cup \{0\}} Z_k = A$ with each Z_k finite, so A must be countable.

1.7.9 Question 22

First we will prove that $P(\overline{x}) = \overline{P(x)}$ for any polynomial $P : \mathbb{C} \to \mathbb{C}$ with real coefficients, $\alpha_0, \alpha_1, \ldots, \alpha_n$. Let $z \in \mathbb{C}$ such that $z = a + bi$ with a and b real. Notice that for any $\alpha \in \mathbb{R}$,

$$\begin{aligned} \alpha\overline{z} &= \alpha(a - bi) \\ &= \alpha a - \alpha bi \\ &= \overline{\alpha z} \end{aligned}$$

From lemma 1.7.1 we get $\overline{zw} = \overline{z}\,\overline{w}$, so it follows that $\overline{z^n} = \overline{z}^n$. Finally from lemma 1.7.1 we also get $\overline{z + w} = \overline{z} + \overline{w}$ so it follows that $\overline{\sum z_j} = \sum \overline{z_j}$. So if $P(x) = \sum\limits_{j=0}^{n} \alpha_j x^j$ then it follows

$$\begin{aligned} P(\overline{x}) &= \sum_{j=0}^{n} \alpha_j \overline{x}^j \\ &= \sum_{j=0}^{n} \alpha_j \overline{x^j} \\ &= \sum_{j=0}^{n} \overline{\alpha_j x^j} \\ &= \overline{\sum_{j=0}^{n} \alpha_j x^j} \\ &= \overline{P(x)} \end{aligned}$$

Therefore if we have any polynomial P with real coefficients, and $P(x) = 0$ then $P(\overline{x}) = \overline{0} = 0$.

2 Chapter 2

2.1 Section 1

2.1.1 Question 8

Let us start with when $n = 0$, then $(a * b)^n = e = a^n * b^n$.

For $n > 0$ we will do induction, so let us assume that $(a * b)^{n-1} = a^{n-1} * b^{n-1}$, therefore

$$\begin{aligned} (a * b)^n &= (a * b)^{n-1} * (a * b) \\ &= (a^{n-1} * b^{n-1}) * (a * b) \\ &= (a^{n-1} * a) * (b^{n-1} * b) \\ &= a^n * b^n \end{aligned}$$

as we already have the case $n = 0$ this induction proves the statement for $n \geq 0$.

Now assume $n < 0$, therefore $a^n = \left(a^{-1}\right)^{-n}$ and as $a^{-1} \in G$ and $-n > 0$ then we simply refer to our previous work and conclude that the statement still holds.

2.1.2 Question 9

Let $a, b \in G$.

$$\begin{aligned}
e &= (a*b)^2 \\
e &= a^2 \\
e &= b^2 \\
e &= e*e \\
&= a^2*b^2 \\
a^2*b^2 &= (a*b)^2 \\
a*a*b*b &= a*b*a*b \\
a^{-1}*a*a*b*b*b^{-1} &= a^{-1}*a*b*a*b*b^{-1} \\
a*b &= b*a
\end{aligned}$$

2.1.3 Question 19

We simply list off all elements of S_3 as S_3 is small.

$x \in S_3$	Does $x^2 = e$	Does $x^3 = e$
$(1,2,3)$	Yes	Yes
$(1,3,2)$	Yes	No
$(2,1,3)$	Yes	No
$(2,3,1)$	No	Yes
$(3,2,1)$	Yes	No
$(3,1,2)$	No	Yes

2.1.4 Question 20

This is all elements $p \in S_4$ such that there does not exist exactly one x such that $p(x) = x$.

1. $(1,2,3,4)$
2. $(1,2,4,3)$
3. $(2,1,3,4)$
4. $(2,1,4,3)$
5. $(1,4,3,2)$
6. $(3,2,1,4)$
7. $(3,4,1,2)$
8. $(1,3,2,4)$
9. $(4,2,3,1)$
10. $(4,3,2,1)$
11. $(2,3,4,1)$
12. $(2,4,1,3)$
13. $(3,4,2,1)$
14. $(3,1,4,2)$
15. $(4,1,2,3)$
16. $(4,3,1,2)$

2.1.5 Question 26

Let G be a finite group. Assume for the sake of contradiction that there is some $a \in G$ such that for all $n \in \mathbb{N}$, $a^n \neq e$. As G is finite there then must be some $n_1 \neq n_2$ such that $a^{n_1} = a^{n_2}$ by the pigeon hole principle. Let us assume without loss of generality that $n_2 > n_1$, it follows then that $a^{n_1} * a^{-n_1} = a^{n_2} * a^{-n_1}$ and therefore $e = a^{n_2 - n_1}$. This means we have a contradiction and therefore there exists some $n \in \mathbb{N}$ such that $a^n = e$ for any $a \in G$.

2.1.6 Question 27

We already have shown that each element $a \in G$ has some specific n_a such that $a^n = e$. It follows then that if $m = \prod_{a \in G} n_a$ then $a^m = e$ for all $a \in G$.

Proof. Choose $a \in G$ and let $m = \prod_{g \in G} n_g$. Now $a^m = a^{(m/n_a)(n_a)}$, and for notation let $m_a = \frac{m}{n_a}$. We now have

$$\begin{aligned} a^m &= a^{n_a \cdot m_a} \\ &= (a^{n_a})^{m_a} \\ &= e^{m_a} \\ &= e \end{aligned}$$

□

2.1.7 Question 28

First we know that for any $a \in G$ there exists some $a^{-1} \in G$ such that $a^{-1}a = e$ We will adopt this notation as well as simply saying $ab = a * b$ for $a, b \in G$. Now we have

$$\begin{aligned} aa^{-1}aa^{-1} &= aea^{-1} \\ &= aa^{-1} \\ \therefore \left(aa^{-1}\right)^{-1} aa^{-1} &= \left(aa^{-1}\right)^{-1} aa^{-1}aa^{-1} \\ \therefore e &= aa^{-1} \end{aligned}$$

Next we wish to prove some a lemma. If $ab = ac$ then $b = c$

Proof.

$$\begin{aligned} ab = ac &\implies a^{-1}ab = a^{-1}ac \\ &\implies eb = ec \\ &\implies b = c \end{aligned}$$

□

Now with this we can say that for all $a \in G$, there exists exactly one inverse as if $ab = e = ac$, then $b = c$. We also can say an element $a \in G$ is the inverse of exactly one element by the exact same proof.

Finally we get

$$\begin{aligned} aea^{-1} &= aa^{-1} \\ &= e \\ \therefore a^{-1} &= (ea)^{-1} \\ \therefore a &= ea \end{aligned}$$

2.2 Section 2

2.2.1 Question 1

2.2.2 Question 2

2.2.3 Question 5

2.3 Section 3

2.3.1 Question 4

2.3.2 Question 5

2.3.3 Question 11

2.3.4 Question 22

2.3.5 Question 24

2.3.6 Question 26

2.3.7 Question 28

2.3.8 Question 29

2.4 Section 4

2.4.1 Question 1

2.4.2 Question 5

2.4.3 Question 18

2.4.4 Question 24

2.4.5 Question 30

2.4.6 Question 35

2.4.7 Question 37

2.4.8 Question 38

2.4.9 Question 42

2.4.10 Question 43

2.5 Section 5

2.5.1 Question 3

2.5.2 Question 17

2.5.3 Question 18

2.5.4 Question 19

2.5.5 Question 24

2.5.6 Question 26

2.5.7 Question 29

2.5.8 Question 38

2.5.9 Question 42