Algebra Homework

Benji Altman

June 15, 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 $a * a = a - a = 0$.

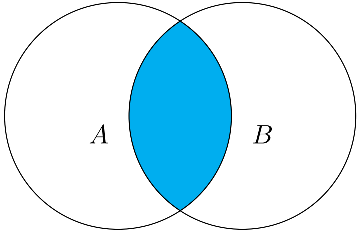
1.2 Section 2

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)

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

[1] $f(A)$ is defined as $\{y \in \boldsymbol{Rng}(f) \,|\, \exists_{x \in \boldsymbol{Dom}(f)} f(x) = y\}$ when $A \subset \boldsymbol{Dom}(f)$ and $A \not\in \boldsymbol{Dom}(f)$.

(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)

$$(fg)^3 : x_1 \to x_1, x_2 \to x_2, x_3 \to x_3, x_4 \to x_4$$
$$(gf)^3 : x_1 \to x_1, x_2 \to x_2, x_3 \to x_3, x_4 \to x_4$$

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

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. □

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

$$\frac{mn}{(m, n)} = k_1 k_2 (m, n) = mk_2 = nk_1$$

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 $d_i > m_i$. □

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 $\prod\limits_{i\in\mathbb{N}} {p_i}^{a_i} = a$ and $\prod\limits_{i\in\mathbb{N}} {p_i}^{b_i} = b$. It follows that $\prod\limits_{i\in\mathbb{N}} {p_i}^{2a_i} = p \prod\limits_{i\in\mathbb{N}} {p_i}^{2b_i}$. 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 $m = \prod\limits_{a \in G} n_a$ then $a^m = e$ for all $a \in G$.

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

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

□

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

Let $a \in G$, therefore there is some $e \in G$ st. $ea = a$ by statement 1. Let $b \in G$ therefore there exists $c \in G$ such that $ca = b$. It follows $be = cae = ca = b$. It has now been shown that there exists $e \in G$ such that for all $x \in G$, $xe = x$.

Now let $a \in G$ then there must exist a $b \in G$ such that $ba = e$. Now we shown that G has the same properties as the set G from Section 1, Question 28, and therefore must be a group.

2.2.2 Question 2

Choose $a \in G$, and let us define $f : G \to G$ as $f(x) = ax$ and $g : G \to G$ as $g(x) = xa$. Now the thing to notice is that f is 1-1 as for any $u, v \in G$ we have $f(u) = au$ and $f(v) = av$, so $av = au$ iff $v = u$. The same statement may be made about g. As f and g are 1-1 on a finite set G we then also have f and g are onto. This means that for any $a, y \in G$ there is some x such that $ax = f(x) = y$ and for any $a, w \in G$ there is some u such that $ua = g(u) = w$. Therefore we have the conditions from Question 1 and can conclude that G is a group.

2.2.3 Question 5

All we need to show that G is abelian is for all $a, b \in G$, $ab = ba$. To start let us choose $a, b \in G$. We know that $a^5b^5 = (ab)^5$ so we get

$$\begin{aligned} a^5b^5 &= (ab)^5 \\ &= a(ba)^4b \\ \therefore a^4b^4 &= (ba)^4 \end{aligned}$$

and we make a similar argument with $a^3b^3 = (ab)^3$ so

$$\begin{aligned} a^3b^3 &= (ab)^3 \\ &= a(ba)^2b \\ \therefore a^2b^2 &= (ba)^2 \end{aligned}$$

We combine these to get that

$$\begin{aligned} a^4b^4 &= (ba)^4 \\ &= \left((ba)^2\right)^2 \\ &= \left(a^2b^2\right)^2 \\ &= a^2b^2a^2b^2 \\ \therefore a^2b^2 &= b^2a^2 \end{aligned}$$

and finally wrap up with

$$\begin{aligned} a^2b^2 &= b^2a^2 \\ &= (ab)^2 \\ \therefore a^2b^2 &= (ab)^2 \\ &= abab \\ \therefore ab &= ba \end{aligned}$$

2.3 Section 3

2.3.1 Question 4

$Z(G)$ is defined as $\{z \in G \,|\, x \in G \,\forall\, zx = xz\}$. First let us choose $a, b \in Z(G)$ therefore for all $x \in G$ we have $ax = xa$ and $bx = xb$. It follows

$$\begin{aligned}(ab)x &= a(bx)\\ &= a(xb)\\ &= (ax)b\\ &= (xa)b\\ &= x(ab)\end{aligned}$$

so $ab \in Z(G)$.

Now choose $a \in Z(G)$, therefore for all $x \in G$, $ax = xa$. It follows then that

$$\begin{aligned}(xa)a^{-1} &= x\\ &= a^{-1}ax\\ &= a^{-1}(xa)\\ xaa^{-1}a^{-1} &= a^{-1}xaa^{-1}\\ \therefore xa^{-1} &= a^{-1}x\end{aligned}$$

and by definition $a^{-1} \in Z(G)$. Now by lemma 2.3.1 $Z(G)$ is a subgroup of G.

2.3.2 Question 5

Let $x \in Z(G)$, it follows that for all $a \in G$, $ax = xa$, so therefore for all $a \in G$, $x \in C(a)$, thus $Z(G) \subset \bigcap\limits_{a \in G} C(a)$. Let $x \in \bigcap\limits_{a \in G} C(A)$, then $xa = ax$ for all $a \in G$, and thus $x \in Z(G)$ and therefore $\bigcap\limits_{a \in G} C(A) \subset Z(G)$. By definition of set equality $Z(G) = \bigcap\limits_{a \in G} C(A)$.

2.3.3 Question 11

Let $a, b \in H$, therefore $a^{n(a)} = e = b^{n(b)}$. Now it follows that

$$\begin{aligned}(ab)^{n(a)\cdot n(b)} &= a^{n(a)n(b)}b^{n(a)n(b)}\\ &= e^{n(b)}e^{n(a)}\\ &= e\end{aligned}$$

thus $ab \in H$.

Let $a \in H$, therefore $a^{n(a)} = e$. It follows that $a^{n(a)-1}a = e$, so $a^{n(a)-1} = a^{-1}$ and as we have already shown H to be closed, then $a^{-1} = a^{n(a)-1} \in H$.

By lemma 2.3.1 it has been demonstrated that H is a subgroup of G.

2.3.4 Question 22

Let us first show that AB is a group. For any $x, y \in AB$, then let $x_a, y_a \in A$ and $x_b, y_b \in B$ such that $x_a x_b = x$ and $y_a y_b = y$. It follows that $xy = x_a x_b y_a y_b = x_a y_a x_b y_b \in AB$ as G is abelian. Now for $x \in AB$ then there exists $a \in A$ and $b \in B$ such that $ab = x$. Therefore $a^{-1} \in A$ and $b^{-1} \in B$ as they are both groups, it then follows that $a^{-1}b^{-1} \in AB$ and $a^{-1}b^{-1}ab = e$ by commutativity, so $a^{-1}b^{-1} = (ab)^{-1}$. Thus it has been shown that AB is a group.

Next we will show that $|AB| = \frac{|A||B|}{|A \cap B|}$.

Let us choose $a \in A$ and $b \in B$ then notice that for all $c \in A \cap B$ then $ac \in A$ and $c^{-1}b \in B$ and therefore $(ac)(c^{-1}b) = ab$. Therefore there are at least as many (a, b) pairs such that ab is equal as there are elements in $A \cap B$. Now assume there is some other $\bar{a} \in A$ and $\bar{b} \in B$ such that there is no $\bar{c} \in A \cap B$ such that $\bar{a}\bar{c} = a$ and $\bar{c}^{-1}\bar{b} = b$. If $\bar{a}\bar{b} = ab$ then $a^{-1}\bar{a} = b\bar{b}^{-1} \in A \cap B$. We will let $\bar{c}^{-1} = b\bar{b}^{-1}$ as we then get $\bar{c}^{-1}\bar{b} = b\bar{b}^{-1}\bar{b} = b$ we then will also find that $\bar{c} = \bar{a}^{-1}a$ and thus $\bar{a}\bar{c} = \bar{a}\bar{a}^{-1}a = a$. Finally we conclude that for any element $ab \in AB$, there exists exactly $|A \cap B|$ pairs $(\bar{a}, \bar{b}) \in A \times B$ such that $ab = \bar{a}\bar{b}$.

Finally if $\bar{A}$ is relatively prime to $\bar{B}$ then $A \cap B = \{e\}$ as for any $a \in A \cap B$ there would be a cyclic set generated by a and that cyclic set's order must divide both A and B. Only if the order is one is this possible so the only element may be the identity element.

2.3.5 Question 24

First we show N to be a group. Let $n, k \in N$, so if we choose $x \in G$ then there exists $h_1 \in H$ such that $n = x^{-1}h_1x$ and $h_2 \in H$ such that $k = x^{-1}h_2x$. It follows that $nk = x^{-1}h_1xx^{-1}h_2x = x^{-1}h_1h_2x$, and therefore is in N as $h_1h_2 \in H$. Now let $n \in N$, and choose $x \in G$ then there exists $h \in H$ such that $n = x^{-1}hx$ then it follows that $n^{-1} = \left(x^{-1}hx\right)^{-1} = x^{-1}h^{-1}x$ and as $h^{-1} \in H$ then $n^{-1} \in N$. This proves N to be a group.

Now let us show that for all $y \in G$, $y^{-1}Ny = N$. Let us choose $n \in N$, and $y \in G$. By $n \in N$ we then choose $x \in G$ and there must exist $h \in H$ such that $n = x^{-1}hx$, then it follows that $y^{-1}ny = y^{-1}x^{-1}hxy$. Now we may choose $z \in G$ and let x be such that $xy = z$ then we find that $y^{-1}x^{-1}hxy = z^{-1}hz$ and therefore $y^{-1}Ny = N$.

2.3.6 Question 26

If there exists $h_1, h_2 \in H$ such that $h_1a = h_2b$ then it follows that $ab^{-1} = {h_1}^{-1}h_2 \in H$. Now for any $\bar{a} \in Ha$ there is some $h \in H$ such that $ha = \bar{a}$. It then must be so that $hab^{-1}b \in B$ as we know that $ab^{-1} \in H$ and as $hab^{-1}b = ha = \bar{a}$ then $Ha \subset Hb$. By symmetry we also know that $Hb \subset Ha$, therefore $Ha = Hb$.

We've now shown if $Ha \cap Hb \neq \varnothing$ then $Ha = Hb$ and otherwise obviously $Ha \cap Hb = \varnothing$.

2.3.7 Question 28

First let us reference the next question as it will prove that $M = x^{-1}Mx$ and $N = x^{-1}Nx$ for all $x \in G$. Now we will proceed to show that MN is a group.

Let $c \in MN$, therefore there is some $a \in M$ and $b \in N$ such that $ab = c$. Now as $N = x^{-1}Nx$ for all $x \in G$ then there exists some $\bar{b} \in N$ such that $a^{-1}\bar{b}a = b$, therefore $ab = aa^{-1}\bar{b}a = \bar{b}a$. We now get inverses as $c^{-1} = a^{-1}\bar{b}^{-1}$ and $a^{-1} \in M$ and $\bar{b}^{-1} \in N$. Now let $d \in MN$ as well, then there is some $m \in M$ and $n \in N$ such that $d = mn$. Now as $m \in M = x^{-1}Mx$ for all $x \in G$ then there is $\bar{m} \in M$ such that $b^{-1}\bar{m}b = m$. It follows that $cd = abmn = abb^{-1}\bar{m}bn = a\bar{m}bn \in MN$ as $a, \bar{m} \in M$ and $b, n \in N$.

Now finally to show that $x^{-1}MNx \subset MN$ for all $x \in G$ we choose $x \in G$ and $d = mn \in MN$ with $m \in M$ and $n \in N$. We then find $x^{-1}mnx = (x^{-1}mx)(x^{-1}nx)$ and of course $x^{-1}mx \in M$ and $x^{-1}nx \in N$.

2.3.8 Question 29

Let $m \in M$ and let $x \in G$. We wish to show the existence of $n \in M$ such that $x^{-1}nx = m$. If we let $x^{-1}nx = m$ then we get $n = xmx^{-1}$ and as $x^{-1} \in G$ and $m \in M$ the we get $n \in x^{-1}Mx \subset M$ so $n \in M$. Now we have shown that $m \in x^{-1}Mx$ and thus $x^{-1}Mx = M$.

2.4 Section 4

2.4.1 Question 1

1. a b for $a, b \in \mathbb{R}$ iff $a - b \in \mathbb{Q}$.

   - **Reflexivity** $a - a = 0 \in \mathbb{Q}$, therefore $a \sim a$.
   - **Symmetry** If $a \sim b$ then $a - b = q \in \mathbb{Q}$, therefore $b - a = -q \in \mathbb{Q}$, so $b \sim a$.
   - **Transitivity** If $a \sim b$ and $b \sim c$ then $a - b = q \in \mathbb{Q}$ and $b - c = p \in \mathbb{Q}$, therefore $a - c = a - b + b - c = q + p \in \mathbb{Q}$, so $a \sim c$.

2. $a \sim b$ for $a, b \in \mathbb{C}$ iff $|a| = |b|$.

    - **Reflexivity** $a \sim a$ is trivial.
    - **Symmetry** If $a \sim b$ then $|a| = |b|$. By symmetry of equality we have $|b| = |a|$ and therefore $a \sim b$.
    - **Transitivity** If $a \sim b$ and $b \sim c$ then $|a| = |b| = |c|$ therefore $|a| = |c|$ so $a \sim c$.

3. $a \sim b$ for lines a, b in the plane if a is parallel to b.

    - **Reflexivity** Any line a is parallel to itself.
    - **Symmetry** If a is parallel to b then b must also be parallel to a.
    - **Transitivity** If a is parallel to b and b is parallel to c then we would also have a parallel to c.

4. $a \sim b$ for people a, b if a's eye color is the same as b's eye color.

    - **Reflexivity** You have the same eye color as yourself.
    - **Symmetry** If $a \sim b$ then a's eye color is b's eye color and therefore b's eye color is a's eye color so $b \sim a$.
    - **Transitivity** If $a \sim b$ and $b \sim c$ then a's eye color is b's eye color and b's eye color is c's eye color then it must be that a's eye color is c's eye color so $a \sim c$.

2.4.2 Question 5

Let us first show that $a \sim b$ is an equivalence relation.

- **Reflexivity** For any $a \in G$, $a^{-1}a = e \in H$ therefore $a \sim a$.
- **Symmetry** For any $a \sim b \in G$ we get $a^{-1}b \in H$. Now $\left(a^{-1}b\right)^{-1} = b^{-1}a$ must also be a member of H, so $b \sim a$.
- **Transitivity** Let $a \sim b$ and $b \sim c$. We get then that $a^{-1}b \in H$ and $b^{-1}c \in H$. It follows then that $\left(a^{-1}b\right)\left(b^{-1}c\right) = a^{-1}c \in H$, so $a \sim c$.

Now we show that $[a] = aH$.

Let $\alpha \in [a]$, therefore $a \sim \alpha$ so $a^{-1}\alpha \in H$. We then get that $aa^{-1}\alpha = \alpha \in aH$, so $[a] \subset aH$.

Now Let $\alpha \in aH$, therefore there is some $h \in H$ such that $\alpha = ah$. It follows then that $a^{-1}\alpha = a^{-1}ah = h \in H$ so $a \sim \alpha$, and therefore $\alpha \in [a]$ so $[a] \supset aH$.

We now conclude $aH = [a]$.

2.4.3 Question 18

Consider the group U_p under multiplication. Notice that for all $0 < n < p$, n is relatively prime to p, so all $0 < n < p$ is included. This yields $p - 1$, an even number of elements so when we multiply them all together we get $(p-1)!$ and from problem 16 we know that this must be some $x \in U_p$ such that $x^2 \equiv 1 \mod p$.

Now there are only two $n \in U_p$ such that $n^2 \equiv 1 \mod p$, $1, -1$. The proof for this is as follows. Obviously $1^2 = (-1)^2 = 1$. Now assume for some $n \in U_p$, $n^2 \equiv 1 \mod p$ therefore $n^2 - 1 = (n+1)(n-1) \equiv 0 \mod p$ so p divides $n+1$ or p divides $n-1$ as p is prime. This leaves only $n \equiv -1 \mod p$ or $n \equiv 1 \mod p$.

Now as only 1^2 and $(-1)^2$ are 1 in U_p we get that every element $x \in U_p$ that is not 1 or -1 has a compliment in U_p, and therefore $(n-1)! \equiv 1 \cdot -1 \mod p$ and this obviously leaves $(n-1) \equiv -1 \mod p$.

2.4.4 Question 24

Let $p = 4n + 3$ and let $\mathbb{Z}/p$ be the set of integers mod p, and further let us adopt the notation that $\mathbb{Z}/p^* = \mathbb{Z}/p - \{0\}$. Now assume $x \in \mathbb{Z}/p$ such that $x^2 \equiv -1 \mod p$. Now we get $x^4 \equiv 1 \mod p$ so $o(x)$ must divide 4, either 1, 2, or 4. If $o(x) = 1$ then $x = 1$ and $x^2 \not\equiv -1 \mod p$ unless $p = 2$ which violates $p = 4n + 3$. If $o(x) = 2$ then $x^2 = 1 \not\equiv -1$ as $p \neq 2$ again. So it must be that $o(x) = 4$. Now $\mathbb{Z}/p^*$ forms a group with order $p - 1$ under multiplication as p is prime, so if $o(x) = 4$ then the cyclic group generated by x would be a subgroup of Z/p^* with order 4. Now $p - 1 = 4n + 2$ which is not divisible by 4 so we have a contradiction due to Lagrange's theorem.

This does overlook if $x = 0$, however then $x^2 = 0 \neq -1$.

2.4.5 Question 30

- $b^2 = aba^4$
- $b^4 = \left(b^2\right)^2 = aba^4aba^4 = ab^2a^4 = a^2ba^3$
- $b^8 = \left(b^4\right)^2 = a^2ba^3a^2ba^3 = a^2b^2a^3 = a^3ba^2$
- $b^{16} = \left(b^8\right)^2 = a^3ba^2a^3ba^2 = a^3b^2a^2 = a^4ba$
- $b^{32} = \left(b^{16}\right)^2 = a^4baa^4ba = a^4b^2a = ebe = b$

So we know $b^{32} = b$, then it follows that $b^{32}b^{-1} = bb^{-1} = e$ so $b^{31} = e$. This means $o(b)$ must be a divisor of 31, however as 31 is prime and we know $o(b) \neq 1$ as $b \neq e$ then $o(b) = 31$.

2.4.6 Question 35

For any permutation we may find it's order by looking at it's cycle structure and taking the least common multiple of all the cycles in the permutation. Now if a permutation has a prime order then it's cycles may either be length 1 or length p, where p is that specific prime. Not all our cycles can be of length p as $|S|$ is not a multiple of p. We conclude there must be some cycle of length 1 and thus some element maps to itself.

2.4.7 Question 37

Let G be a cyclic group of order n with g as a primitive element. Choose m such that m is a divisor of n and choose $k \leq m$ such that $\gcd(k, m) = 1$. It follows that $\left(g^{k\frac{n}{m}}\right)^m = g^{k\frac{n}{m}m} = g^{kn} = e$ so $o\left(g^{k\frac{n}{m}}\right)|m$. Let us assume for the sake of contradiction now that $o\left(g^{k\frac{n}{m}}\right) \neq m$, therefore $o\left(g^{k\frac{n}{m}}\right) < m$. Let then $\bar{m} < m = o\left(g^{k\frac{n}{m}}\right)$, therefore we get $\left(g^{k\frac{n}{m}}\right)^{\bar{m}} = g^{k\frac{n}{m}\bar{m}} = e$ so we get that $k\frac{n}{m}\bar{m} \equiv 0 \mod n$ and therefore there is some $\bar{k}$ such that $k\frac{n}{m}\bar{m} = \bar{k}n$. Dividing by n e get $\frac{k\bar{m}}{m} = \bar{k}n$. We know that k is relatively prime to m so $\frac{\bar{m}}{m}$ is an integer which yields a contradiction as $\bar{m} < m$ and therefore $\frac{\bar{m}}{m} < 1$. This means that for all m divisible by n, and any $k \leq m$ such that $\gcd(k, m) = 1$, we get $o\left(g^{k\frac{n}{m}}\right) = m$.

Next we show that for all a with $0 < a \leq n$ there is some $m|n$ and k with $\gcd(m, k) = 1$ such that $a = \frac{n}{m}k$. For notational sake let for all $x \in \mathbb{N}$, $x = \prod\limits_{i\in\mathbb{N}} {p_i}^{x_i}$, where p_i is the i^{th}. This means that we wish to show that

$$\prod_{i\in\mathbb{N}} {p_i}^{a_i} = \frac{\prod\limits_{i\in\mathbb{N}} {p_i}^{n_i}}{\prod\limits_{i\in\mathbb{N}} {p_i}^{m_i}} \prod_{i\in\mathbb{N}} {p_i}^{k_i}$$

, we may simplify this and show

$$\prod_{i\in\mathbb{N}} {p_i}^{a_i} = \prod_{i\in\mathbb{N}} {p_i}^{n_i - m_i + k_i}$$

and due to properties of primes we need only show that for all $i \in \mathbb{N}$, $a_i = n_i - m_i + k_i$. Now we have the restriction that $m|n$ which simply means that for all $i \in \mathbb{N}$, $m_i \leq n_i$. We also have the restriction that $\gcd(m, k) = 1$ this can be taken to mean there are no prime divisors shared between m and k so $k_i \neq 0 \implies m_i = 0$ and $m_i \neq 0 \implies k_i = 0$ for all $i \in \mathbb{N}$. With these restrictions we can construct m and k. For all $i \in \mathbb{N}$ we follow these rules:

- If $0 \leq a_i \leq n_i$, then let $m_i = n_i - a_i$ and $k_i = 0$, therefore we get $n_i - m_i + k_i = n_i - (n_i - a_i) + 0 = a_i$.
- If $n_i < a_i$ then let $k_i = a_i - n_i$ and $m_i = 0$ therefore we get $n_i - m_i + k_i = n_i - 0 + (a_i - n_i) = a_i$.

Notice also that $k \geq m$ as otherwise $a = \frac{n}{m}k = n\frac{k}{m} < n$ and we know $a \leq n$.

Finally this means that for any $\alpha \in G$ we know that there exists $0 < a \leq n$ such that $g^a = \alpha$ and therefore there is some $m|n$ such that there is a $k \leq m$ where $\gcd(k, m) = 1$ and $\frac{m}{n}k = a$ so $\alpha = g^{\frac{m}{n}k}$ and therefore as we have already shown $o(\alpha) = m$. This means that for all $m|n$ there are exactly $\varphi(m)$ elements $\alpha \in G$ such that $o(\alpha) = m$.

2.4.8 Question 38

Let there be a cyclic group G of order n. One must exist for all $n \in \mathbb{N}$ as the integers mod n under addition are a cyclic group of order n with 1 as their primitive root. For each divisor of m of n there are $\varphi(m)$ elements $\alpha \in G$ such that $o(\alpha) = m$. There can be no elements $\alpha \in G$ such that $o(\alpha)$ does not divide n by Lagrange's theorem so we know that $n = \sum\limits_{m|n} \varphi(m)$.

2.4.9 Question 42

Let $p = 4n + 1$.

$$\begin{aligned}
\frac{p-1}{2}! = \frac{4n}{2}! &= (2n)! \\
&= 1 \cdot 2 \cdots 2n \\
&= (1 \cdot (n+1)) \cdot (2 \cdot (n+2)) \cdots (n \cdot (n+n)) \\
&= (-1 \cdot -(n+1)) \cdot (-2 \cdot -(n+2)) \cdots (-n \cdot -(n+n)) \\
&\equiv ((p-1) \cdot (p-(n+1)) \cdot ((p-2) \cdot (p-(n+2)) \cdots ((p-n) \cdot (p-(n+n))) \mod p \\
&\equiv (p-1) \cdot (p-2) \cdots (p-n) \cdot (p-(n+1)) \cdot (p-(n+2)) \cdots (p-(n+n)) \mod p \\
&\equiv (p-1) \cdot (p-2) \cdots (p-2n) \mod p \\
&\equiv (4n) \cdot (4n-1) \cdots (2n+1) \mod (p = 4n+1) \\
&\equiv \frac{(4n)!}{(2n)!} \mod p \\
\therefore \left(\frac{p-1}{2}!\right)^2 &\equiv (2n)! \cdot \frac{(4n)!}{(2n)!} \mod p \\
&\equiv (4n)! \mod p \\
&\equiv (p-1)! \mod p
\end{aligned}$$

Now by wilson's theorem we may state that if p is prime with $p = 4n + 1$ then $\frac{p-1}{2}! \equiv -1 \mod p$

2.4.10 Question 43

Let G be an abelian group with order n and elements $a_1, a_2, \ldots, a_n$ and let $x = a_1 a_2 \cdots a_n$.

(a) Suppose G has exactly one element $b \neq e$ such that $b^2 = e$. Then it follows that for all elements $g \in G$ with $g \neq b$ and $g \neq e$ we have $g \neq g^{-1}$. This means that every element except b and e has it's inverse in the product that gives us x so this reduces to $x = bee^{\frac{n-1}{2}} = b$.

(b) Consider the $B = \left\{b \in G \,\middle|\, b^2 = e\right\} \subset G$. B is a subgroup of G as for any $a, b \in B$, $(ab)^2 = a^2b^2 = e$ and for any $a \in B$, $a = a^{-1}$. Now for our problem we suppose that $|B| > 2$ and as this is the case we may take some element $b_1 \in B$ and we get a cyclic subgroup $B_1 = \left\{{b_1}^0, {b_1}^1\right\} \subset B$. Now if $B_1 \neq B$ then there exists some $b_2 \in B - B_1$ and this generates $B_2 = \left\{{b_2}^0, {b_2}^1\right\}$ and it follows that $B_1B_2 = \left\{{b_1}^{i_1}{b_2}^{i_2} \,\middle|\, \forall_{k\in\{1,2\}} i_k \in \{0,1\}\right\}$. Now by some sort of induction we will find that $B = B_1B_2 \cdots B_k$ where $B_i = \{e, b_i\}$ and $b_i \notin B_1B_2 \cdots B_{i-1}$ This means that for all $b \in B$, $b = \prod\limits_{r=1}^{k} {b_r}^{i_r}$ with $i_r \in \{0,1\}$ for all r and for all $(i_1, i_2, \ldots, i_k)$ with $i_r \in \{0,1\}$, we get a unique $\prod\limits_{r=1}^{k} {b_r}^{i_r} \in B$. That is to say that $f : \{0,1\}^k \to B$ defined as $f(r) = \prod\limits_{r=1}^{k} {b_r}^{i_r}$ is 1-1 and onto.

This means that if we take the product of all these elements we get

$$\begin{aligned}\prod_{b\in B} b &= \prod_{i\in\{0,1\}^k}\left[\prod_{r=1}^{k} {b_r}^{i_r}\right]\\ &= \prod_{r=1}^{k}\left[\prod_{i\in\{0,1\}^k} {b_r}^{i_r}\right]\\ &= \prod_{r=1}^{k}\left[\left({b_r}^0\right)^{2^{k-1}}\left({b_r}^1\right)^{2^{k-1}}\right]\\ &= \prod_{r=1}^{k} {b_r}^{2^{k-1}}\end{aligned}$$

If $k=1$ we get the result from part (a) where $B=\{b_1,e\}$ and our product simplifies to just b_1. If $k>1$ then we get ${b_r}^{2^{k-1}} = \left({b_r}^2\right)^{2^{k-2}} = e^{2^{k-2}}$. Now for any G we would have $x=\prod_{b\in B} b$ where $B=\left\{g\in G \,\middle|\, g^2=e\right\}$ as all other elements will be paired up with inverses and cancel out. So if there is more than one element in B then we get $x=\prod_{b\in B} b = e$.

(c) If n is odd we get that there can be no subgroup of G with order two, so if there is any element $b\in G$ such that $b=b^{-1}$ we would get the cyclic group B formed by b would be of order two as $b^2=e$. This means that if n is odd all elements in G have an inverse that is not themselves, unless that element is e itself so we end with $x=e$ after everything has canceled out.

2.5 Section 5

2.5.1 Question 3

(a) Let $L_a : G\to G$ be defined as $L_a(x)=xa^{-1}$. Show that $L_a\in A(G)$, this is equivalent to showing that L_a is 1-1 as we already know $L_a : G\to G$.

Let $b,c\in G$ and if $L_a(b)=L_a(b)$ then $ba^{-1}=ca^{-1}$ and it follows by cancellation that $b=c$, therefore L_a is 1-1 and $L_a\in A(G)$

(b) Show that $L_aL_b = L_aL_b$

Let $a,b,x\in G$. It follows that

$$\begin{aligned}L_aL_b(x) &= L_a(L_b(x))\\ &= L_a(xb^{-1})\\ &= xb^{-1}a^{-1}\\ &= x(ab)^{-1}\\ &= L_{ab}(x)\end{aligned}$$

therefore $L_aL_b = L_{ab}$

(c) Let $\psi : G\to A(G)$ be defined as $\psi(a)=L_a$. Show that ψ is a monomorphism.

Proof. We know ψ is a homomorphism as if $a,b\in G$ then $\psi(a)\psi(b)=L_aL_b=L_{ab}=\psi(ab)$.

To show ψ is 1-1 let $a,b\in G$ such that $\psi(a)=\psi(b)$, we then get $L_a=L_b$. If we choose $x\in G$ then

$$\begin{aligned}L_a(x) &= L_b(x)\\ \therefore xa^{-1} &= xb^{-1}\\ \therefore a^{-1} &= b^{-1}\\ \therefore a &= b\end{aligned}$$

so we may conclude that ψ is 1-1 and thus a monomorphism. □

2.5.2 Question 17

We already know that the intersection of subgroups is a group so we simply need show that $M \cap N$ is normal if M and N are normal subgroups of G. This means we need to show that for all $x \in M \cap N$ and for all $g \in G$, $g^{-1}xg \in M \cap N$. Let us start by choosing an arbitrary $x \in M \cap N$ and $g \in G$ We find that $g^{-1}xg \in M$ by the fact that M is normal and $x \in M$ and the same argument goes for $g^{-1}xg \in N$ so $g^{-1}xg \in M \cap N$ and therefore $M \cap N \triangleleft G$.

2.5.3 Question 18

Let H be a subgroup of G and $N = \bigcap\limits_{a \in G} a^{-1}Ha$. We will show that $N \triangleleft G$.

Let $n \in N$, by definition on N we have $\forall_{a \in G} \exists_{h \in H} \left(a^{-1}ha = n\right)$. Now if we choose $g \in G$ and we find that if we choose $a \in H \subset G$ then there exists $h \in H$ such that $n = a^{-1}ha \in H$ and therefore $g^{-1}ng \in N$. We now can conclude that for all $g \in G$, $g^{-1}Ng \subset N$ and therefore $N \triangleleft G$.

2.5.4 Question 19

(a) First let us show $H \subset N(H)$. Let $h \in H$ and $\ell \in H$ then $h^{-1}\ell h \in H$ and therefore $h^{-1}Hh \subset H$. If $\ell \in h^{-1}Hh$ then there is $k \in H$ such that $\ell = h^{-1}Kh \in H$ and therefore $h^{-1}Hh \subset H$. It follows that $h^{-1}Hh = H$ and thus $H \subset N(H)$.

Now let us show that $N(H)$ is a subgroup of G. If $n \in N(H)$ then $n \in a^{-1}Ha$ for all $a \in G$. This implies there is some $h \in H$ such that $n = a^{-1}ha$ and therefore $n^{-1} = \left(a^{-1}ha\right)^{-1} = a^{-1}h^{-1}a$. We then know that for all $n \in N(H)$, $n^{-1} \in N(H)$. If $n, m \in N(H)$ then for any $a \in G$ there is some $h, k \in H$ such that $n = a^{-1}ha$ and $m = a^{-1}ka$ and therefore $nm = a^{-1}haa^{-1}ka = a^{-1}hka$ and as $hk \in H$ then $nm \in N(H)$ so $N(H)$ must be a subgroup of G.

(b) Let us choose an arbitrary $x \in N(H)$, therefore we get $x^{-1}Hx = H$. It follows by definition that $H \triangleleft N$.

(c) Let K be a subgroup of G such that $H \triangleleft K$. If we choose $k \in K$ then we get $k^{-1}Hk = H$ and thus $k \in N(H)$. It follows that $K \subset N(H)$.

2.5.5 Question 24

For notation we will adopt the practice that if $x \in A \times B$ then $x = (x_1, x_2)$ with $x_1 \in A$ and $x_2 \in B$.

(a) Let $a, b \in G = G_1 \times G_2$, therefore $ab = (a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2)$ and as $a_1b_1 \in G_1$ and $a_2b_2 \in G_2$ we get $ab \in G$, so G has closure.

Let $a, b, c \in G$, we find

$$\begin{aligned}
(ab)c &= ((a_1, a_2)(b_1, b_2))(c_1, c_2) \\
&= (a_1b_1, a_2b_2)(c_1, c_2) \\
&= (a_1b_1c_1, a_2b_2c_2) \\
a(bc) &= (a_1, a_2)((b_1, b_2)(c_1, c_2)) \\
&= (a_1, a_2)(b_1c_1, b_2c_2) \\
&= (a_1b_1c_1, a_2b_2c_2) \\
\therefore (ab)c &= a(bc)
\end{aligned}$$

so we have associativity.

Consider (e_1, e_2) where e_1 is the identity of G_1 and e_2 is the identity of G_2. Choose $a \in G$ and we find

$$\begin{aligned} a\left(e_1, e_2\right) &= \left(a_1, a_2\right)\left(e_1, e_2\right) \\ &= \left(a_1 e_1, a_2 e_2\right) \\ &= \left(a_1, a_2\right) \\ &= a \\ \left(e_1, e_2\right) a &= \left(e_1, e_2\right)\left(a_1, a_2\right) \\ &= \left(e_1 a_1, e_2 a_2\right) \\ &= \left(a_1, a_2\right) \\ &= a \end{aligned}$$

therefore we have an identity $e = (e_1, e_2)$.

Let $a \in G$. We find that $a\left({a_1}^{-1}, {a_2}^{-1}\right) = \left(a_1 {a_1}^{-1}, a_2 {a_2}^{-1}\right) = (e_1, e_2) = e$ and $\left({a_1}^{-1}, {a_2}^{-1}\right) a = \left({a_1}^{-1} a_1, {a_2}^{-1} a_2\right) = (e_1, e_2) = e$ and therefore we have inverses with $a^{-1} = \left({a_1}^{-1}, {a_2}^{-1}\right)$.

(b) Let $x, y \in G_1$. We get $\varphi_1(x)\varphi_1(y) = (x, e_2)(y, e_2) = (xy, e_2) = \varphi_1(xy)$, so φ_1 is a homomorphism.

Let $x, y \in G_1$ such that $\varphi_1(x) = \varphi_1(y)$. It follows that $(x, e_2) = (y, e_2)$ and thus $x = y$, so φ_1 is a monomorphism.

(c) Let us define $\varphi_2 : G_2 \to G$ as $\varphi_2(x) = (e_1, x)$. Now we can make the exact same argument to show φ_2 is a monomorphism as we did for φ_1 and thus φ_2 is a monomorphism by symmetry.

(d) It is trivial that $\varphi_1(G_1)\varphi_2(G_2) \subset G$ as G is the co-domain of both φ_1 and φ_2 and additionally G is closed.

Choose $g \in G$, therefore $g = (g_1, g_2)$ with $g_1 \in G_1$ and $g_2 \in G_2$. It follows that $(g_1, g_2) = (g_1 e_1, e_2 g_2) = (g_1, e_2)(e_1, g_2) = \varphi_1(g_1)\varphi_2(g_2)$ and thus $G \subset \varphi_1(G_1)\varphi_2(G_2)$ so $G = \varphi_1(G_1)\varphi_2(G_2)$.

Now consider $(g_1, g_2) \in \varphi_1(G_1) \cap \varphi_2(G_2)$. Now for all $x \in G_1$, $\varphi_1(x) = (x, e_2)$ and thus $g_2 = e_2$. For all $x \in G_2$, $\varphi_2(x) = (e_1, x)$ and thus $g_1 = e_1$ so we have $(g_1, g_2) = e$ for all $(g_1, g_2) \in \varphi_1(G_1) \cap \varphi_2(G_2)$. It follows that $\{e\} = \varphi_1(G_1) \cap \varphi_2(G_2)$.

(e) Let us define $f : G_1 \times G2 \to G_2 \times G_1$ as $f(g) = f((g_1, g_2)) = (g_2, g_1)$. We know $G_1 \times G_2$ is a group and by symmetry $G_2 \times G_1$ must also be a group. Now if we choose $a, b \in G_1 \times G_2$ then we get

$$\begin{aligned} f(a)f(b) &= f((a_1, a_2))f((b_1, b_2)) \\ &= \left(a_2, a_1\right)\left(b_2, b_1\right) \\ &= \left(a_2 b_2, a_1 b_1\right) \\ &= f((a_1 b_1, a_2 b_2)) \\ &= f(ab) \end{aligned}$$

so f is a homomorphism, however we may go a step further as if $f(a) = f(b)$ then we get $f((a_1, a_2)) = f((b_1, b_2))$. By definition of f we get $(a_2, a_1) = (b_2, b_1)$ and therefore we get $a_2 = b_2$ and $a_1 = b_1$ so it must be that $a = b$ yielding f to be a monomorphism. Now we cay say $G_1 \times G_2 \simeq G_2 \times G_1$.

2.5.6 Question 26

(a) Let $a, b, x \in G$ then

$$\begin{aligned} \sigma_a \sigma_b(x) &= \sigma_a(\sigma_b(x)) \\ &= \sigma_a\left(bxb^{-1}\right) \\ &= abxb^{-1}a^{-1} \\ &= (ab)x(ba)^{-1} \\ &= \sigma_{ab}(x) \end{aligned}$$

so it follows that $\psi(a)\psi(b) = \sigma_a\sigma_b = \sigma_{ab} = \psi(ab)$ so ψ is a homomorphism.

Now let us show that $\ker(\psi) = Z(G)$.

First let $x \in Z(G)$, and $a, y \in G$. We then get

$$\begin{aligned}\sigma_y\sigma_x(a) &= yxax^{-1}y^{-1}\\ &= yaxx^{-1}y^{-1}\\ &= yay^{-1}\\ &= \sigma_y(a)\end{aligned}$$

and therefore $\psi(y)\psi(x) = \psi(y)$, thus $x \in \ker(\psi)$ and $Z(G) \subset \ker(\psi)$.

Now let $a \in \ker(\psi)$ It follows then that $\psi(a)\psi(e) = \psi(e)$. Therefore if we choose $x \in G$ we get $\sigma_a\sigma_e(x) = aexe^{-1}a^{-1} = exe^{-1} = \psi(e)$. If we simplify somewhat we get $axa^{-1} = x$ and therefore $ax = xa$. This implies $x \in Z(G)$ and thus $\ker(\psi) \subset Z(G)$.

We are now finished with $Z(G) = \ker(\psi)$.

2.5.7 Question 29

(a) Let $m \in M$ and we must show that for all $a \in G$, $a^{-1}ma \in M$.
We have $T_a(x) = a^{-1}xa$ is an automorphism as

$$\begin{aligned}T_a(x)T_a(y) &= a^{-1}xaa^{-1}ya\\ &= a^{-1}xya & &= T_a(xy)\end{aligned}$$

and if $T_a(x) = T_a(y)$ then $a^{-1}xa = a^{-1}ya$ and thus $x = y$ and for all $x \in G$ $T_a(axa^{-1}) = a^{-1}axa^{-1}a = x$.

It follows that if $m \in M$ then $a^{-1}ma = T_a(m) \in M$ by definition of M and thus $M \triangleleft G$.

(b) If $a \in MN$ then $mn = a$ for some $m \in M$ and $n \in N$. Therefore for any automorphism φ we have $\varphi(a) = \varphi(mn) = \varphi(m)\varphi(n)$ and we know $\varphi(m) \in M$ and $\varphi(n) \in N$ so $\varphi(a) = \varphi(m)\varphi(n) \in MN$. Thus MN is a characteristic subgroup of G.

(c) Let A be a group. We already have shown then that $A \times A = A^2$ is a group when $(a, b)(x, y) = (ax, by)$. We also get that $A \times \{e\}$ is a subgroup of A^2 as for $(a, e) \in A \times \{e\}$, and $(b, e) \in A \times \{e\}$, we have $(a, e)(b, e) = (ab, e) \in A \times \{e\}$ and $\left(a^{-1}, e\right)(a, e) = (e, e)$. Additionally A is normal as for any $a = (x, y) \in G$ and $b = (z, e) \in A \times \{e\}$ we have $a^{-1}ba = \left(x^{-1}, y^{-1}\right)(z, e)(x, y) = \left(x^{-1}zx, y^{-1}ey\right) = \left(x^{-1}zx, e\right) \in A \times \{e\}$. However $A \times \{e\}$ is not a characteristic subgroup of A^2 as for $\phi : A^2 \to A^2$ defined as $\phi((a, b)) = (b, a)$ we get $\phi((a, e)) = (e, a)$ and if $A \neq \{e\}$ then there exists some a for which $(e, a) \notin A \times \{e\}$.

2.5.8 Question 38

(a) Let $a, b \in G$ and $q \in S$ therefore there is some $x \in G$ such that $q = Hx$

$$\begin{aligned}T_aT_b(q) &= T_aT_b(Hx)\\ &= T_a(T_b(Hx))\\ &= T_a(Hxb)\\ &= Hxba\\ &= T_{ba}(Hx)\\ &= T_{ba}(q)\end{aligned}$$

So $T_aT_b = T_{ab}$, so if we define $\psi : G \to A(S)$ as $\psi(x) = T_x$ then we get a homomorphism.

(b) If $x \in \ker(\psi)$ we get $\psi(b) = \psi(ba)$ for all $b \in G$. It follows that $T_b(Hx) = T_{ba}(Hx)$ for all $x \in G$. We then get $Hxb = Hxba$ and therefore $T_a(Hxb) = Hxb$ for all x, b so T_a is the identity if $a \in \ker(\psi)$. We also get the converse as if $T_a(Hx) = Hx = T_e(Hx)$ then $\psi(a) = \psi(e)$.

Further then that we may state that if $x \in \ker(\psi)$ then we get $T_x(Ha) = Ha$ as T_x for all $a \in G$ as is the identity. It follows that $Hax = Ha$ and therefore $Haxa^{-1} = H$. Thus for any $h \in H$ there is $\bar{h} \in H$ such that $haxa^{-1} = \bar{h}$ and thus $axa^{-1} = h^{-1}\bar{h} \in H$. This also implies that $x \in a^{-1}Ha$ for all $a \in G$ and thus $\ker(\psi) \subset \bigcap\limits_{a \in G} a^{-1}Ha$. Now if $x \in \bigcap\limits_{a \in G} a^{-1}Ha$ then $x \in a^{-1}Ha$ for all $a \in G$ and therefore $axa^{-1} \in H$. We now can say that $Haxa^{-1} = H$ and thus $Hax = Ha$ so $T_x(Ha) = Ha$ for any $a \in G$. This means that T_x is the identity and thus $x \in \ker(\psi)$ and we can finish by stating $\ker(\psi) = \bigcap\limits_{a \in G} a^{-1}Ha$

(c) We know $\ker(\psi) = \bigcap\limits_{a \in G} a^{-1}Ha \subset e^{-1}He = H$ so $\ker(\psi)$ is obviously a subset of H. We also know $\ker(\psi) \lhd G$ as it is the kernel of a homomorphism. Now if there is a K such that $K \lhd G$ and $K \subset H$ then for all $k \in K$ and $g \in G$ we have $gkg^{-1} \in K$. It then follows that $gkg^{-1} \in H$, so $k \in g^{-1}Hg$ so $k \in \ker(\psi)$.

2.5.9 Question 42

As we did in the last problem let us define $S = \{Ha \,|\, a \in G\}$ and $T_a : S \to S$ as $T_a(Hx) = Hxa$. We may also define $\psi : G \to A(S)$ as $\psi(a) = T_a$.

Now first we need to show that $|S| = 4$. We know this as we may define $a \sim b$ if $Ha = Hb$. This is nearly trivially an equivalence relation so I won't bother showing that however we will find that $[a] = \{ha \,|\, h \in G\}$. The proof is as follows: Consider $x \in [a]$, it then follows that $Hx = Ha$ so if we choose $h \in H$ then there is some $\bar{h} \in H$ such that $ha = \bar{h}x$ and therefore $a = (h^{-1}\bar{h})x \in \{ha \,|\, h \in H\}$. Consider $x \in \{ha \,|\, h \in H\}$, therefore $x = ha$ for some $h \in H$ and thus $Hx = Hha = Ha$ so $x \sim a$. This means that for each $x \in G$, $|[x]| = |H| = 9$, so there must be 4 equivalence classes and as each equivalence class corresponds to a co-set of H we get 4 co-sets of H.

Now as $|S| = 4$ then it follows that $|A(S)| = 4!$. Now we need a lemma

Lemma 2.1. *Let $f : A \to B$ be a homomorphism. If $\ker(f) = (e)$ then f is a monomorphism.*

Proof. Suppose f is not 1-1, therefore there is some $a \neq b \in A$ such that $f(a) = f(b)$. It follows then that $f(ab^{-1}) = f(a)f(b^{-1}) = f(b)f(b^{-1}) = f(bb^{-1}) = f(e)$ so $ab^{-1} \neq e$ is in $\ker(f)$. Therefore by contrapositive we get if $\ker(f) = (e)$ then f is 1-1. □

We know our function ψ is not a monomorphism as $|G| > |A(S)|$. This means that $\ker(\psi) \neq (e)$. Now the last thing we need to show is $\ker(\psi) \subset H$. We can show this by considering $x \in G - H$ and we find that in order for $x \in \ker(\psi)$ we would expect $\psi(x)\psi(y) = \psi(y)$ for all $y \in G$ which therefore means $T_yT_x(Ha) = T_y(Ha)$ for all $a \in G$. Consider $a = e$ and we get $Hexe = Hee$ so $Hx = H$ and this would mean $x \in H$ contradicting our previous statement. So as we know $\ker(\psi) \subset H$ and $\ker(\psi) \neq (e)$ and we already know that the kernel of a homomorphism is a normal subgroup, so as it is contained in H which is of order 9, then this subgroup must be of order 3 or 9. This concludes our proof that either $H \lhd G$ or there is $N \subset H$ with $|N| = 3$ such that $N \lhd G$.

2.6 Section 6

2.6.1 Question 11

2.6.2 Question 12

2.6.3 Question 13

2.6.4 Question 18

2.7 Section 7

2.7.1 Question 4

2.7.2 Question 5

2.7.3 Question 7

2.8 Section 8

2.8.1 Question 4

2.8.2 Question 6

2.8.3 Question 7

2.8.4 Question 8

2.8.5 Question 11

2.8.6 Question 12

2.9 Section 9

2.9.1 Question 1

2.9.2 Question 2

2.9.3 Question 3