Algebra Homework

Benji Altman

June 30, 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 $(A-B)\cup(B-A) = (A\cup B)-(A\cap B)$.

The pictures I will hand into you separately.

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)

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

(b)

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

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

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

implies $f(S) = S$.

1.4 Section 4

1.4.1 Question 5

(a) First identity:

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

(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 $fg \neq gf$.

1.4.3 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 $\prod_{i\in\mathbb{N}} {p_i}^{a_i} = a$ 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 $\bigcup_{k \in \mathbb{N} \cup \{0\}} Z_k = A$ 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 $P(x) = \sum_{j=0}^{n} \alpha_j x^j$ 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

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 $\{z \in G \mid x \in G \; \forall \; zx = xz\}$. 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 $Z(G) \subset \bigcap_{a \in G} C(a)$. Let $x \in \bigcap_{a \in G} C(A)$, then $xa = ax$ for all $a \in G$, and thus $x \in Z(G)$ and therefore $\bigcap_{a \in G} C(A) \subset Z(G)$. By definition of set equality $Z(G) = \bigcap_{a \in G} C(A)$.

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 $x \in \mathbb{N}$, $x = \prod_{i\in\mathbb{N}} {p_i}^{x_i}$, where p_i is the i^{th}. This means that we wish to show that

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

, 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 $n = \sum_{m|n} \varphi(m)$.

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 $B_1 B_2 = \left\{{b_1}^{i_1} {b_2}^{i_2} \,\middle|\, \forall_{k \in \{1,2\}} i_k \in \{0,1\}\right\}$. Now by some sort of induction we will find that $B = B_1 B_2 \cdots B_k$ where $B_i = \{e, b_i\}$ and $b_i \notin B_1 B_2 \cdots B_{i-1}$ This means that for all $b \in B$, $b = \prod_{r=1}^{k} {b_r}^{i_r}$ 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 $\prod_{r=1}^{k} {b_r}^{i_r} \in B$. That is to say that $f : \{0,1\}^k \to B$ defined as $f(r) = \prod_{r=1}^{k} {b_r}^{i_r}$ 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 $N = \bigcap_{a \in G} a^{-1}Ha$. 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

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

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

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

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

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

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 $\ker(\psi) \subset \bigcap_{a \in G} a^{-1}Ha$. Now if $x \in \bigcap_{a \in G} a^{-1}Ha$ 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 $\ker(\psi) = \bigcap_{a \in G} a^{-1}Ha$

(c) We know $\ker(\psi) = \bigcap_{a \in G} a^{-1}Ha \subset e^{-1}He = H$ so $\ker(\psi)$ is obviously a subset of H. We also know $\ker(\psi) \triangleleft G$ as it is the kernel of a homomorphism. Now if there is a K such that $K \triangleleft G$ 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 $H \triangleleft G$ or there is $N \subset H$ with $|N| = 3$ such that $N \triangleleft G$.

2.6 Section 6

2.6.1 Question 11

Suppose G is a group and let $Z(G) = Z$. It is trivial to show that $Z \triangleleft G$ so suppose further that G/Z is cyclic. As G/Z is cyclic it has some primitive element, $[g]$. Now for any $x, y \in G$ we have $x \in Zg^n$ and $y \in Zg^m$ for some $n, m \in \mathbb{N}$ as all elements are in some coset of Z. We also have then that for some $z, w \in Z$ there is $x = zg^n$ and $y = wg^m$. We now do some manipulation

$$\begin{aligned} xy &= zg^n wg^m \\ &= zwg^n g^m \\ &= wzg^m g^n \\ &= wg^m zg^n \\ &= yz \end{aligned}$$

and we find G is abelian. This means $Z = Z(G) = G$ so $G/Z = (e)$.

2.6.2 Question 12

If G/N is abelian then we get $Nab = Nba$. This means there is some $n, m \in N$ such that $nab = mba$, and it follows that $(nab)^{-1} = (mba)^{-1} = a^{-1}b^{-1}m^{-1}$. We now get that $e = nab(nab)^{-1} = naba^{-1}b^{-1}m^{-1}$ so $n^{-1}m = aba^{-1}b^{-1}$. It follows from N being a subgroup of G that $aba^{-1}b^{-1} \in N$.

2.6.3 Question 13

Let $a, b \in G$. We get $aba^{-1}b^{-1} \in N$, and therefore $[e] = \left[aba^{-1}b^{-1}\right] = [ab]\left[a^{-1}b^{-1}\right]$. It follows then that $[ab] = \left[a^{-1}b^{-1}\right]^{-1} = \left[\left(a^{-1}b^{-1}\right)^{-1}\right] = [ba]$ so G/N is abelian.

2.6.4 Question 18

Choose $a, b \in T$ then $a^n = e$ and $b^m = e$ and therefore $(ab)^{nm} = a^{nm}b^{nm} = e$ so $ab \in T$. Choose $a \in T$ and we get $a^n = e$ so $a^{n-1}a = e$ and thus $a^{n-1} = a^{-1} \in T$. We have now shown that T is a subgroup of G.

Now for any $[a] \in G/T$ if $[a]^n = [e]$ for some $n > 0$ then we would get $Ta^n = T$ and further for some $u, v \in T$, $va^n = u$. Now we if we let $t = v^{-1}u$ then we get $a^n = t \in T$. By definition of T we get $t^m = e$ for some $m > 1$ and thus $(a^n)^m = a^{nm} = e$ so $a \in T$. It follows then that $[a] = [e]$, so only the identity has a finite order in G/T.

2.7 Section 7

2.7.1 Question 4

(a) We know that the kernel of a homomorphism is a normal subgroup, so let us construct $\pi_2 : G \to G_2$ as $\pi_2(a, b) = b$. π_2 is a homomorphism as $\pi_2(a, b)\pi_2(c, d) = ac = \pi_2(ac, bd)$.

Now we will show $\ker(\pi_2) = N$. First let $(x, e_2) \in N$ and $(a, b) \in G$ and therefore $\pi_2(a, b)\pi_2(x, e_2) = be_2 = b = \pi_2(a, b)$ so $N \subset \ker(\pi_2)$. Now let $(x, y) \in \ker(\pi_2)$ and we get $\pi_2(x, y)\pi_2(a, b) = \pi_2(a, b)$ for $(a, b) \in G$. It follows then that $yb = b$ and therefore $y = e_2$ so $\ker(\pi_2) = N$.

(b) Let $\pi_1 : N \to G_1$ be defined as $\pi_1(a, e_2) = a$. We find that $\pi_1(a, e_2)\pi_1(b, e_2) = ab = \pi_1(ab, e_2)$ so it a homomorphism. If $\pi_1(a, e_2) = \pi_1(b, e_2)$ then $a = b$ so π_1 is a monomorphism. If $a \in G_1$ then $\pi_1(a, e_2) = a$ so π_1 is a isomorphism and thus $N \simeq G_1$.

(c) Now let us define $\psi : G/N \to G_2$ as $\psi(N(a, b)) = b$. First we must show that this is a well defined function. Consider $N(a, b) = N(c, d)$, then it follows that $(a, b) = (n, e_2)(c, d)$. We get from this $b = e_2 d = d$ so $\psi(N(a, b)) = b = d = \psi(N(c, d))$. Before we show We get for any $(a, b), (c, d) \in G$, $\psi(N(a, b))\psi(N(c, d)) = bd = \psi(N(a, b)(c, d))$ and therefore ψ is a homomorphism. If $\psi(N(a, b)) = \psi(N(c, d))$ then we get $b = d$. Now if $(x, y) \in N(a, b)$ then $x = na$ and $y = b$ for some $n \in G_1$, and thus $(x, y) \in N(c, d)$ as $x = na = nac^{-1}c$ and $b = d = ed$. This shows that $N(a, b) \subset N(c, d)$ and we get $N(c, d) \subset N(a, b)$ by symmetry so we conclude that if $\psi(N(a, b)) = \psi(N(c, d))$ then $N(a, b) = N(c, d)$ so ψ is a monomorphism. For any $g \in G_2$ I may construct (a, g) with $a \in G_1$ and find that $\psi(N(a, g)) = g$ so ψ is a isomorphism and thus $G_2 \simeq G/N$.

2.7.2 Question 5

(a) We know that $H \cap N$ is a subgroup of H as intersections form subgroups. Now consider $x \in H \cap N$ and $h \in H$. We wish to show that $h^{-1}xh \in H \cap N$. We know that $h^{-1}xh \in N$ as $N \triangleleft G$, and as $h \in H$ and $n \in H$ we get $h^{-1}xh \in H$ so $h^{-1}xh \in H \cap N$ and thus $N \cap H \triangleleft H$.

(b) For $x, y \in HN$ we get $x = h_1n_1$ and $y = h_2n_2$ for some $h_1, h_2 \in H$ and $n_1, n_2 \in N$, so $xy = h_1n_1h_2n_2$. Now $N \triangleleft G$ so for some $\bar{n} \in N$ we get $h_1h_2\bar{n}{h_2}^{-1}h_2n_2 = h_1h_2\bar{n}n_2 \in HN$. For $hn \in HN$ we also have $(hn)^{-1} = n^{-1}h^{-1} = h^{-1}\bar{n}hh^{-1} = h^{-1}\bar{n}$ for some $\bar{n} \in N$. Therefore HN is a subgroup of G.

(c) For all $n \in N$, we have $n = en \in HN$ as $e \in H$, therefore $N \subset HN$. Now as $N \triangleleft G$ and HN is a subgroup of G then $N \triangleleft HN$ is implied by $N \triangleleft G$.

(d) Let us define $Q = H \cap N$. We find $H/Q = \{hQ \mid h \in H\}$ and $HN/N = \{hnN \mid h \in H \wedge n \in N\} = \{hN \mid h \in H\}$. Now we define $\phi : HN/N \to H/Q$ as $\phi(hN) = hQ$. First to show that ϕ is a function let $qN = hN$ with $h, q \in H$. Now choose $qn \in \phi(qN) = qQ$. As $n \in Q$ this implies $n \in N$. As $qn \in qN = hN$ there is some $m \in N$ such that $hm = qn$. We then have $m = h^{-1}qn$ and as all $h, q, n \in H$ we get $m \in H$, and therefore $m \in Q$. It follows then that $qn = hm \in hQ$ and therefore $\phi(qN) = qQ \subset hQ = \phi(hN)$. By symmetry we may make the same argument that $\phi(qN) \supset \phi(hN)$ and therefore ϕ is well defined.

If we take $hN, qN \in HN/N$ we find $\phi(hN)\phi(qN) = (hQ)(qQ) = hqQ = \phi(hqQ)$. If $\phi(hN) = \phi(qN)$ then we find $hQ = qQ$. Now take $hn \in hN$ and as $hQ = qQ$ then there is some $v \in Q$ so that $he = h = qv$ and therefore $hn = qvn = q(vn) \in qN$. By symmetry we also know that for any $qn \in qN$, $qn \in hN$ so $hN = qN$.

Finally for any $hQ \in H/Q$ we know $hN \in HN/N$ so that $\phi(hN) = hQ$ and therefore ϕ is a isomorphism giving $HN/N \simeq H/Q$.

2.7.3 Question 7

Let $\varphi : G \to G'$ be a homomorphism and onto and let $N \triangleleft G$. Choose $a' \in G'$, and $n' \in \varphi(N)$. It follows that for some $a \in G$ and some $n \in N$, $\varphi(a) = a'$ and $\varphi(n) = n'$. Now if $a'^{-1}n'a' \in \varphi(N)$ then $\varphi(N) \triangleleft G$.

$$\begin{aligned} a'^{-1}n'a' &= \varphi(a)^{-1}\varphi(n)\varphi(a) \\ &= \varphi(a^{-1})\varphi(n)\varphi(a) \\ &= \varphi(a^{-1}na) \end{aligned}$$

We know $a^{-1}na \in N$ and therefore $a'^{-1}n'a' \in \varphi(N)$ so $\varphi(N) \triangleleft G'$.

2.8 Section 8

2.8.1 Question 4

Let a and b be elements with order 7 and 3 respectively. It follows that $b^{-1}ab = a^i$ for some $0 \leq i < 7$. We then have

$$\begin{aligned} a &= eae \\ &= b^{-3}ab^3 \\ &= b^{-2}a^ib^2 \\ &= b^{-1}a^{i^2}b \\ &= a^{i^3} \end{aligned}$$

and therefore $i^3 \equiv 1 \mod 7$. If we let $i = 2$ we find that $2^3 = 8 \equiv 1 \mod 7$ and additionally this is consistent with Fermat's little theorem so $2^6 \equiv 1^2 \equiv 1 \mod 7$. We go ahead then and define $b^{-1}ab = a^2$ so $ab = ba^2$. Now consider

$$\begin{aligned} a^nb^m &= a^{n-1}ba^2b^{m-1} \\ &= a^{n-k}ba^{2k}b^{m-1} \\ &= ba^{2k}b^{m-1} \\ &= b^2a^{4n}b^{m-2} \\ &= b^\ell a^{2^\ell n}b^{m-\ell} \\ &= b^m a^{2^m n} \end{aligned}$$

Now we can show that $G = \{a^nb^m \mid n \in \mathbb{Z} \wedge m \in \mathbb{Z}\}$ is closed under this operation.

$$\begin{aligned} a^nb^ma^ob^p &= b^m a^{2^m n+o}b^p \\ &= b^{m+p}a^{2^p(2^m n+o)} \in G \end{aligned}$$

This is a group as it obviously has an identity a^0b^0 and gets inverses from it's closure with $(a^nb^m)^{-1} = b^{-m}a^{-n} = a^0b^{-m}a^{-n}b^0 \in G$. Finally it's order is 21 as we may make the bijection $f(a^nb^m) = (n \mod 7, m \mod 3) \in \mathbb{Z}/7 \times \mathbb{Z}/3$. This is well defined due to the assumed order of a and b in G. It is 1-1 as if $f(a^nb^m) = f(a^ob^p)$ then $n \equiv o \mod 7$ and $m \equiv p \mod 7$ so it follows that $a^nb^m = a^ob^p$. Finally f is onto as for any $(n, m) = f(a^nb^m)$.

2.8.2 Question 6

Consider $|AB|$. From a previous problem we showed that $|AB| = \frac{|A||B|}{|A \cap B|}$. $AB \subset G$ so $|AB| \leq |G|$. From this it follows that $|A \cap B| = \frac{|A||B|}{|AB|} \geq \frac{|A||B|}{|G|} > \frac{|\sqrt{G}||\sqrt{G}|}{|G|} = 1$, so $A \cap B$ must have more than just the identity.

2.8.3 Question 7

We know that $A \cap B$ is a subgroup of both A and B so $|A \cap B| \, |A$ and $|A \cap B| \, |B$ by Lagrange's theorem, which in turn implies that $|A \cap B| = 1$ as $|A|$ relatively prime to $|B|$ and therefore $A \cap B = (e)$. We also know that $|AB| = \frac{|A||B|}{|A \cap B|} = |A| \, |B|$.

2.8.4 Question 8

99 has prime divisors 3 and 11 so there is some element $a \in G$ with $o(a) = 3$ and $b \in G$ with $o(b) = 11$. It follows then that $o(ab) = 33$ so (ab) is a subgroup of G with order 33.

Now we construct as $S = \{(ab)x \, | \, x \in G\}$ and $T_x : S \to S$ as $T_x((ab)y) = (ab)yx$, which we note is in $A(S)$. Now we construct $\psi : G \to A(S)$ as $\psi(x) = T_x$. We get that ψ is homomorphism from our work chapter 2, section 4, and additionally that $|S| = \frac{|G|}{|(ab)|} = 3$. Now ψ is not a monomorphism as it's domain is larger then it's co-domain. We then conclude that $\ker(\psi)$ must be a non-trivial subgroup of G as $\ker(\psi) \neq (e)$ and kernels are always normal subgroups.

2.8.5 Question 11

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 $ab = \bar{a}\bar{b}$.

2.8.6 Question 12

If G is of order 21 then let $a, b \in G$ such that $o(a) = 7$ and $o(b) = 3$ we then know that $b^{-1}ab = a^i$ for some i and from this we get $i^3 \equiv 1 \mod 7$. Well for $i^3 \equiv 1 \mod 7$ we need either $i = 1$, $i = 2$, or $i = 4$. If $i = 1$ then we get $b^{-1}ab = a$ so $ab = ba$ and G is abelian. So either $i = 2$ or $i = 4$. Now consider $c = b^2$, $o(c) = 3$ as we get $(c) = \left\{b^2, b^4 = b^1, b^3 = e\right\}$. In question 4 we found that $a^n b^m = b^m a^{2^m+n}$ and here we find it more generally is $a^n b^m = b^m a^{i^m n}$. If $i = 2$ and we get

$$\begin{aligned} a^n c^m &= a^n b^{2m} \\ &= b^{2m} a^{2^{2m} n} \\ &= b^{2m} a^{\left(2^2\right)^m n} \\ &= c^m a^{4^m n} \end{aligned}$$

and therefore we find that even if we set $i = 2$ then we also have the group that we would get if $i = 4$. This means the two must be isomorphic with the isomorphism $f(a^n b^m) = a^n \left(b^2\right)^m$.

2.9 Section 9

2.9.1 Question 1

Let $f : G_1 \times G_2 \to G_2 \times G_1$ be defined as $f((a, b)) = (b, a)$. We have

$$\begin{aligned} f((a,b))f((c,d)) &= (b,a)\,(d,c) \\ &= (bd, ac) \\ &= f((ac, bd)) \\ &= f((a,b)\,(c,d)) \end{aligned}$$

so f is a homomorphism. We have if $f((a, b)) = f((c, d))$ then $(b, a) = (d, c)$ so $a = c$ and $b = d$, therefore $(a, b) = (c, d)$, so f is a monomorphism. For any $(a, b) \in G_2 \times G_1$ we have $f((b, a)) = (a, b)$ and $(b, a) \in G_1 \times G_2$ by definition so we have f is an isomorphism. Therefore $G_1 \simeq G_2$.

2.9.2 Question 2

Suppose G_1 and G_2 are cyclic groups of order m, n respectively. The group $G_1 \times G_2$ has order mn and therefore to say that $G_1 \times G_2$ is cyclic is equivalent to saying there is some element $(a, b) \in G_1 \times G_2$ with order mn. Now for any $(a, b) \in G_1 \times G_2$ we get $(a, b)^{mn} = (a^{mn}, b^{mn}) = (e, e) = e$, so therefore in order of $G_1 \times G_2$ not to be cyclic we need to show that for all elements there is some $i < mn$ such that $(a, b) = e$. Well this i needs to be such that $n|i$ so that $b^i = e$ and $m|i$ so that $a^i = e$, and $i|ab$ by Lagrange's theorem. This exists if and only if $(m, n) \neq 1$ otherwise stated if and only if m and n are not relatively prime.

2.9.3 Question 3

(a) Consider $f : G \to T$ as $f(a) = (a, a)$. We get $f(a)f(b) = (a, a)(b, b) = (ab, ab) = f(ab)$. If $f(a) = f(b)$ we get $(a, a) = (b, b)$and therefore $a = b$. Finally if $(a, a) \in T$ then $f(a) = (a, a)$ so we know f to be an isomorphism.

(b) First iff G is abelian is $G \times G$ abelian.

Proof. Let G be abelian. It follows then that $(a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b)$ so $G \times G$ so G is abelian implies $G \times G$ is abelian. Let $G \times G$ be abelian. Then as G is isomorphic to the subgroup $\{(g, g) \mid g \in G\}$ we get G being abelian. □

So it follows that if G is abelian then any subgroup is normal including T. If T is a normal subgroup then we get for any $a, b, c \in G$ there exists $d \in G$ such that $(a, b)^{-1}(c, c)(a, b) = (d, d)$. This means From this we get $a^{-1}ca = d = b^{-1}cb$, and further for any $g \in G$, $g^{-1}cg = d$. It logically follows then that $e^{-1}ce = d = c$. Now finally we have $a^{-1}ca = c$ for any $a, c \in G$ and by multiplying a in the front we get $ca = ac$ for any $a, c \in G$ so G is abelian.

2.10 Section 11

2.10.1 Question 3

Let $c \in C\left(x^{-1}ax\right)$. By definition we get $cx^{-1}ax = x^{-1}axc$. It follows from this that $x^{-1}ax = c^{-1}x^{-1}axc = (xc)^{-1}axc$, and therefore $xcx^{-1} \in C(a)$. This means $x^{-1}xcx^{-1}x = c \in x^{-1}C(a)x$ so $C\left(x^{-1}ax\right) \subset x^{-1}C(a)x$. Going the other direction, let $x^{-1}cx \in x^{-1}C(a)x$, so $ca = ac$. We then get $\left(x^{-1}cx\right)\left(x^{-1}ax\right) = x^{-1}cax = x^{-1}acx = \left(x^{-1}ax\right)\left(x^{-1}cx\right)$. This means $x^{-1}cx \in C(x^{-1}ax)$ and we conclude our proof that $C\left(x^{-1}ax\right) = x^{-1}C(a)x$.

2.10.2 Question 4

Let $\varphi(b) \in \varphi(C(a))$ therefore $b \in C(a)$. Now we get $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a)$ so $\varphi(b) \in C(\varphi(a))$, and therefore $\varphi(C(a)) \subset C(\varphi(a))$.

Let $b \in C(\varphi(a))$, and as φ is 1-1 there is some c, such that $\varphi(c) = b$. Now we have $ac = \varphi^{-1}(\varphi(ac))$, which we can do again due to φ being 1-1 and onto. This gives

$$\begin{aligned} ac &= \varphi^{-1}(\varphi(ac)) \\ &= \varphi^{-1}(\varphi(a)\varphi(c)) \\ &= \varphi^{-1}(\varphi(c)\varphi(a)) \\ &= \varphi^{-1}(\varphi(ca)) \\ &= ca \end{aligned}$$

so $c \in C(a)$ and thus $\varphi(c) = b \in \varphi(C(a))$ so we finish with $\varphi(C(a)) = C(\varphi(a))$.

2.10.3 Question 11

For any subgroup H of G we have $H \subset N(H)$ as if we choose $h \in H$ we get $h^{-1}gh \in H$ if $g \in H$ due to closure and we get $g \in H$ if $h^{-1}gh \in H$ as we would have $g = hqh^{-1}$ for some $q \in H$. This simply shows that if P is a p-Sylow subgroup of G then it must also be a subgroup of $N(P)$ and as $N(P)$ is trivially a subgroup of G, by Lagrange's theorem we know if there was some p-Sylow subgroup of $N(P)$ larger then H it would be a subgroup of G and thus P would no longer be a p-Sylow group, so therefore P is a p-Sylow subgroup of H.

let Q be a subgroup of $N(P)$ such that $|Q| = |P| = p^n$ Now consider the set $PQ = \{pq \,|\, p \in P \wedge q \in Q\}$, we wish to show this is a group. Consider $p_1q_1p_2q_2$ with $p_1, p_2 \in P$ and $q_1, q_2 \in Q$. Now $p_1q_1p_2q_2 = p_1\left(q_1p_2{q_1}^{-1}\right)q_1q_2 = p_1p_3q_1q_2$ with $p_3 = q_1p_2{q_1}^{-1}$ and we know $p_3 \in P$ as $Q \subset N(P)$. This shows closure of PQ. Now we get inverses as $(pq)^{-1} = q^{-1}p^{-1} = eq^{-1}p^{-1}e$ and $eq^{-1} \in PQ$ as is $p^{-1}e \in PQ$, considering that we already have PQ is closed we have now shown PQ to be a subgroup of G and as both P and Q are subgroups of $N(P)$ this is also a subgroup of $N(P)$. Finally we consider the size of this group, $|PQ| = \frac{|P||Q|}{|P \cap Q|}$. $|P \cap Q| = p^k$ for some $k \leq n$ as it is a subgroup of both P and Q which have order p^n. $|P|\,|Q| = p^{2n}$, so $|PQ| = p^{2n-k}$. It follows that $k = n$ as otherwise P would not be p-Sylow group. Therefore $|P \cap N| = 2^p$ so $P \cap N = P$. Finally we then conclude that $N = P$ and therefore P is the only p-Sylow subgroup of $N(P)$.

2.10.4 Question 14

Suppose $a \sim b$ if $a^{-1}Pa = b^{-1}Pb$. We get that $\sim$ is an equivalence relation very quickly as

- $a \sim a$ trivial
- $a \sim b \implies a^{-1}Pa = b^{-1}Pb \implies b^{-1}Pb = a^{-1}Pa \implies b \sim a$.
- if $a \sim b$ and $b \sim c$ then $a^{-1}Pa = b^{-1}Pb = c^{-1}Pc$ so $a \sim c$.

Now we may construct equivalence classes $[a] = \{x \in G \,|\, x \sim a\}$, and notice that the question of how many distinct $a^{-1}Pa$ there are is the same as how many equivalence classes there are. Now first consider $[e]$. This is the set of all x such that $x^{-1}Px = e^{-1}Pe = P$. This trivially contains all of P and is in-fact itself a subgroup of G as

- If $a, b \in [e]$ then $a^{-1}Pa = b^{-1}Pb = P$. It follows that $(ab)^{-1}Pab = b^{-1}a^{-1}Pab = b^{-1}Pb = P$ and therefore $ab \in [e]$.
- If $a \in [e]$ then $a^{-1}Pa = P$. It follows then that $aPa^{-1} = aa^{-1}Paa^{-1} = P$ so $a^{-1} \in [e]$.

so this means it's order is a multiple of $|P| = p^n$. Finally we now wish to prove that for all $a, b \in G$, $|[a]| = |[b]|$. To do this we construct a bijection $f_a : [e] \to [a]$ as $f_a(x) = xa$.

First to show this function is well defined. If $x \in [e]$ then $x^{-1}Px = P$ and therefore $(xa)^{-1}Pxa = a^{-1}x^{-1}Pxa = a^{-1}Pa$ so $f_a(x) \in [a]$ and our function is shown to be well defined. Next it is 1-1 as if $f_a(x) = f_a(y)$ then $ax = ay$ and $x = y$. Our function is also onto as if I choose $y \in [a]$ then consider $x = ya^{-1}$, if $x \in [e]$ then we get $f_a(x) = y$ and f_a would be onto. To show $x \in [e]$ we consider $x^{-1}Px = \left(ya^{-1}\right)^{-1}P\left(ya^{-1}\right) = ay^{-1}Pya^{-1}$. We know $y \sim a$ so $y^{-1}Py = a^{-1}Pa$ and therefore $ay^{-1}Pya^{-1} = aa^{-1}Paa^{-1} = P$ so $x \in [e]$. We conclude then that f_a is onto and therefore for any $a \in G$, $|[a]| = |[e]|$. It follows from this that the number of distinct $[a]$ is $\frac{|G|}{|[e]|}$ We know $|G| = p^nm$ and $|[e]| = p^nk$ for some k, we then get the number of distinct equality classes to be $\frac{m}{k}$. Due to m not being divisible by p then $\frac{m}{k}$ must also not be divisible by p as it is a divisor of m. Therefore we conclude that the number of distinct equivalence classes, also the number of distinct $x^{-1}Px$ can not be a multiple of p.

2.10.5 Question 18

Let $a \in N(N(P))$, with P, p-Sylow. It follows that $a^{-1}N(P)a \subset N(P)$. We know $P \subset N(P)$ so $a^{-1}Pa \subset a^{-1}N(P)a \subset N(P)$. Now we have $a^{-1}Pa$ as a p-Sylow subgroup of $N(P)$. $N(P)$ contains only one p-Sylow subgroup, P (as we have already shown in a previous question) so $a^{-1}Pa = P$. Now we have that $a \in N(P)$ and therefore $N(N(P)) \subset N(P)$. We already had $N(P) \subset N(N(P))$ as this is true for any subgroup H of G that $H \subset N(H)$ and $N(P)$ is a subgroup of G. We now conclude $N(N(P)) = N(P)$.

2.10.6 Question 19

Obviously if $|G| = p^n$, then G contains the trivial subgroup of order p^n, itself. Now assume that for some m with $0 \leq m \leq n$ that there is a subgroup of G with order p^m, from this and theorem 2.11.6, we get that there is a subgroup of this group (the one with order p^m) that has order p^{m-1}, so we get G having a subgroup of order p^m implies G has a subgroup of order p^{m-1}. Now we finish by invoking induction and we have shown that for all m, $0 \leq m \leq n$ that G has a subgroup of order p^m.

2.10.7 Question 25

First a lemma from a previous problem that was not assigned.

Lemma 2.2. *Suppose $a \in G$ such that $o(a) = p^m$, and $a^{-1}Pa = P$, with P a p-Sylow subgroup of G then $a \in P$.*

Proof. First we get that for all k, $a^- kPa^k = P$, and it follows that $Pa^k = a^{-k}P$. It follows from this that $(a)P = P(a)$, so let us show that this is a subgroup of G. Any element will have the form $a^k p$, with $p \in P$ so

- $a^{k_1}p_1a^{k_2}p_2 = a^{k_1+k_2}\left(a^{-k_2}p_1a^{k_2}\right)p_2 \in (a)P$.
- $\left(a^k p\right)^{-1} = p^{-1}a^{-m} = a^{-m}\left(a^m p^{-1}a^{-m}\right) \in (a)P$.

so we get $(a)P$ is a group. Now the order of $(a)P$ must be $\frac{|(a)||P|}{|(a)\cap P|} = \frac{p^m p^n}{|(a)\cap P|}$. This must then be in the form p^k for some k, so $k \leq n$ as we have a p-Sylow group of order p^n. Now we then get that $|(a) \cap P| = p^m$ which is the order (a) and thus $(a) \subset P$. □

Now let P and Q be p-Sylow subgroups of G and $Q \neq P$. Consider $a \in P \cap N(Q)$ it follows that $a \in N(Q)$ so $a^{-1}Qa = Q$. By our lemma we have that $a \in Q$ and as $a \in P$ it's order must divide the order of P so we get $a \in Q$. It follows then that $P \cap N(Q) \subset P \cap Q$ and as $P \neq Q$ then $P \cap Q \neq P$. Now $P \cap Q$ is a subgroup of P and as $P \cap N(Q)$ is a subgroup of that we get $P \cap N(Q)$ is a subgroup of P so its order must divide p and not be p^n. Now we get $i_P(N(Q) \cap N) = p^k > 1$, and as $i_G(N(H))$ is the number of double co-sets of H in G we get that the number of double co-sets of Q in P is in the form $p^k > 1$ so must be a multiple of p.

2.10.8 Question 26

Let P be p-Sylow. For any $Q \neq P$ such that Q is p-Sylow we get a multiple of p, kp distinct double co-sets of Q, which in turn are all p-Sylow subgroups of G and are not P. Therefore we get the number of distinct p-Sylow subgroups of G must be 1 plus a multiple of p as we have P and a multiple of p other p-Sylow groups.

2.10.9 Question 28

Suppose H is a subgroup of G with order p^m and further assume that it is not contained in any p-Sylow subgroup of G. Now consider Q, a p-Sylow subgroup of G and let $a \in H \cap N(Q)$ and we find that $a \in Q$ by our lemma 2.2 in my answers (part of question 25). Therefore it follows that $H \cap Q \supset H \cap N(Q)$. Now consider $i_H(H \cap N(Q)) = \frac{p^k}{p^m} \neq 1$ and we know $k \neq p$ as that would imply that $H \subset Q$ and contradict the assumption that it is not contained in a p-Sylow group. Now we find that there is a multiple of p double co-sets for any p-Sylow group, Q and therefore a multiple of p, p-Sylow groups. This contradicts the fact that there is always 1 plus a multiple of p, p-Sylow groups so H must be contained in a p-Sylow group.

3 Chapter 3

3.1 Section 1

3.1.1 Question 1

(a) $(4, 5, 2, 1, 3, 6)$

(b) $(3, 1, 2, 4, 5)$
(c) $(1, 4, 3, 2, 5)$

3.1.2 Question 2

(a)

1. $(2, 3, 4, 5, 6, 1)$
2. $(3, 4, 5, 6, 1, 2)$
3. $(4, 5, 6, 1, 2, 3)$
4. $(5, 6, 1, 2, 3, 4)$
5. $(6, 1, 2, 3, 4, 5)$
6. $(1, 2, 3, 4, 5, 6)$

(b)

1. $(2, 1, 3, 4, 6, 5, 7)$
2. $(1, 2, 3, 4, 5, 6, 7)$

(c)

1. $(6, 4, 5, 2, 1, 3)$
2. $(3, 2, 1, 4, 6, 5)$
3. $(5, 4, 6, 2, 3, 1)$
4. $(1, 2, 3, 4, 5, 6)$

3.1.3 Question 3

Consider $a = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{smallmatrix}\right)$ and $b = \left(\begin{smallmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{smallmatrix}\right)$. We then get $ba = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ b_1 & b_2 & \cdots & b_n \end{smallmatrix}\right)$. So in order for $ba = e$ we need $k = b_k$ for all k. This implies that $a^{-1} = \left(\begin{smallmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 2 & \cdots & n \end{smallmatrix}\right)$.

3.2 Section 2

3.2.1 Question 3

(a) $\begin{pmatrix}1 & 2 & 4\end{pmatrix}\begin{pmatrix}3 & 5 & 7 & 6\end{pmatrix}$ has order 12.
(b) $\begin{pmatrix}1 & 4 & 3 & 2\end{pmatrix}$ has order 4.
(c) $\begin{pmatrix}1 & 4 & 7 & 3 & 6 & 2 & 5\end{pmatrix}$ has order 7.
(d) $\begin{pmatrix}1\end{pmatrix}\begin{pmatrix}2\end{pmatrix}\begin{pmatrix}3\end{pmatrix}$ has order 1.
(e) $\begin{pmatrix}1 & 5 & 7 & 9\end{pmatrix}\begin{pmatrix}2\end{pmatrix}$ has order 4.
(f) $\begin{pmatrix}1 & 4 & 2 & 5 & 3\end{pmatrix}$ has order 5.

3.2.2 Question 9

When $\sigma = \begin{pmatrix}2 & 3\end{pmatrix}$.

3.2.3 Question 12

Let $p = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$ and let $a \in \{1, 2, \ldots, 7\}$ and suppose $\sigma(a) = b$. Now if $a \notin \{1, 2, 3\}$ then it follows that $p(a) = a$, and therefore $\sigma p \sigma^{-1}(b) = \sigma(p(\sigma^{-1}(b))) = \sigma(p(a)) = \sigma(a) = b$. From this we get that for any $\sigma^{-1}(b) \notin \{1, 2, 3\}$ then $\sigma p \sigma^{-1}(b) = b$. Therefore there at most 3 b such that $\sigma p \sigma^{-1}(b) \neq b$, and therefore $\sigma p \sigma^{-1}$ can not be $\begin{pmatrix}1 & 2 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7\end{pmatrix}$.

3.2.4 Question 21

By the fact that σ and τ have no letters in common we get that if $\sigma(a) \neq a$ then $\tau(a) = a$ and if $\tau(a) \neq a$ then $\sigma(a) = a$. Now if $\sigma\tau = e$ then for any a we have $\sigma(\tau(a)) = a$. If for some a, $\tau(a) \neq a$ then $\sigma(a) = a$ and therefore $\sigma(\tau(a)) \neq a$. If for some a, $\sigma(a) \neq a$, then we have $\tau(a) = a$ and therefore $\sigma(\tau(a)) = \sigma(a) \neq a$ so σ and τ must both be the identity.

3.2.5 Question 23

For any of the disjoint cycles a in σ there is a corresponding cycle α with the same length in τ. Now we can think of these cycles as finite sequences simply be choosing one element to fix at the beginning, and it does not mater which we fix, so we can say $a = (a_1, a_2, \ldots, a_k)$ and $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$. Now we can set $p(a_i) = \alpha_i$ and therefore $p\sigma p^{-1}(\alpha_i) = p(\sigma(p^1(\alpha_i))) = p(\sigma(a_i)) = p(a_{i+1}) = \alpha_{i+1}$ as we would want for τ. Note we may need to think mod k in order for this to work as we want $k + 1 = 1$. Now we can construct this for all the cycles and we get $p\sigma p^{-1} = \tau$.

3.2.6 Question 24

Theorem 3.1. *The conjugacy class for any permutation is the set of permutations with the same cycle structure as it.*

Proof. Suppose $f, g \in S_n$ and choose $a \in \{1, 2, \ldots, n\}$. Every permutation is composed of distinct cycles so $g(a)$ is in some cycle in f, $(c_1, c_2, \ldots, c_k)$, so let $g(a) = c_1$ (from this we also get that $a = c_k$). Note also this is a cycle in f, so $f(c_1) = c_2$ and $f(c_i) = c_j$ where $j \equiv i + 1 \mod k$ and $0 < j \leq k$. Now consider

$$\begin{aligned}\left(g^{-1}fg\right)^i(a) &= g^{-1}f^ig(a)\\ &= g^{-1}f^i(c_1)\\ &= g^{-1}(c_i)\end{aligned}$$

therefore if we let $g^{-1}(c_i) = b_i$ we find $g^{-1}fg$ contains a cycle $(b_1, b_2, \ldots, b_k)$. Notice that $g^{-1}fg$ is 1-1 and onto so if $g(\alpha) = c_i$ then $\alpha = b_i$ so cycles in $g^{-1}fg$ map to cycles of the same length in f, therefore $g^{-1}fg$ has the same cycle structure as f. □

From this we find that the conjugacy class for this permutation is the set of all single cycle permutations in S_n.

The centralizer of our permutation is a little easier. If we let $f, g \in S_n$ such that $fg = gf$ then we suppose $(a_1, a_2, \ldots, a_k)$ is a cycle in f then we know $f(a_i) = a_{i+1}$ so $g(a_i) = gf(a_{i-1}) = fg(a_{i-1})$ we then find that f maps $g(a_i) \to g(a_{i+1})$ This means that $(g(a_1), g(a_2), \ldots, g(a_k))$ is a cycle in f.

So for our permutation we are looking for any g such that $g(k) + 1 \equiv g(k + 1) \mod n$. In order for this to be true g must must be a power of f.

3.2.7 Question 25

From our solution to the last problem we know that σ's conjugacy class is the set of all permutations in S_4 with two cycles of size two.

From our solution to the last problem we also know that in order for a permutation $g \in S_4$ to commute with σ we need $f(g(1)) = g(2)$ and $f(g(2)) = g(1)$ and then the same with 3 and 4.

3.3 Section 3

3.3.1 Question 1

(a) even
(b) odd
(c) even
(d) even

3.3.2 Question 3

We have already shown that for any permutation σ it's conjugacy class is the set of permutations with the same cycle structure as it. This means that it must have the same parity.

Another proof is using our homomorphism θ to $\{-1, 1\}$. We have $\theta(\tau^{-1}\sigma\tau) = \theta(\tau)\theta(\sigma)\theta(\tau) = \theta(\tau)\theta(\tau)\theta(\sigma)$ and as in $\{-1, 1\}$ 3very element squared gives the identity 1, we conclude that $\theta(\tau^{-1}\sigma\tau) = \theta(\sigma)$.

3.3.3 Question 5

We must have $4 \to 5$ and $5 \to 4$.

3.3.4 Question 6

A_n is the set of permutations that are written as the product of an even number of transpositions, so let us show that the product of two transpositions can be written as the product of 3-cycles, from this we will get that any element of A_n can be written in such a way as we could decompose a transposition representation into a product of 3-cycles.

Consider $p = \begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix}$ and insist that $a \neq b$ and $c \neq d$. If there is overlap between these two transpositions then the problem becomes nearly trivial. I'll go through all the cases: if there is only one overlap (any of $a = c, b = c, a = d, b = d$ and the remaining pair does not overlap then we have a 3-cycle and this is trivial, if there are two overlaps then we get the identity and this can be written as the product of any 3-cycle with it's inverse, which also will be a 3-cycle. So assume a, b, c, d all to be distinct. Now consider the permutation $\rho = \begin{pmatrix} a & d & c \end{pmatrix}\begin{pmatrix} a & b & c \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix}$.

3.3.5 Question 8

$$\left\{e, \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}\right\}$$

4 Chapter 4

4.1 Section 1

4.1.1 Question 9

Consider $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and suppose that for all 2×2 matrices $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $AB = BA$. We get

$$AB = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix} = BA = \begin{pmatrix} a\alpha + c\beta & b\alpha + d\beta \\ a\gamma + c\delta & b\gamma + d\delta \end{pmatrix}$$

From this we get first by looking in the top left entry that $a\alpha + b\gamma = a\alpha + c\beta$, and therefore $b\gamma = c\beta$. This means that for any γ, β we need some b, c such that this equality holds, and that only happens if $b = c = 0$, so we already figured out half of A. Next look at the entry on the top right and we get $a\beta + b\delta = b\alpha + d\beta$. We already know $b = 0$ so this reduces to $a\beta = d\beta$ and therefore it follows that $a = d$.

So far we have shown that it is necessary for $a = d$ and $b = c = 0$ for our matrix to commute with all 2×2 matrices, so now we need to show this is sufficient. Consider the matrix $A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$ and an arbitrary matrix $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we then have

$$AB = \begin{pmatrix} a\alpha & b\alpha \\ c\alpha & d\alpha \end{pmatrix} = BA$$

so this must be sufficient as well as necessary.

4.1.2 Question 11

(a) Let $x = a + bi \in \mathbb{C}$ and $y = \alpha + \beta i \in \mathbb{C}$. We then get

$$\begin{aligned} F(xy) &= F((a+bi)(\alpha+\beta i)) \\ &= F(a\alpha - b\beta + (a\beta + b\alpha)i) \\ &= a\alpha - b\beta - (a\beta + b\alpha)i \end{aligned}$$

$$\begin{aligned} F(x)F(y) &= F(a+bi)F(\alpha+\beta i) \\ &= (a-bi)(\alpha-\beta i) \\ &= a\alpha - b\beta - (a\beta + b\alpha)i \end{aligned}$$

(b) Remember that by definition $\sqrt{x\overline{x}} = |x|$ for $x \in \mathbb{C}$, and as $F(x) = \bar{x}$ we can use what we proved in the previous part of this question and write $F(x\overline{x}) = F(x)F(\overline{x}) = \overline{x}x = |x|^2$.

(c) Suppose $x = a + bi$ and $y = c + di$. We get $F(x\overline{x})F(y\overline{y}) = |x|^2 |y|^2 = (a^2 + b^2)(c^2 + d^2)$ from part b. We also can say $F(x\overline{x})F(y\overline{y}) = F(xy\overline{xy}) = |xy|^2 = (ac - bd)^2 + (bc + ad)^2$.

4.1.3 Question 13

(a)

$$\begin{aligned} (i+j)(i-j) &= i^2 - ij + ji - j^2 \\ &= -1 - k - k + 1 \\ &= -2k \end{aligned}$$

(b)

$$\begin{aligned} (1 - i + 2j - 2k)(1 + 2i - 4j + 6k) &= 1 + 2 + 8 + 12 + (2 - 1 + 12 - 8)i + (-4 + 2 + 6 - 4)j + (6 - 2 + 4 - 4)k \\ &= 23 + 5i + 4k \end{aligned}$$

(c)

$$\begin{aligned} (2i - 3j + 4k)^2 &= -4 - 9 - 16 + (-12 + 12)i + (8 - 8)j + (-6 + 6)k \\ &= -29 \end{aligned}$$

(d)

$$\begin{aligned} i(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) - (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)i &= \alpha_0 i - \alpha_1 + \alpha_2 k - \alpha_3 j - (\alpha_0 i - \alpha_1 - \alpha_2 k + \alpha_3 j) \\ &= -\alpha_1 + \alpha_0 i - \alpha_3 j + \alpha_2 k + \alpha_1 - \alpha_0 i - \alpha_3 j + \alpha_2 k \\ &= -2\alpha_3 j + 2\alpha_2 k \end{aligned}$$

4.1.4 Question 16

When using our definition for multiplication we find that if we let our solution take the form $\gamma_0 + \gamma_1 i + \gamma_2 j + \gamma_3 k$ then we get $\gamma_0 = {\alpha_0}^2 + {\alpha_1}^2 + {\alpha_2}^2 + {\alpha_3}^2$ and $\gamma_1 = \gamma_2 = \gamma_3 = 0$ as all of these will haver alternating parts that cancel themselves out.

4.1.5 Question 23

For this question let $x = a + bi + cj + dk$ and $y = \alpha + \beta i + \gamma j + \delta k$.

(a)

$$\begin{aligned} x^{**} &= (a - bi - cj - dk)^* \\ &= a + bi + ci + dk \\ &= x \end{aligned}$$

(b)

$$\begin{aligned}(x+y)^* &= (a+\alpha+(b+\beta)i+(c+\gamma)j+(d+\delta)k)^* \\ &= a+\alpha-(b+\beta)i-(c+\gamma)j-(d+\delta)k \\ &= a-bi-ci-dk+\alpha-\beta i-\gamma j-\delta k \\ &= x^*+y^*\end{aligned}$$

(c)

$$\begin{aligned}xx^* &= (a+bi+cj+dk)(a-bi-cj-dk) \\ &= a^2+b^2+c^2+d^2\end{aligned}$$

(see problem 16) Note this is real and non-negative

$$\begin{aligned}x^*x &= (a-bi-cj-dk)(a+bi+cj+dk) \\ &= a^2+b^2+c^2+d^2\end{aligned}$$

(d) As margins in this are rather limiting I will adopt the notation

$$x = a+bi+cj+dk = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

, note that despite this looking like a row vector it is simply a representation of a quaternion, I am going to stick to using this throughout the section and possibly the chapter. If there is any possibility for confusion I will state which is being used.

$$\begin{aligned}(xy)^* &= \begin{bmatrix} a\alpha-b\beta-c\gamma-d\delta \\ a\beta+b\alpha+c\delta-d\gamma \\ a\gamma+c\alpha+d\beta-b\delta \\ a\delta+d\alpha+b\gamma-c\beta \end{bmatrix}^* \\ &= \begin{bmatrix} a\alpha-b\beta-c\gamma-d\delta \\ -a\beta-b\alpha-c\delta+d\gamma \\ -a\gamma-c\alpha-d\beta+b\delta \\ -a\delta-d\alpha-b\gamma+c\beta \end{bmatrix}\end{aligned}$$

$$\begin{aligned}y^*x^* &= \begin{bmatrix} \alpha \\ -\beta \\ -\gamma \\ -\delta \end{bmatrix} \begin{bmatrix} a \\ -b \\ -c \\ -d \end{bmatrix} \\ &= \begin{bmatrix} a\alpha-b\beta-c\gamma-d\delta \\ -a\beta-b\alpha+d\gamma-c\delta \\ -a\gamma-c\alpha+b\delta-d\beta \\ -a\delta-d\alpha+c\beta-b\gamma \end{bmatrix}\end{aligned}$$

and therefore $(xy)^* = y^*x^*$.

4.1.6 Question 36

We know that if some element is a zero-divisor then it does not have an inverse, so all we need to do in order to show that $H(\mathbb{C})$ is not a division ring is to find $a, b \in H(\mathbb{C})$ such that $ab = 0$ and $a \neq 0 \neq b$. We will use

the representation from the previous problem ans write elements of $H(\mathbb{C})$ in the form

$$\begin{bmatrix} a_0 + b_0 i \\ a_1 + b_1 i \\ a_2 + b_2 i \\ a_3 + b_3 i \end{bmatrix}$$

Now consider $a = \begin{bmatrix} 1 \\ i \\ 0 \\ 0 \end{bmatrix}$ and $b = \begin{bmatrix} 1 \\ -i \\ 0 \\ 0 \end{bmatrix}$. We then find

$$\begin{aligned} ab &= \begin{bmatrix} 1-1 \\ -i+i \\ 0 \\ 0 \end{bmatrix} \\ &= 0 \end{aligned}$$

4.1.7 Question 37

Using again the notation from before, consider

$$\begin{aligned} x &= \begin{bmatrix} 0 \\ 3 \\ 4 \\ 5i \end{bmatrix} \\ \therefore x^2 &= \begin{bmatrix} 0^2 - 3^2 - 4^2 - (5i)^2 \\ 2 \cdot 0 \cdot 3 \\ 2 \cdot 0 \cdot 4 \\ 2 \cdot 0 \cdot 5i \end{bmatrix} \\ &= \begin{bmatrix} 5^2 - 3^2 + 4^2 \\ 0 \\ 0 \\ 0 \end{bmatrix} \\ &= 0 \end{aligned}$$

4.2 Section 2

4.2.1 Question 2

Let R be an integral domain ring and let $a, b, c \in R$ such that $ab = ac$ and $a \neq 0$.

$$\begin{aligned} ab &= ac \\ ab - ab &= ac - ab \\ 0 &= a(c - b) \\ c - b &= 0 \\ c &= b \end{aligned}$$

We also get this from $ba = ca$ by doing analogous operations from the right.

4.2.2 Question 3

Consider some element of R, $\alpha \neq 0$ and we find first that all powers of α are not 0 by the integral domain axioms and second that as R is finite there is some $n > k > 0$ such that $\alpha^n = \alpha^k$ and therefore $\alpha^{n-k}\alpha^k = \alpha^k$.

Now let us relabel a bit and suppose $a = \alpha^{n-k}$ and $b = \alpha^k = \alpha^n$. Now $aab = a(ab) = ab$ so we can infer from what we proved in the previous question that $aa = a$. Now let $c \in R$ and we find $ac = aac$ and thus $c = ac$ and from the other side $ca = caa$ so $c = ca$. From this we can infer that $a = 1$, and thus R has a unit. Next we need inverses on our multiplication. Now for every α we have some $n(\alpha) > 1$ such that $\alpha^{n(\alpha)} = 1$, therefore it follows that $\alpha^{n(\alpha)-1}\alpha = \alpha\alpha^{n(\alpha)-1} = 1$ and therefore for any α, we have $\alpha^{-1} = \alpha^{n(\alpha)-1}$. Finally we get commutativity from the fact that R is an integral domain so we can now conclude that we have a commutative division ring, and thus a field.

4.2.3 Question 7

We know from lemma 4.2.1 that $(-a)(-b) = ab$ in any ring and therefore it follows that $(-a)^4 = a^4$, so in our ring R we get for any $r \in R$, $r = r^4 = (-r)^4 = -r$. From this we get that $r + r = 0$. Now notice that in R if we have $a^n = 0$ then $a = 0$, as $a^n = a^k$ for $k \equiv n \mod 3$ and $1 \leq k < 4$ so either $a^1 = a = 0$, $a^2 = 0$ which means that $a = a^4 = 0 \cdot a^{4-k} = 0$ so $a = 0$. Now consider an element in $t \in R$ such that $t^2 = t$ and choose $l \in R$. We find

$$\begin{aligned}(tl - tlt)^2 &= (tl)^2 - (tl)(tlt) - (tlt)(tl) + (tlt)^2 \\ &= tltl - tltlt - tlt^2l + tlt^2lt \\ &= tltl - tltl - tltlt + tltlt \\ &= 0\end{aligned}$$

and

$$\begin{aligned}(lt - tlt)^2 &= (lt)^2 - (lt)(tlt) - (tlt)(lt) + (tlt)^2 \\ &= ltlt - lt^2lt - tltlt + tlt^2lt \\ &= ltlt - ltlt - tltlt + tltlt \\ &= 0\end{aligned}$$

From this we find that $tl - tlt = 0$ and $lt - tlt = 0$ and so we can conclude that $tlt = -tl$ and $tlt = -lt$ so $lt = tl$. So from this we know that for any $x, y \in R$, $(x^2 + x)y = y(x^2 + x)$. From this we may choose $x, y \in R$ and we would find $z((x^2 + y)^2 + (x^2 + y)) = ((x^2 + y)^2 + (x^2 + y))z$ for all $z \in R$. We may expand out $(x^2 + y)^2 + (x^2 + y)$ and get

$$\begin{aligned}(x^2 + y)^2 + x^2 + y &= x^4 + x^2y + yx^2 + y^2 + x^2 + y \\ &= x + x^2y + yx^2 + y^2 + x^2 + y \\ &= (x^2 + x) + (y^2 + y) + (x^2y + yx^2)\end{aligned}$$

and it follows then that

$$\begin{aligned}z((x^2 + y)^2 + (x^2 + y)) &= ((x^2 + y)^2 + (x^2 + y))z \\ \therefore z((x^2 + x) + (y^2 + y) + (x^2y + yx^2)) &= ((x^2 + x) + (y^2 + y) + (x^2y + yx^2))z \\ z(x^2 + x) + z(y^2 + y) + z(x^2y + yx^2) &= (x^2 + x)z + (y^2 + y)z + (x^2y + yx^2)z \\ &= z(x^2 + x) + z(y^2 + y) + (x^2y + yx^2)z \\ \therefore z(x^2y + yx^2) &= (x^2y + yx^2)z\end{aligned}$$

And now finally if we let $z = x^2$ we get

$$\begin{aligned}x^2(x^2y + yx^2) &= (x^2y + yx^2)x^2 \\ x^4y + x^2yx^2 &= x^2yx^2 + yx^4 \\ \therefore xy &= yx\end{aligned}$$

and thus we conclude that R is commutative.

4.2.4 Question 9

First we try and do our sum the traditional way, without simplification and we get

$$\sum_{n=1}^{p-1} \frac{1}{n} = \frac{\sum\limits_{n=1}^{p-1} (p-1)!\frac{1}{n}}{(p-1)!}$$

and we can let $a = \sum\limits_{n=1}^{p-1} (p-1)!\frac{1}{n}$ and $b = (p-1)!$. Now notice that if $p|a$ so mus the simplified form of the fraction's numerator as that would be $\frac{a/\gcd(a,b)}{b/\gcd(a,b)}$ and b is not a multiple of p due to p being prime so $p \not| \gcd(a,b)$ and therefore $p|\frac{a}{\gcd(a,b)}$. Further any possible numerator in a fraction equaling $\frac{a}{b}$ would be a multiple of the simplified forms fractions so if $p|a$ then p must always divide the numerator of this fraction. Next we know that $(p-1)! \equiv -1 \mod p$ as every element has an inverse other than itself which cancels itself out except 1 and $p-1$ who's inverses are themselves. When we do divide this then by some n with $0 < n < p$ then we get $(p-1)! \equiv -[n]^{-1}$, so when we take the sum we get

$$\sum_{n=1}^{p-1} (p-1)!\frac{1}{n} \equiv \sum_{n=1}^{p-1} -[n]^{-1}$$

Each negative inverse just simply becomes a separate element in $\mathbb{Z}/p$ and still never the 0 element as it has no inverse and is it's own negative, therefore this simply is the sum $\sum\limits_{n=1}^{p-1} [n]$ with a different ordering. Now $\mathbb{Z}/p$ is a field so each element has it's additive inverse in the sum and there are no elements a such that $a + a = 0$ with the exception of 0 then we can use each element to cancel it's negative out and we get

$$\sum_{n=1}^{p-1} (p-1)!\frac{1}{n} \equiv [0]$$

and otherwise stated $a \equiv 0 \mod p$ so $p|a$ and we are done.

4.3 Section 3

4.3.1 Question 3

Choose $a \in R$ then we get $1a = a = a1$ and therefore $\varphi(1a) = \varphi(a) = \varphi(a1)$ and we conclude with $\varphi(1)\varphi(a) = \varphi(a) = \varphi(a)\varphi(1)$ so $\varphi(1)$ is the unit of R'.

4.3.2 Question 4

If $x, y \in I + J$ then $x = a + c$ and $y = b + d$ for some $a, b \in I$ and $c, d \in J$ therefore $x + y = a + c + b + d = a + b + c + d \in I + J$ so we have closure under addition. If $x \in I + J$ then $x = i + j$ for some $i \in I$ and $j \in J$, therefore $-x = -(i + j) = -i + (-j) \in I + J$ so we have additive inverses. From this we already know that $I + J$ is an additive subgroup of R. Now consider $r \in R$ and $a \in I + J$. As $a \in I + J$ there is some $i \in I$ and $j \in J$ such that $a = I + J$. Now we have $ra = r(i + j) = ri + rj \in I + J$ and $ar = (i + j)r = ir + ij \in I + J$. From this we conclude that $I + J$ is an ideal of R.

4.3.3 Question 17

(a) In order to show that some set A is a subring of some ring B we need to show

1. $A \subset B$
2. $a, b \in A \implies a + b \in A$
3. $a \in A \implies -a \in A$

4. $a, b \in A \implies ab \in A$

$A + I \subset R$ is trivial. For any $x, y \in A + I$, $x = a + i$ and $y = b + j$ for some $a, b \in A$ and $i, j \in I$. From this we get $x + y = a + i + b + j = (a + b) + (i + j) \in A + I$ so we get item 2. We also have $xy = (a+i)(b+j) = ab+aj+ib+ij$ and we have $ab \in A$ and $aj, ib, ij \in I$ so $xy \in A+I$ which fulfills item 4. Now consider $a + i \in A + I$ and we get $-(a + i) = -a + (-i) \in A + I$, and therefore $A + I$ is a subring of R. Also note that $A + I \supset I$ as $0 \in A$.

(b) First notice that if $x \in (A + I)/I$ then $x = a + i + I = a + I$ for some $a \in A$ and $i \in I$ and from this it follows that $(A + I)/I = \{a + I \mid a \in A\}$. Now let us define $B = A \cap I$ and we can now try and define $\varphi : (A + I)/I \to A/B$ as $\varphi(a + I) = a + B$.

φ is a function as if $a, b \in A$ and $a + I = b + I$ then we get $a - b \in I$ and $a - b \in A$ due to closure so $a - b \in B$. From this we now conclude $b + B = b + a - b + B = a + B$, so φ must be well defined.

φ is a homomorphism as if $a, b \in A$ then

$$\varphi(a + I) + \varphi(b + I) = (a + B) + (b + B) = a + b + B = \varphi(a + b + I)$$

and

$$\varphi(a + I)\varphi(b + I) = (a + B)(b + B) = ab + B = \varphi(ab + B) = \varphi((a + B)(b + B))$$

φ is 1-1 as if $\varphi(a + I) = \varphi(b + I)$ then $a + B = b + B$ so $b - a \in B$ and therefore $b - a \in I$ as $B = A \cap I$. From this we conclude $a + I = a + b - a + I = b + I$.

Finally φ is onto as if $x \in A/B$ then $x = a + B$ for some $a \in A$ and therefore $a + I \in (A + I)/I$ so $\varphi(a + I) = a + B = x$.

Now we have constructed a isomorphism, $\varphi : (A + I)/I \to A/(A \cap I)$ so $(A + I)/I \simeq A/(A \cap I)$.

4.3.4 Question 20

Suppose $a, b \in R$. Now we get

$$\begin{aligned}\varphi(a + b) &= (a + b + I, a + b + J) \\ &= ((a + I) + (b + I), (a + J) + (b + J)) \\ &= (a + I, a + J) + (b + I, b + J) \\ &= \varphi(a) + \varphi(b)\end{aligned}$$

and

$$\begin{aligned}\varphi(ab) &= (ab + I, ab + J) \\ &= ((a + I)(b + I), (a + J)(b + J)) \\ &= (a + I, a + J)\,(b + I, b + J) \\ &= \varphi(a)\varphi(b)\end{aligned}$$

so φ is a homomorphism.

Now consider $\varphi(0)$, we find that the 0 in $R_1 \oplus R_2$ must be $(0 + I, 0 + J) = (I, J)$. So now we find $\ker(\varphi) = \{x \in R \mid \varphi(x) = (I, J)\}$. From this we can infer that $x \in \ker(\varphi)$ iff $x + I = I$ and $x + J = J$, so from this we get $x \in I$ and $x \in J$ so $x \in \ker(\varphi) \iff x \in I \cap J$ so $\ker(\varphi) = I \cap J$.

4.3.5 Question 24

Let m and n be relatively prime integers and consider the function $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ defined as $f(x) = (x, x)$. If we have $f(x) = f(y)$ then we have $x \equiv y \mod m$ and $x \equiv y \mod n$ so it follows that $x \equiv y \mod mn$. Now $\mathbb{Z}_{mn}$ has exactly $m \cdot n$ elements and $\mathbb{Z}_m \oplus \mathbb{Z}_n$ also has exactly $m \cdot n$ so if f is 1-1 then f is also onto. Finally we may then take any $a, b \in \mathbb{Z}$ and let $f^{-1}((a, b)) = x$. We know this to be well defined as f is onto so we then have $x \equiv a \mod m$ and $x \equiv b \mod n$.

4.3.6 Question 27

Let P be the product of our n primes and we get from our previous question that we may define $f : \mathbb{Z}_p \to \prod_{i=1}^{n} \mathbb{Z}_{p_i}$ just as before with $f(x) = (x, x, \ldots, x)$ and again this function will be 1-1 as if $f(x) = f(y)$ then we get $x \equiv y \mod p_i$ for all $0 < i \leq n$, and therefore $x \equiv y \mod \prod_{i=1}^{n} p_i$ otherwise stated as $x \equiv y \mod P$. Just like before this is a map from two spaces with the same finite cardinality of P so f being 1-1 also makes f onto. Here we also will note that f is a homomorphism as

$$f(xy) = (xy, xy, \ldots, xy) = (x, x, \ldots, x)(y, y, \ldots, y) = f(x)f(y)$$

and

$$f(x + y) = (x + y, x + y, \ldots, x + y) = (x, x, \ldots, x) + (y, y, \ldots, y) = f(x) + f(y)$$

Now from this we get that in order for $x^2 \equiv x \mod P$ then $f(x) = f(x^2) = (f(x))^2$ and also that if $f(x^2) \neq f(x)$ then $x^2 \neq x$ as f is an isomorphism, so we simply need to count the number of $(a_1, a_2, \ldots, a_n) \in \prod_{i=1}^{n} \mathbb{Z}_{p_i}$ such that $(a_1, a_2, \ldots, a_n)^2 = (a_1, a_2, \ldots, a_n)$. From this we need ${a_i}^2 \equiv a_i \mod p_i$ and that happens exactly when $a_i \equiv 1 \mod p_i$ or $a_i \equiv 0 \mod p_1$. This gives us two options for each a_i and as each option is independent we then have 2^n total ways to create $x \in Z_P$ such that $x^2 \equiv x \mod P$.

4.4 Section 4

4.4.1 Question 1

Notice that $1^2 \equiv 1 \mod 3$ and $2^2 \equiv 1 \mod 3$ so if $a \not\equiv 0 \mod 3$ and $b \not\equiv 0 \mod 3$ then $a^2 + b^2 \equiv 1 + 1 \mod 3$ so $a^2 + b^2 \equiv 2 \mod 3$.

4.4.2 Question 9

Assume that $a^2 \equiv b^2 \mod p$ with $a \neq 0 \neq b$. We then find that $a^2 - b^2 \equiv 0 \mod p$ so $(a + b)(a - b) \equiv 0 \mod p$. We know that $\mathbb{Z}_p$ is a division ring when p is prime so then either $a + b \equiv 0 \mod p$ or $a - b \equiv 0 \mod p$. From this we get that the only way for $a^2 \equiv b^2 \mod p$ is if $a \equiv \pm b \mod p$. This means that every non-zero quadratic residue in a prime modulus has exactly two ways to be represented as for all $a \not\equiv 0 \mod p$, $a \not\equiv -a \mod p$ as then $a + a = 2a \equiv 0$ and we would then have $2 \equiv 0 \mod p$, which would be true if $p = 2$, however we are assuming p to be an odd prime. Now we finish the proof by saying each a^2 has two distinct representations and thus there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic nonresidues mod p.

Consider $Q = \left\{x^2 \,\middle|\, x \neq 0 \in \mathbb{Z}_p\right\}$ with p prime. It follows then that for any $a^2, b^2 \in Q$ that $a^2b^2 = (ab)^2 \in Q$ as multiplication is commutative in $\mathbb{Z}_p$. We also have for any $a^2 \in Q$, that $a^{-1} \in \mathbb{Z}_p$ and therefore $\left(a^{-1}\right)^2 = a^{-2} = \left(a^2\right)^{-1} \in Q$. From this we get that Q is a group, and more specifically a subgroup of $\mathbb{Z}_p - \{0\}$ under multiplication.

4.4.3 Question 10

Choose $m \in \mathbb{Z}$ such that $m > 0$ and $\sqrt{m} \notin Z$ and define $R = \{a + b\sqrt{m} \,|\, a, b \in \mathbb{Z}\}$ and define addition and multiplication on R in the standard way from the reals. It is obvious that $R \subset \mathbb{R}$ so in order to show that R is a ring we simply need to show it to be a subring of $\mathbb{R}$, and to do this we only need show it is closed under addition and multiplication and that it has additive inverses.

Choose $a + b\sqrt{m} \in R$, then we find

$$-\left(a + b\sqrt{m}\right) = -a + -b\sqrt{m} \in R$$

so we have additive inverses.

Choose $a_1 + b_1\sqrt{m} \in R$ and $a_2 + b_2\sqrt{m} \in R$. We then have

$$\left(a_1 + b_1\sqrt{m}\right) + \left(a_2 + b_2\sqrt{m}\right) = (a_1 + a_2) + (b_1 + b_2)\sqrt{m} \in R$$

and

$$\begin{aligned}\left(a_1+b_1\sqrt{m}\right)\left(a_2+b_2\sqrt{m}\right) &= a_1a_2+a_1b_2\sqrt{m}+a_2b_1\sqrt{m}+b_1\sqrt{m}b_2\sqrt{m}\\ &= (a_1a_2+b_1b_2m)+(a_1b_2+a_2b_1)\sqrt{m}\in R\end{aligned}$$

so we have closures.

Now we conclude that R is a subring of $\mathbb{R}$.

4.4.4 Question 11

First let us show that I_p is an additive subgroup of R. Let $a+b\sqrt{m}\in I_p$ and $c+d\sqrt{m}\in I_p$. Then

$$a+b\sqrt{m}+c+d\sqrt{m}=(a+c)+(b+d)\sqrt{m}$$

and we know $p|a$ and $p|c$ so $p|(a+c)$ and the same is true for $b+d$, therefore I_p is closed under addition. Also

$$-\left(a+b\sqrt{m}\right)=-a+-b\sqrt{m}$$

and as $p|a$ then $p|-a$ and again the same argument goes for $-b$ so we now know that I_p is an additive subgroup of R.

Now consider $a+b\sqrt{m}\in I_p$ and $c+d\sqrt{m}\in R$. We only need show that this is an ideal from one side as multiplication is commutative in $\mathbb{R}$, which this is all contained within. So we find

$$\left(a+b\sqrt{m}\right)\left(c+d\sqrt{m}\right)=ac+bdm+(ad+bc)\sqrt{m}$$

We know $p|a$ so $p|ac$. We also know that $p|b$ so we know that $p|bdm$ and therefore $p|(ac+bdm)$. Next we know that $p|a$ so $p|ad$ and we know $p|b$ so $p|ac$ and therefore $p|(ad+bc)$ so we conclude that $ac+bdm+(ad+bc)\sqrt{m}\in I_p$ and therefore I_p is an ideal of R.

4.5 Section 5

4.5.1 Question 2

For this problem I will assume that x commutes with R as otherwise I end up with ax^nbx^m and can't be sure that this is really can be written as cx^k. I feel this is a a safe assumption, despite the book not stating this in the problem, as it does say that it is mostly dealing with commutative rings. To be more precise I'm really saying that for any $p(x)\in R[x]$, $p(x)$ is a function $p:A\to B$ and for any $x\in A$ and $r\in R$, we need to have $xr=rx$.

(a) Consider $f(x),g(x)\in R[x]$ with $f(x)\neq 0\neq g(x)$. Let $\deg f(x)=n$ and $\deg g(x)=m$ and we get that $f(x)=\sum_{i=0}^{n}f_ix^i$ and $g(x)=\sum_{i=0}^{m}g_ix^i$ for some $f_1,f_2,\ldots,f_n,g_1,g_2,\ldots,g_m\in R$. From this we get

$$\begin{aligned}f(x)g(x) &= \sum_{i=0}^{n}\left[f_ix^i\right]\sum_{i=0}^{m}\left[g_ix^i\right]\\ &= \sum_{j=0}^{n}\left[f_jx^j\sum_{i=0}^{m}\left[g_ix^i\right]\right]\\ &= \sum_{j=0}^{n}\left[\sum_{i=0}^{m}\left[f_jx^jg_ix^i\right]\right]\\ &= \sum_{j=0}^{n}\left[\sum_{i=0}^{m}\left[f_jg_ix^{j+i}\right]\right]\end{aligned}$$

so we get that the largest power possible for x to be $n+m$ and therefore $\deg(f(x)g(x))\leq m+n=\deg f(x)+\deg g(x)$.

(b) Consider the ring $\mathbb{Z}_{ab}$, with $a,b>1$. Then we can have $f(x)=ax$ and $g(x)=bx+1$ and so we find $f(x)g(x)=abx^2+ax=0x^2+ax=ax$ as $ab\equiv 0 \mod ab$.

4.5.2 Question 3

Using the Euclidean algorithm, I will not show the work as it's quite a lot to be typed up, however the algorithm takes in $a_0(x)$ and $b_0(x)$ and then finds $a_0 = q_0(x)b_0(x) + r_0(x)$ with $\deg r_0(x) < \deg b_0(x)$ as per the division algorithm. Then we let $a_1(x) = b_0(x)$ and $b_1(x) = r_1(x)$ and we repeat. This means we have $a_i = b_{i-1}$ and $b_i = r_{i-1}$ and $a_i = q_i(x)b_i(x) + r_i(x)$ with $\deg r_i(x) < \deg b_i(x)$. Eventually there is some n such that $b_n(x) = 0$, and then $a_n(x) = \gcd(a_0(x), b_0(x))$. Some normalizing may be required to keep the polynomials monic, but this does not mess with the algorithm. Remember that if $a(x)|f(x)$ then any $ca(x)|f(x)$ as $a(x)b(x) = f(x)$ so $ca(x)c^{-1}b(x)|f(x)$ as c^{-1} must exist due to us working in $F[x]$ with F a field. With no further ado, the solutions:

(a) 1

(b) $x - 1$

(c) 1

(d) $x^3 - 1$

4.5.3 Question 10

(a) $x^2 + 7$ over $\mathbb{R}$. If a polynomial is not irreducible then it can be written as the product of irreducible polynomials. For $x^2 + 7$ over $\mathbb{R}$ we would have to have some $g(x), f(x) \in \mathbb{R}[x]$ such that $g(x)$ is monic irreducible and $\deg f(x), \deg g(x) > 0$. This means that $\deg f(x) = 1 = \deg g(x)$ so $f(x) = ax + b$ and $g(x) = x + c$. From this we would have $f(x)g(x) = ax^2 + (ac + b)x + bc = x^2 + 7$. From this we get $a = 1$, $ac + b = 0$ and $bc = 7$. We then have $c + b = 0$ so $b = -c$. That means that $bc = -b^2$ and all squares are positive in $\mathbb{R}$ so we can not have $-b^2 = 7$ so we have a contradiction.

(b) $x^3 - 3x + 3$ over $\mathbb{Q}$. If this is not irreducible then it is the product of some smaller monic polynomials and a constant so by it being degree 3 this must be a polynomial of order 1 and order 2. Therefore we let $f(x) = x^2 + ax + b$ and $g(x) = x + c$ and finally $d \in \mathbb{R}$ such that $f(x)g(x)d = x^3 - 3x + 3$. Immediately we get $d = 1$ as $x^3 - 3x + 3$ is monic, so we are left with

$$x^3 - 3x + 3 = x^3 + (a + 1)x^2 + (ac + b)x + bc$$

and from that $a + 1 = 0$ so $a = -1$, $ac + b = b - c = -3$ and $bc = 3$. It follows that $c - b = 3 = bc$. From this the sign of b and c must be the same as bc is positive, so that means $c > 3$ as otherwise we could not have $c - b = 3$. Now we let $\frac{n}{m} = c$ and $\frac{p}{q} = b$, with $p, q, n, m \in \mathbb{Z}$ and $\gcd(n, m) = 1 = \gcd(p, q)$. We know $a, b > 0$ so $p, q, n, m > 0$. We know $c > 3$ so $\frac{n}{m} > 3$ and thus $n > 3m \geq 3$. And finally we know $\frac{n}{m}\frac{p}{q} = 3 = \frac{n}{m} - \frac{p}{q}$ which we rewrite as $\frac{np}{mq} = 3 = \frac{nq - mp}{mq}$ and then one step further we get

$$np = 3mq = nq - mp$$

Here we divide by n and p and we get two equalities: first

$$n = \frac{3mq}{p} = \frac{nq}{p} - m$$

and therefore $p|3mq$ and $p|nq$, and as we know $\gcd(p, q) = 1$ then $p|3m$ and $p|n$; and our second equation

$$p = \frac{3mq}{n} = q + \frac{mp}{n}$$

and therefore $n|3mq$ and $n|mp$, however we know $\gcd(n, m) = 1$ so we have $n|3q$ and $n|p$. We now have shown $n|p$ and $p|n$ so $p = n$ and therefore we know that $n|3m$ as we had $p|3m$. We know $\gcd(n, m) = 1$ so $n|3m \implies n|3$ and thus $n \leq 3$ which contradicts $n > 3m \geq 3$ we already had, so thus there can not possibly be any polynomials $g(x), f(x)$ over $\mathbb{Q}$ such that $g(x)f(x) = x^3 - 3x + 3$ with both being lower order than three, so $x^3 - 3x + 3$ is irreducible.

(c) $x^2 + x + 1$ over $\mathbb{Z}_2$. From our previous results we know that in order for this not to be irreducible we need $g(x), f(x) \in \mathbb{Z}_2[x]$, both with lower order and monic be such that $g(x)f(x) = x^2 + x + 1$. It follows that $g(x) = x + a$ and $f(x) = x + b$ and therefore $f(x)g(x) = x^2 + (a + b)x + ab$. We know then that $ab = 1$

and $a+b=1$. In order for $ab=1$ we need both $a,b=1$ and therefore $a+b=0$ so we have a contradiction and thus x^2+x+1 is irreducible.

(d) x^2+1 over $\mathbb{Z}_{19}$. Just like before let $g(x)=x+a$ and $f(x)=x+b$ and we get $a+b=0$ and $ab=1$. From this we get that $a=-b$ so $ab=-bb=-b^2=1$ so $b^2=-1$ which is not a square in $\mathbb{Z}_{19}$ which we can show simply by listing all the squares. I will not do that here, however here is python code that will verify the result.

```
[pow(x,2,19) for x in range(0,19)]
```

(e) x^3-9 over $\mathbb{Z}_{13}$. Just like before let $f(x)+x^2+ax+b$ and $g(x)=x+c$ and we find

$$f(x)g(x)=x^3+(a+c)x^2+(ac+b)x+bc$$

so $a+c=0$, $ac+b=0$ and $bc=1$. From this we get $a=-c$ and therefore $ac+b=-c^2+b=0$, so $b=c^2$ and thus finally $bc=c^3=-9$. $\mathbb{Z}_{13}$ is a small space so we can just check to see if -9 is a cube, notice $-9=13-9=4$ and 4 is not a cube. I verified this with the following python code.

```
[pow(x,3,13) for x in range(0,13)]
```

(f) x^4+2x^2+2 over $\mathbb{Q}$. If this is reducible then either it is a degree 3 and a degree 1 or two degree 2 polynomials. Let us degree 3 and 1 and then two degree 2 polynomials.

Let $f(x)=x^3+ax^2+bx+c$ and $g(x)=x+d$, then we have

$$f(x)g(x)=x^4+(a+d)x^3+(ad+b)x^2+(bd+c)x+cd$$

so $a+d=0$, $ad+b=2$, $bd+c=0$, and $cd=2$. We then have $a=-d$ and therefore $-a^2+b=2$ so $b=2+a^2$. Further $bd+c=(2+a^2)(-a)+c=0$ so $c=a(2+a^3)$ and $cd=a(2+a^3)(-a)=2$, so we have $-a^2(2+a^3)=2$. Now $a^2>0$ so $2+a^3<0$ for the multiplication to work, this simply means $a^3<-2$ and therefore $a<-\sqrt[3]{2}$. Now we also know that $a\in\mathbb{Q}$ and a is negative so $a=-\frac{p}{q}$ with integers $p,q>0$. From this we get

$$\begin{aligned}
2&=-\left(-\frac{p}{q}\right)^2\left(2+\left(-\frac{p}{q}\right)^3\right)\\
&=-\frac{p^2}{q^2}\left(2-\frac{p^3}{q^3}\right)\\
&=-2\frac{p^2}{q^2}+\frac{p^5}{q^5}\\
2q^2&=-2p^2+\frac{p^5}{q^3}\\
2q^2+2p^2&=\frac{p^5}{q^3}\\
2q^5+2p^2q^3&=p^5\\
\frac{2q^5}{p^2}+2q^3&=p^3
\end{aligned}$$

so we have $p^2|2q^5$, however as $\gcd(p,q)=1$ then $p^2|2$ and therefore $p=1$. From this we get $\frac{p}{q}\leq 1$ so $2-\left(\frac{p}{q}\right)^3>0$ and $-\left(\frac{p}{q}\right)^2<0$ so then $2=-\left(\frac{p}{q}\right)^2\left(2-\left(\frac{p}{q}\right)^3\right)<0$ and we have a contradiction.

Now let us try two order 2 polynomials, $f(x)=x^2+ax+b$ and $g(x)=x^2+cx+d$ and we find

$$f(x)g(x)=x^4+(a+c)x^3+(b+ac+d)x^2+(ad+bc)x+bd$$

so $a+c=0$, $b+ac+d=2$, $ad+bc=0$ and $bd=2$. From $a+c=0$ we get $a=-c$ and therefore our equality $ad=bc=0$ becomes $ad-ab=0$ so $ad=ab$ and therefore either $a=0$ or $b=d$.

If $b=d$ then $bd=b^2=2$ and therefore $b=\sqrt{2}$ which is known to be irrational, so this can not be.

If $a = 0$ then $b - ac + d = 2$ becomes $b + d = 2$ and we also have $bd = 2$ so $a + b = 2 = bd$. bd is positive and therefore b and d must share a sign, however $b+d$ is also positive so if they are to share a sign they both must be positive. Now let $b = \frac{n}{m}$ and $d = \frac{p}{q}$ with p, q, n, m positive integers and $\gcd(p, q) = 1 = \gcd(n, m)$. Now we have $\frac{n}{m} + \frac{p}{q} = 2 = \frac{n}{m} \cdot \frac{p}{q}$ so it follows that $\frac{nq+pm}{mq} = 2 = \frac{np}{mq}$ and therefore

$$2mq = nq + pm = np$$

From this we can do some division and find

$$\frac{2mq}{n} = q + \frac{pm}{q} = p$$

so $n|pm$ and $n|2mq$ and by $\gcd(n, m) = 1$ we get $n|p$ and $n|2q$; and we find

$$\frac{2mq}{p} = \frac{nq}{p} + m = n$$

so $p|2mq$ and $p|nq$ and by $\gcd(p, q) = 1$ we get $p|n$ and $p|2m$. From this we then have $p|n$ and $n|p$ so it follows that $n = p$ and therefore $n|2$ as $n = p|2m$ so either $n = 1$ or $n = 2$. If $n = 1$ then $2 = \frac{1}{mq}$ which is impossible, so $n \neq 1$. If $n = 2$ then $2mq = 2q + m = 4$. From this we get $mq = q + m = 2$, in order for $mq = 2$ we need one of m, q to be 1 and the other to be 2, however that would give $q + m = 3 \neq 2$ so we have a contradiction, and are now done.

4.5.4 Question 11

Suppose $p(x) \in F[x]$ is of order 3. If $p(x)$ is reducible then there must be some $f(x), g(x) \in F[x]$ and some $a_0 \in F$ such that $p(x) = a_0 f(x)g(x)$ and both $f(x)$ and $g(x)$ have lower order then $p(x)$ and are monic. This means one will have order 2 while the other has order 1. Suppose then without loss of generality $f(x)$ has order 2 and $f(x) = x + b$. Then we notice that $f(-b) = 0$ so $a_0 f(-b)g(-b) = 0$ and thus $p(x) = 0$ for at least some value in F. It follows then that if $p(x) \not\emptyset$ for all $x \in F$ then $p(x)$ is irreducible.

4.5.5 Question 12

By theorem 4.5.9 in the book we have if $f(x), g(x)$ are relatively prime then there is some $a(x), b(x)$ such that $a(x)f(x)+b(x)g(x) = 1$. This means that there is $a(x), f(x), b(x), g(x) \in F$ such that $a(x)f(x)+b(x)g(x) = 1$, and as $F \subset K$ then $a(x)f(x) + b(x)g(x) = 1$ is also true in $K[x]$. Now by theorem 4.5.9 again we get that this means $f(x)$ and $g(x)$ are relatively prime.

4.5.6 Question 13

Let $p(x) = x^2 + 1$. Now $\mathbb{R}[x]$ is an principal ideal domain, so for all $f(x) \in (p(x))$, $f(x) = a(x)p(x)$ for some $a(x)$. So the first thing we wish to show is that if $\deg f(x) \geq 2$ then there is some $g(x)$ of order less than 2 such that $(p(x)) + f(x) = (p(x)) + g(x)$ or $f(x) \in (p(x))$.

Proof. Suppose $\deg f(x) \geq 2$, then there exists $q(x), r(x)$ such that $f(x) = q(x)p(x) + r(x)$ and $\deg r(x) < \deg p(x)$ or $r(x) = 0$ by the division algorithm. From this we get $\deg r(x) < 2$ or $r(x) = 0$. If $r(x) = 0$ then $f(x) = q(x)p(x) \in (p(x))$. If $\deg r(x) < 2$ then $f(x) \in (p(x)) + r(x)$. □

Now further we wish to show that for any $a(x), b(x)$ with order less than 2, if $a(x) \neq b(x)$ then $(p(x)) + a(x) \neq (p(x)) + b(x)$. We include the 0 function as having order less than 2.

Proof. Suppose $a(x) \neq b(x)$ and both have order less than 2, then assume for the sake of contradiction that $(p(x)) + a(x) = (p(x)) + b(x)$. From this we get $a(x) = c(x)p(x) + b(x)$ and we find $\deg(c(x)p(x) + b(x)) = \max(\deg c(x) + \deg p(x), \deg b(x)) = \deg c(x) + \deg p(x)$ as $\deg p(x) > \deg b(x)$ unless $c(x) = 0$. If $c(x) = 0$ then we get $a(x) = b(x)$ which we already said it is not, and otherwise we get $\deg a(x) = \deg c(x) + \deg p(x) \geq \deg p(x) = 2$ thus contradiction that $a(x)$ has order 2 or less, so we conclude that $(p(x)) + a(x) \neq (p(x)) + b(x)$ □

So every element in $\mathbb{R}[x]/(p(x))$ has a unique representation by a polynomial with that is either 0, or has order less than 2. Notice finally that $f(x) = x$ has $f(x)^2 = x^2$ and $(p(x)) + x^2 = (p(x)) - 1$ by the division algorithm. So we can conclude that $\varphi : \mathbb{C} \to \mathbb{R}[x]/p(x)$ defined as $\varphi(a + bi) = (p(x)) + bx + a$ is a isomorphism.

4.5.7 Question 19

Consider $P(x) = x^2 - a \in \mathbb{Z}_p[x]$ with p an odd prime. If $P(x)$ is reducible then there is some $f(x)g(x) = P(x)$ with both having lower order and monic as $P(x)$ is monic. Let $f(x) = x + c$ and $g(x) = c + d$ so

$$P(x) = x^2 - a = f(x)g(x) = (x + c)(x + d) = x^2 + (c + d)x + cd$$

and therefore $c + d = 0$ so $c = -d$ and we also have $cd = -a$ so $-c^2 = -a$ and therefore $c^2 = a$. So only if a is a square in $\mathbb{Z}_p$ is $P(x)$ reducible, so let a be a quadratic nonresidue mod p, and we know such an element exists from Question 9 in Section 4.

Now consider $\mathbb{Z}_p[x]/P(x)$ and we know from the last problem that every element of this has a unique representation by a polynomial of order less than 2.[2] So now we already know this is a commutative ring, so we simply need to show the existence of a unit and inverses and we have a field. So as every element of this has a unique second degree polynomial representing it then any element takes the form $[bx + c]$ and there are p^2 such polynomials.

So for a unit we have $e(x) = 1$, as $e(x)(bx + c) = 1(bx + c) = bx + c$. Now consider $f(x) = bx + c$ and we find

$$[f(x)]^2 = \left[b^2x^2 + 2bcx + c^2\right] = \left[2bcx + b^2a + c^2\right]$$

, thus in order for $[f(x)]^2 = 0$ we need $2bc = 0$ so either $b = 0$ or $c = 0$ and either way then $b^2a + c^2 = 0$ would imply that the other (between b and c) must be 0. From this we get that no element multiplied by itself is 0, unless that element was the 0 element. So we can conclude that $[f(x)]^{2^n} \neq [0]$. This in-fact means all powers of $f(x)$ are not zero as then there would some 2^n power greater then it which would be zero. Now from some results we had in finite groups we can be sure that $[f(x)]$ has an inverse. Now we know that $\mathbb{Z}_p[x]/P(x)$ is a field with order p^2.

4.5.8 Question 26

4.5.9 Question 28

4.6 Section 6

4.6.1 Question 3

Any a such that $a = 5k$ with $k \equiv 0 \mod 5$ or $a = 3k$ with $k \equiv 0 \mod 3$.

4.6.2 Question 4

Consider $g(x) = {a_0}^{n-1} f(x)$ and then let $y = a_0 x$ and we find $h(y)$ such that $h(y) = g(x)$. Therefore we have

$$h(y) = h(a_0 x) = g(x)$$

The first term of $g(x)$ is $a_0 x^n$ so then $h(y)$ must be monic, and we may use the Einstein criterion on this to test if $f(x)$ is reducible.

4.6.3 Question 7

For this we will define arbitrary polynomial $f(x) = \sum_{i=0}^{\infty} \left[f_i x^i\right]$ with $f_i = 0$ for all $i > \deg f(x)$. This will make notation much smoother.

[2] While we didn't actually prove it in the last problem the steps we went through would also work for this case, so I'm not going to go through the work again.

- φ is a homomorphism as:

$$\begin{aligned}
\varphi(f(x)) + \varphi(g(x)) &= f(x+1) + g(x+1) \\
&= \sum_{i=0}^{\infty} \left[f_i \left(x+1\right)^i \right] + \sum_{i=0}^{\infty} \left[g_i \left(x+1\right)^i \right] \\
&= \sum_{i=0}^{\infty} \left[(f_i + g_i)(x+1)^i \right] \\
&= \varphi \left(\sum_{i=0}^{\infty} \left[(f_i + g_i) x^i \right] \right) \\
&= \varphi(f(x) + g(x))
\end{aligned}$$

$$\begin{aligned}
\varphi(f(x))\varphi(g(x)) &= f(x+1)g(x+1) \\
&= \sum_{i=0}^{\infty} \left[\sum_{j=0}^{i} \left[f_{i-j} g_j \right] (x+1)^i \right] \\
&= \varphi \left(\sum_{i=0}^{\infty} \left[\sum_{j=0}^{\infty} \left[f_{i-j} g_j \right] x^i \right] \right) \\
&= \varphi(f(x)g(x))
\end{aligned}$$

- φ is 1-1 as if $\varphi(f(x)) = \varphi(g(x))$ then $f(x+1) = g(x+1)$ and we can define $p(x) = f(x+1)$ and $q(x) = g(x+1)$ so we have $p(x) = q(x)$ and it follows then that $p(x-1) = q(x-1)$ so $f(x) = g(x)$.
- φ is onto as $f(x) = g(x+1)$ with $g(x) = f(x-1)$, so $\varphi(g(x)) = f(x)$.

Further consider that for any $a \in F$, we can construct $f(x) = a$ and then $\varphi(f(x)) = a$, so $\varphi(a) = a$.

4.6.4 Question 11

We have $\varphi : F[x] \to F[x]$ is an automorphism and $\varphi(a) = a$ for all $a \in F$. Now we have

$$\varphi(f(x)) = \varphi \left(\sum_{i=0}^{n} \left[f_i x^i \right] \right) = \sum_{i=0}^{n} \left[\varphi(f_i) \varphi(x)^i \right] = \sum_{i=0}^{n} \left[f_i \varphi(x)^i \right]$$

. Now as $x \in F[x]$ then so must $\varphi(x) \in F[x]$ as φ is an automorphism. From this we get $\varphi(x) = p(x) \in F[x]$, so $\varphi(f(x)) = f(p(x))$. Now we have $\deg f(g(x)) = \deg f(x) \cdot \deg g(x)$, so $\deg p(x) = 1$ as if it were greater we could never map to a order 1 polynomial and if it were less everything would map to the zero function or a constant. So now $\sigma(f(x)) = f(p(x))$ and $\deg p(x) = 1$ so $p(x) = ax + b$ for some $a, b \in F$ with $a \neq 0$.

4.7 Section 7

4.7.1 Question 3

We have $[a,b][c,d] = [ac, bd]$. So

$$\begin{aligned}[a,b]\left([c,d][e,f]\right) &= [a,b][ce,df] \\ &= [ace, bdf] \\ &= [ac,bd][e,f] \\ &= \left([a,b][c,d]\right)[e,f]\end{aligned}$$

$$\begin{aligned}[a,b][c,d] &= [ac,bd] \\ &= [ca,db] \\ &= [c,d][a,b]\end{aligned}$$

so we have associativity and commutativity for multiplication.

4.7.2 Question 4

Let K be a field and D an integral domain with $D \subset K$. Let F be the quotient field generated by D. Now assume for the sake of contradiction there is some $\frac{a}{b} \in F$ such that $\frac{a}{b} \notin K$. If $\frac{1}{b} \in K$ then we get $\frac{a}{b} \in K$ as $a \in K$ and thus we would have $a\frac{1}{b} \in K$. Now $\frac{1}{b} = b^{-1}$ so therefore we have found some $b \neq 0$ such that b does not have an inverse in K, so K is not a field. Therefore $\frac{a}{b} \in K$ so $F \subset K$.

5 Chapter 5

5.1 Section 1

5.1.1 Question 3

For notational reasons we will let polynomials be the sum of infinite terms, with only finitely many having non-zero coefficients.

(a) Consider $f(x,y) \in S[y]$, then

$$f(x,y) = \sum_{i=0}^{\infty} \left[f_i(x) y^i\right] = \sum_{i=0}^{\infty} \left[\sum_{j=0}^{\infty} \left[f_{i,j} x^j\right] y^i\right]$$

(b) If $f(x,y) = \sum_{i=0}^{\infty} \left[\sum_{j=0}^{\infty} \left[f_{i,j} x^j\right] y^i\right]$ and $g(x,y) = \sum_{i=0}^{\infty} \left[\sum_{j=0}^{\infty} \left[g_{i,j} x^j\right] y^i\right]$ then simply, we need $f_{i,j} = g_{i,j}$ for all i, j.

(c)

$$
\begin{aligned}
f(x,y)+g(x,y) &= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[f_{i,j}x^j\right]y^i\right]+\sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[g_{i,j}x^j\right]y^i\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[f_{i,j}x^j\right]y^i+\sum_{j=0}^{\infty}\left[g_{i,j}x^j\right]y^i\right] \\
&= \sum_{i=0}^{\infty}\left[\left(\sum_{j=0}^{\infty}\left[f_{i,j}x^j\right]+\sum_{j=0}^{\infty}\left[g_{i,j}x^j\right]\right)y^i\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[f_{i,j}x^j+gi,jx^j\right]y^i\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[\left(f_{i,j}+g_{i,j}\right)x^j\right]y^i\right]
\end{aligned}
$$

(d)

$$
\begin{aligned}
f(x,y)g(x,y) &= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[f_{i,j}x^j\right]y^i\right]\sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[g_{i,j}x^j\right]y^i\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[f_{i,j}x^j\right]y^i\sum_{k=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[g_{k,j}x^j\right]y^k\right]\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[\sum_{k=0}^{\infty}\left[f_{i,k}x^k\right]y^i\sum_{k=0}^{\infty}\left[g_{j,k}x^k\right]y^j\right]\right] \\
\text{(If } R \text{ is commutative)} \quad &= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[\sum_{k=0}^{\infty}\left[f_{i,k}x^k\right]\sum_{k=0}^{\infty}\left[g_{j,k}x^k\right]y^iy^j\right]\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[\sum_{k=0}^{\infty}\left[\sum_{l=0}^{\infty}\left[f_{i,l}x^l\right]g_{j,k}x^k\right]y^{i+j}\right]\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[\sum_{k=0}^{\infty}\left[\sum_{l=0}^{\infty}\left[f_{i,l}x^lg_{j,k}x^k\right]\right]y^{i+j}\right]\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{\infty}\left[\sum_{k=0}^{\infty}\left[\sum_{l=0}^{\infty}\left[f_{i,l}g_{j,k}x^{l+k}\right]\right]y^{i+j}\right]\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{i}\left[\sum_{k=0}^{\infty}\left[\sum_{l=0}^{\infty}\left[f_{i-j,l}g_{j,k}x^{l+k}\right]\right]\right]y^i\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{j=0}^{i}\left[\sum_{k=0}^{\infty}\left[\sum_{l=0}^{k}\left[f_{i-j,l}g_{j,k-l}\right]x^k\right]\right]y^i\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{k=0}^{\infty}\left[\sum_{j=0}^{i}\left[\sum_{l=0}^{k}\left[f_{i-j,l}g_{j,k-l}\right]x^k\right]\right]y^i\right] \\
&= \sum_{i=0}^{\infty}\left[\sum_{k=0}^{\infty}\left[\sum_{j=0}^{i}\left[\sum_{l=0}^{k}\left[f_{i-j,l}g_{j,k-l}\right]\right]x^k\right]y^i\right]
\end{aligned}
$$

5.1.2 Question 8

Let us do this by induction on n where $m = p^n$. If $n = 0$ this is trivial and when $n = 1$ we get $(a+b)^p = \sum_{i=0}^{p}\binom{p}{i}a^ib^{p-i}$ and as $p|\binom{p}{i}$ for all i such that $0 < i < p$ we then get $(a+b)^p = a^p + b^p$. Choose $n \in \mathbb{N}$ and suppose that for all $k < n$ that

$$(a+b)^{p^k} = (a+b)^{p\cdot p^k} = ((a+b)^p)^{p^{k-1}} = (a^p+b^p)^{p^{k-1}} = a^{p\cdot p^{k-1}} + b^{p\cdot p^{k-1}} = a^{p^n} + b^{p^n}$$

5.1.3 Question 9

(a) First

$$\varphi(ab) = (ab)^p = a^pb^p = \varphi(a)\varphi(b)$$

Second, using the result from our previous problem

$$\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$$

Finally if $\varphi(a) = \varphi(b)$ then $a^p = b^p$, $b = a + c$ for some $c \in F$, so $a^p = (a + c)^p = a^p + c^p$ and therefore $c^p = 0$, and as F is a field, $c^p = 0 \implies c = 0$. From this we have $b = a + 0$ so $b = a$.

If you do not believe that $c^p = 0 \implies c = 0$ then suppose $c \neq 0$ let n be such that $c^n = 0$ and for all $0 < m < n$, $c^m \neq 0$, that is n is the lowest power c that is zero. Now consider these statements

$$c(c^{n-1}c^{1-n}) = c1 = c$$
$$(cc^{n-1})c^{1-n} = 0c^{1-n} = 0$$

and now we have a contradiction, so $c^n \neq 0$ and thus all powers of non zero elements of fields are non zero.

(b) Consider $\mathbb{Z}_p$ and we have a finite field. From this we can construct the field of quotients over $\mathbb{Z}_p[x]$, and let us call this field K. For any $\frac{f(x)}{g(x)} \in K$ we have $p\frac{f(x)}{g(x)} = 0$ as $pf(x) = p\sum_{i=0}^{\infty} f_i x^i = \sum_{i=0}^{\infty} pf_i x^i = 0$. Now there is so $\frac{f(x)}{g(x)}$ such that $\varphi\left(\frac{f(x)}{g(x)}\right) = x$ as $\varphi\left(\frac{f(x)}{g(x)}\right) = \frac{f(\varphi(x))}{g(\varphi(x))} = \frac{f(x^p)}{g(x^p)}$ so the numerator's order will be $p \cdot \deg f(x)$ and the denominator's will be $p \cdot \deg g(x)$. Only if $g(x^p) | f(x^p)$ then can we reduce this to a polynomial and in that case we will have something of order $p \cdot \deg f(x) - p \cdot \deg g(x) = p(\deg f(x) - \deg g(x)) \neq 1$.

5.1.4 Question 10

If $f : A \to A$ is 1-1 and A is finite then f must be onto, therefore we have F is finite and $\varphi : F \to F$ is 1-1 so φ must be onto and thus a n automorphism as we already know it to be a monomorphism.

5.2 Section 2

5.2.1 Question 2

Only the trivial solution exists. I proved this by brute force checking all 125 possible solutions, and only the trivial one worked.

5.2.2 Question 3

If V has dimension n over $\mathbb{Z}_p$ then choose a basis $a_1, a_2, \ldots, a_n \in V$. Then any element of V has a unique representation as $\sum_{i=1}^{n} \alpha_i a_i$ with every $\alpha_i \in \mathbb{Z}_p$. This gives us a bijection $f : V \to {\mathbb{Z}_p}^n$ as $f(\sum_{i=1}^{n} \alpha_i a_i) = (a_1, a_2, \ldots, a_n)$ and this we know has p^n possible distinct values.

5.2.3 Question 6

(a) Assume there is some set of linearly independent vectors in W, therefore this set is also linearly independent in V. So by theorem 5.2.7 if W were to have dimension greater than V's dimension, it would imply that it has a set S of linearly independent vectors with $|S| > \dim_F(V)$. Now S is also linearly independent in V which gives us a contradiction by theorem 5.2.6.

If $\dim_F(W) = \dim_F(V) = n$ then we can choose some basis for W with n elements. This is then linearly independent in W and thus also linearly independent in V and forms a basis by theorem 5.2.7.

5.2.4 Question 10

I assume a vector space homomorphism ψ must follow $\psi(a + b) = \psi(a) + \psi(b)$ and $\alpha\psi(a) = \psi(\alpha a)$. If we view V and V' as groups under addition then by one of our homomorphism theorems from groups we already have $V' \simeq V/K$, So that means that there is a group isomorphism from V' to V/K, let us call it ϕ. All we need to do is show that $\alpha\phi(a) = \phi(\alpha a)$. Let $a \in V'$ and then consider $\{v \in V \mid \psi(v) = a\} = \psi^{-1}(a) \in V/K$. Remember $\psi : V \to V'$ is a vector space homomorphism. Let us try and construct ϕ as $\phi = \psi^{-1}$. We should already have this to be a group isomorphism so let us simply consider scaler multiplication.

$$\begin{aligned}\alpha\phi(a) &= \alpha\psi^{-1}(a) \\ &= \alpha\{v \in V \mid \psi(v) = a\} \\ &= \{\alpha v \mid v \in V, \psi(v) = a\}\end{aligned}$$

Then we would have $\psi(v) = a \implies \psi(\alpha v) = \alpha a$ so $\alpha\phi(a) = \{v \in V \mid \psi(v) = \alpha a\} = \psi^{-1}(\alpha a) = \phi(\alpha a)$ and we have shown ϕ to be a vector space isomorphism.

5.2.5 Question 11

Let us proceed with a proof by contradiction. Suppose there is some finite dimensional vector space V over F with a linearly independent set of vectors $v_1, v_2, \ldots, v_n$ and $\dim_F(v) > n$ such that we can not add another vector v_{n+1} without breaking linear independence. This is impossible as $v_1, v_2, \ldots, v_n$ is not a basis as $\dim_F(v) > n$ so we can find some v such that $v \notin < v_1, v_2, \ldots, v_n >$ and let $v_{n+1} = v$ and this must maintain linear independence. Now going back to our problem, we may simply keep adding v_{m+i} in this manner until we have a basis for V over F.

5.2.6 Question 14

Consider the candidate basis $[1], [x], \left[x^2\right], \ldots, \left[x^{\deg f(x)-1}\right]$. There are quite obviously $\deg f(x)$ elements in this so all that remains is to show it is a basis. For any $g(x) \in F[x]$, we know $[g(x)] = [h(x)]$ for some $h(x)$ with $\deg h(x) < \deg f(x)$ by the division algorithm, so this supposed basis can generate all of $F[x]/J$. Now if one were to remove $\left[x^i\right]$ then there would be no way ever get element of $\left[x^i\right]$ (with the exception of 0) as they all have order i and when we add together functions we simply take the max of their orders, and we aren't allowed multiplication so we can't ever get anything with order x^i or even with a non-zero i^{th} coefficient.

5.2.7 Question 17

(a) Because $\dim_F(K) = m$ then there is a basis $k_1, k_2, \ldots, k_m$ of K over F and thus any element of K can be represented as $\sum_{i=0}^{m} \alpha_i k_i$ with $\alpha_i \in F$ for all i. Now if V is a vector space over K then there is some basis that may or may not be finite for V over K, let us denote this basis as the set S. Now any element of V may be represented as $\sum_{v \in S} h_v v$ with $h_v \in K$ for all $v \in S$. as $h_v \in K$ we may then say $h_v = \sum_{i=0}^{m} \alpha_{v,i} k_i$ and therefore

$$\sum_{v \in S} h_v v = \sum_{v \in S} \sum_{i=0}^{m} \alpha_{v,i} k_i v$$

and $k_i v \in V$ and $\alpha v, i \in F$ so then V must be a vector space over F.

(b) If V is finite dimensional over K then using the equation we have already laid out becomes a finite sum and thus $\dim_F(V)$ must be finite.

(c) In-fact, going a step further, $\{k_i v \mid v \in S, 0 < i \leq m\}$ is a basis for V. To show this all we need it show linear independence. We know all the v are linearly independent over K and all the k_i are linearly independent over F. Assume they are not linearly independent, it follows then that there is some non-trivial solution to

$$\sum_{v \in S} \sum_{i=0}^{m} \alpha_{v,i} k_i v = 0$$

so there is some set $\alpha v, i$ that are not 0. From this we then say that if $\alpha_{w,j}$ is not zero then we get $\sum_{i=0}^{m} \alpha_{w,i} k_i \neq 0 \in K$ by the k_is forming a basis. From this we go another step and we realize that we have one $h_w \neq 0$ so again $\sum_{v \in S} h_v v \neq 0$. Now we have shown that if any coefficient is nonzero then so must the entire sum.

From this if S is finite then we have a basis of size $m\,|S|$ which is also $\dim_K(V) \dim_F(K) = \dim_F(V)$.

5.3 Section 3

5.3.1 Question 1

(a) Let $a = \sqrt{2} + \sqrt{3}$, then $a^2 = 5 + 2\sqrt{6}$ and $a^4 = 31 + 10\sqrt{6}$. so $a^4 - 5a^2 = 6$ and therefore $a^4 - 5a^2 - a = 0$.

(b) Consider $\sqrt{7}^2 - 7 = 0$ and $\sqrt[3]{12}^3 - 12 = 0$ so both $\sqrt{7}$ and $\sqrt[3]{12}$ are algebraic, and we know algebraic numbers are a field in $\mathbb{C}$ so their sum must be algebraic.

(c) 2 is algebraic as $2^2 - 2 \cdot 2^1 = 0$ and i is algebraic as $i^2 + 1 = 0$ and $\sqrt{3}$ is algebraic as $\sqrt{3}^2 - 3 = 0$ so again as the algebraic numbers are a field in $\mathbb{C}$ then $2 + i\sqrt{3}$ must be algebraic.

(d) $\cos(2\pi/k) + i\sin(2\pi/k) = e^{i2\pi/k} = a$ is algebraic when k is a positive integer as $\left(e^{i2\pi/k}\right)^k = e^{i2\pi} = 1$ so $a^k - 1 = 0$.

5.3.2 Question 4

First we have $\cos(2\pi/8)+i\sin(2\pi/8) = e^{i2\pi/8} = e^{i\pi/4}$, so now consider $\left(e^{i\pi/4}\right)^4 = e^{i\pi} = -1$ so if $f(x) = x^4+1$ then $f(e^{i\pi/4}) = 0$, so the degree can be no greater than 4. Now $f(x+1) = (x+1)^4+1 = x^4+4x^3+6x^2+4x+2$ therefore is irreducible by Einstein criterion. From this we get there are no $g(x)q(x) = f(x)$ with $\deg q(x) > 0$. Now let $g(x) \neq 0$ such that $g(e^{i\pi/4}) = 0$ with $g(x)$ being a minimal nontrivial polynomial with $g(e^{i\pi/4}) = 0$, we then would find by the division algorithm that $g(x)q(x)+r(x) = f(x)$ for some $q(x), r(x)$ with $\deg r(x) < g(x)$. Well then we would have $g(e^{i\pi/4})q(e^{i\pi/4}) + r(e^{i\pi/4}) = f(e^{i\pi/4}) = 0$ and as we assumed $g(e^{i\pi/4}) = 0$ then we have $0q(e^{i\pi/4}) + r(e^{i\pi/4}) = f(e^{i\pi/4}) = 0$ so $r(e^{i\pi/4}) = 0$ and we know $\deg r(x) < \deg g(x)$ and due to $g(x)$ being minimal then it must be that $r(x) = 0$. From this we find $g(x)q(x) = f(x)$ and as $f(x)$ is irreducible then $\deg g(x) = \deg f(x)$. Thus $e^{i\pi/4}$ is of degree 4.

5.3.3 Question 6

Let us start with

$$e = \sum_{i=0}^{\infty} \frac{1}{n!}$$

and assume for the sake of contradiction that $e \in \mathbb{Q}$, so $e = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $b \neq 0$. Now suppose

$$x = b!\left(e - \sum_{n=0}^{b} \frac{1}{n!}\right)$$

and we get two immediate results about x. First as $e = \frac{a}{b}$ we have

$$x = b!\left(\frac{a}{b} - \sum_{n=0}^{b} \frac{1}{n!}\right) = a(b-1)! - \sum_{n=0}^{b} \frac{b!}{n!}$$

and as $b > n$ for all n in the sum then we get x is an integer. Our second result is from $e = \sum\limits_{n=0}^{\infty} \frac{1}{n!}$ where we get

$$x = b!\left(\sum_{n=0}^{\infty} \frac{1}{n!} - \sum_{n=0}^{b} \frac{1}{n!}\right) = b! \sum_{n=b+1}^{\infty} \frac{1}{n!} > 0$$

so x must be a positive integer. Now consider $n \geq b+1$ and we would find

$$\frac{n!}{b!} = \prod_{k=b+1}^{n} k \geq \prod_{k=b+1}^{n} b+1 = (b+1)^{n-b}$$

and therefore

$$\frac{b!}{n!} \leq \frac{1}{(b+1)^{n-b}}$$

for any $n \geq b+1$, and further note that if $n \geq b+2$ then $\frac{b!}{n!} < \frac{1}{(b+1)^{n-b}}$. From this we now look again at x and we find

$$x = b! \sum_{n=b+1}^{\infty} \frac{1}{n!} = \sum_{n=b+1}^{\infty} \frac{b!}{n!} < \sum_{n=b+1}^{\infty} \frac{1}{(b+1)^{n-b}} = \sum_{n=1}^{\infty} (b+1)^n = \frac{1}{b} \leq 1$$

So we find our selves with $x \in Z$ and $0 < x < 1$ so we have ourselves a contradiction and thus $e \notin \mathbb{Q}$.

5.3.4 Question 10

Consider first that $1^\circ = \frac{\pi}{180}$ and therefore $\cos(1^\circ) + i\sin(1^\circ)$ is algebraic due to Question 1 part (d) of this section. Now $\cos(1^\circ) + i\sin(1^\circ) \neq 0$ so $(\cos(1^\circ) + i\sin(1^\circ))^{-1}$ must be algebraic. We find by De Moivre's theorem that $(\cos(1^\circ) + i\sin(1^\circ))^{-1} = \cos(-1^\circ) + i\sin(-1^\circ)$. Now from basic trigonometry we have $\cos(-x) = \cos(x)$ and $\sin(-x) = -\sin(x)$ so we therefore have $\cos(-1^\circ) + i\sin(-1^\circ) = \cos(1^\circ) - i\sin(1^\circ)$. Now we can take the sum of these two algebraic numbers and have

$$(\cos(1^\circ) + i\sin(1^\circ)) + (\cos(1^\circ) - i\sin(1^\circ)) = 2\cos(1^\circ)$$

must be algebraic. Now from here we multiply by $\frac{1}{2}$ which is trivially algebraic and get $\cos(1^\circ)$ which must be algebraic.

5.3.5 Question 13

K forms a vector space over F, with $\dim_F(K) = n$. This means there is a basis $b_1, b_2, \ldots, b_n$ for K over F, and each element of K has a unique representation as $\sum_{k=0}^{n} \alpha_k b_k$ with each $\alpha_k \in F$. So then simply by specifying a sequence of n elements of F we get a unique representation of a value in K so if $|F| = q$ is finite then $|K| = q^n$.

5.3.6 Question 14

If F is a finite field then F has a nonzero finite characteristic, p. We know then that p is prime, so we can construct a subfield of F isomorphic to $\mathbb{Z}_p$, by taking the 1 element and then including any number that is formed by simply adding 1 to itself repeatedly. We can call $1+1=2$ and $1+1+1=3$ and so on up till p at which point we have $1 + 1 + \ldots + 1 = 0$ because F has characteristic p. Now that we have this subfield we know that F can be viewed of as a vector space over this subfield we generated and therefore by the problem above we know that $|F| = p^n$ for some n.

5.4 Section 4

5.4.1 Question 1

Without much work one find $a^2 = 5 - 2\sqrt{3}\sqrt{2}$ and $a^4 = 49 - \sqrt{3}\sqrt{2}$ so if $f(x) = x^4 - x^2 - 44$ then $f(a) = 0$.

5.4.2 Question 3

Consider $K_0 = \mathbb{Q}(\sqrt{2})$ and we get that $[k_0 : \mathbb{Q}] = 2$, then we can construct $K_1 = K_0(\sqrt{5})$ and $K_2 = K_1(\sqrt{7})$ and finally $K_3 = K_2(\sqrt{11})$. It follows then that $[K_4 : \mathbb{Q}] = [K_4 : K_3][K_3 : K_2][K_2 : K_1][K_1 : K_0][K_0 : \mathbb{Q}]$ from the corollary to theorem 5.4.1 in the book. Each one of $[K_i : K_{i-1}] \leq 2$ so $[K_4 : \mathbb{Q}] \leq 2^4$ now we go one step further and realize $p(x) \in K_4[x]$ so for any a such that $p(a) = 0$ then $[K_4(a) : K_4 \leq \deg p(x) = 5$ and thus $[K_4(a) : \mathbb{Q}] \leq 2^4 \cdot 5 = 80$. This tells us a is an algebraic number of degree no greater than 80.

5.4.3 Question 5

Well we know $[K : T]$ is some positive integer, lets call it k and therefore if we let $h = [T : F]$ we have h also being a positive integer such that $hk = 2^n$. From this it follows that both h and k are smaller powers of 2 then 2^n.

5.4.4 Question 6

Consider $a = \sqrt[3]{2}$ and $b = 1 + \sqrt{3}i$. Now a is quite obviously of degree 3. For b we have $b^2 = 1 - 3 + 2\sqrt{3}i = -2 + 2\sqrt{3}i$, therefore $b^2 - 2b = -4$ and so we can see that b is degree 2. When we multiply together we get $ab = \sqrt[3]{2}\left(1 + \sqrt{3}i\right)$. Let us now consider

$$(ab)^3 = 2\left(1 + 3\sqrt{3}i - 9 - 3\sqrt{3}i\right) = -16$$

and therefore ab is algebraic of degree no greater than 3.

5.5 Section 5

5.5.1 Question 2

Consider $f(x) = x^3 - 3x - 1$. Suppose that it is reducible, if that is so then it would reduce into $(x^2 + ax + b)(x + c) = f(x)$ and therefore

$$x^3 + (c + a)x^2 + (ac + b)x + bc = x^3 - 3x - 1$$

so $c + a = 0$, $ac + b = -3$, and $bc = -1$. It follows from this that $a = -c$ and $c = -b^{-1}$ so $-c^2 - c^{-1} = -3$ or $c^2 + c^{-1} = 3$ and we know $c \neq 0$. Consider $c = \frac{p}{q}$ with $q > 0$ and $\gcd(p, q) = 1$, we then have $\frac{p^2}{q^2} + \frac{q}{p} = 3$, so we know

$$p^3 + q^3 = 3pq^2$$

. Now if we divide by q and rearrange a bit we get $\frac{p^3}{q} = 3pq - q^2$ so $q|p^3$ and therefore as $\gcd(p, q) = 1$, we have $q = 1$. We also can divide through by p and rearrange and get $\frac{q^3}{p} = 3q^2 - p^2$ so $p|q^3$ and again as $\gcd(p, q) = 1$ we have $p = 1$. Now we go back and see that $p^3 + q^3 = 2 \neq 3 = 3pq^2$ so we have a contradiction. Therefore $f(x)$ is irreducible in $\mathbb{Q}$.

5.5.2 Question 3

Drawing diagrams is hard in LaTeX so I will assume one is looking at the diagram in the book that the question is referring to. Consider first $\angle AEB$, which is known to be a right angle.[3] Now we will use the Pythagorean theorem to come up with a few equivalences. Now by our construction a is the length of AD and DB is our unit. Let p be the length AE, let q be the length of EB, and let h be the length of ED. Now using the Pythagorean theorem we get

$$\begin{aligned} p^2 &= a^2 + h^2 \\ q^2 &= 1^2 + h^2 \\ (a + 1)^2 &= p^2 + q^2 \end{aligned}$$

and therefore we can do some substitution and find

$$a^2 + h^2 + 1^2 + h^2 = (a + 1)^2 = a^2 + 2a + 1$$

and we can simplify to having $h^2 = a$ so therefore $h = \sqrt{a}$.

5.5.3 Question 4

Every angle in the regular heptagon will be be $\frac{5}{7}\pi$, so for a regular heptagon to be constructible we would need $\frac{5}{7}\pi$ to be a constructible angle. If we could construct the angle $\frac{5}{7}\pi$ we would also be able to construct the angle $\pi - \frac{5}{7}\pi = \frac{2}{7}\pi$. If we can construct this angle then we can surely construct a right triangle with one angle $\frac{2}{7}\pi$ and a hypotenuse of unit length. This gives us side lengths of $\cos\left(\frac{2}{7}\pi\right)$ and $\sin\left(\frac{2}{7}\pi\right)$ so both of these would need to be constructible numbers. From this we would then have $\left[\mathbb{Q}\left(\cos\left(\frac{2}{7}\pi\right), \sin\left(\frac{2}{7}\pi\right)\right) : \mathbb{Q}\right] = 2^n$ for some n. Within $\mathbb{Q}\left(\cos\left(\frac{2}{7}\pi\right), \sin\left(\frac{2}{7}\pi\right)\right)$, $e^{i\frac{2}{7}\pi} = \cos\left(\frac{2}{7}\pi\right) + i\sin\left(\frac{2}{7}\pi\right)$ would be of degree two so $\left[\mathbb{Q}\left(e^{i\frac{2}{7}\pi}\right) : \mathbb{Q}\left(\cos\left(\frac{2}{7}\pi\right), \sin\left(\frac{2}{7}\pi\right)\right)\right] = 2$ and therefore $\left[\mathbb{Q}\left(e^{i\frac{2}{7}\pi}\right) : \mathbb{Q}\right] = 2^{n+1}$. However $e^{i\frac{2}{7}\pi}$ is of degree 6 due to the polynomial $x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 1$, which is irreducible and has $e^{i\frac{2}{7}\pi}$ as a root.

[3] I do not know what the theorem that states this is called but I didn't think it relevant to prove here.

5.6 Section 6

5.6.1 Question 3

Notice that $p(x)(x-1) = x^5 - 1$. $x^5 - 1$ has as roots any number who's fifth power is 1 and therefore any number a integer multiple fifth of the way around the complex unit circle, so $e^{i\frac{2k}{5}\pi}$ for all $k \in \mathbb{Z}$ are roots of $p(x)$ with the exception of 1 as that we get from the $x-1$. This leaves us with the other four possible values as the roots. These numbers are of degree 4 as $p(x)$ is irreducible and they are roots for it, so we then get $p(x) = \prod_{i=1}^{4} \left[x - e^{i\frac{2i}{5}\pi}\right]$ so we have factorized it into 4 linear parts in $\mathbb{Q}\left(e^{i\frac{2k}{5}\pi}\right)$.

5.6.2 Question 4

Let us rewrite the coefficients of $q(x)$ so that $q(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$, this does not change the problem in any ways, simply changes the notation to be one that I prefer. To take things a step further let $a_n = 1$ and then we have

$$q(x) = \sum_{k=0}^{n} \left[a_k x^k\right]$$

Now if this thing has a rational root, then it will take the form of $\frac{s}{t}$ with s, t relatively prime and $t > 0$. So we then have

$$q\left(\frac{s}{t}\right) = \sum_{k=0}^{n} \left[a_k \frac{s^k}{t^k}\right] = 0$$

We can multiply out and get

$$t^n q\left(\frac{s}{t}\right) = t^n \sum_{k=0}^{n} \left[a_k \frac{s^k}{t^k}\right] = \sum_{k=0}^{n} \left[a_k s^k t^{n-k}\right] = 0$$

Now we isolate the first term and we have

$$\sum_{k=1}^{n} \left[a_k s^k t^{n-K}\right] + a_0 t^n = 0$$
$$\therefore s \sum_{k=1}^{n} \left[a_k s^{k-1} t^{n-K}\right] = -a_0 t^n$$

so $s | a_0 t^n$ and as $\gcd(s,t) = 1$ hen $s | a_0$. We can also go the other direction when we isolate the last term of our sum and get

$$\sum_{k=0}^{n-1} \left[a_k s^k t^{n-k}\right] + a_n s^n = 0$$
$$\therefore t \sum_{k=0}^{n-1} \left[a_k s^k t^{n-1-k}\right] = -a_n s^n$$

so $t | a_n s^n$, however remember we said $a_n = 1$ so then we have $t | s^n$ and as $\gcd(t,s) = 1$ then $t = 1$.

When we put this together we have $\frac{s}{t} = s$ and $s | a_0$ which concludes the proof. Notice that I relabeled the coefficients so a_0 is the coefficient of x^0 in $q(x)$.

5.6.3 Question 7

See solution to Section 1, Question 8 of this chapter. The problems are identical.

5.6.4 Question 8

Notice that $x^m - x$ is of degree m so it would be impossible for it to have more than m roots in any field. Now we need to show that these roots form a field, under our specified conditions. They will be the subfield of a finite extension to $\mathbb{Z}_p$ so $(a+b)^m = a^m + b^m$ for any a, b in this field

So first to show addition, assume a, b are roots of our polynomial, then

$$(a+b)^m - (a+b) = a^m + b^m - a - b = (a^m - a) + (b^m - b) = 0 + 0 = 0$$

$$(-a)^m - (-a) = -a^m + a = -(a^m - a) = -0 = 0$$

so we have the additive group.

For the multiplicative rules we again assume a, b are roots of our polynomial, then notice first that as a and b are roots that $a^m - a = 0$ so $a^m = a$ and the same for $b^m = b$, from this we get

$$(ab)^m - ab = a^m b^m - ab = ab - ab = 0$$

and if $a \neq 0$ then

$$\left(a^{-1}\right)^m - a^{-1} = a^{-m} - a^{-1} = (a^m)^{-1} - a^{-1} = a^{-1} - a^{-1} = 0$$

so we have multiplication done and thus a field.

5.6.5 Question 11

First we will denote $f(x) \in F[x]$ as

$$f(x) = \sum_{n=0}^{\infty} [f_n x^n]$$

with $a_n = 0$ for all $n > \deg f(x)$ and use this notation for any polynomial in $F[x]$. From this we also have

$$\delta(f(x)) = \sum_{n=1}^{\infty} \left[n f_n x^{n-1}\right] = \sum_{n=0}^{\infty} [(n+1) f_{n+1} x^n]$$

and that

$$f(x)g(x) = \sum_{n=0}^{\infty} \left[\sum_{k=0}^{n} [f_k g_{n-k}]\, x^n \right]$$

(a) Here we have

$$\begin{aligned}
\delta(f(x)) + \delta(g(x)) &= \sum_{n=1}^{\infty} \left[n f_n x^{n-1}\right] + \sum_{n=1}^{\infty} \left[n g_n x^{n-1}\right] \\
&= \sum_{n=1}^{\infty} \left[n(f_n + g_n) x^{n-1}\right] \\
&= \delta(f(x) + g(x))
\end{aligned}$$

(b) Now since we already have that $\delta(f(x)) + \delta(g(x)) = \delta(f(x) + g(x))$ then it follows that we only need to show that this is true for functions in the form ax^n, as we can construct other polynomials as sums of these polynomials. Now if we let $f(x) = ax^n$ and $g(x) = bx^m$ then

$$\begin{aligned}
\delta(f(x)g(x)) &= \delta(abx^{n+m}) \\
&= ab(n+m)x^{n+m-1} \\
&= abnx^{n+m-1} + abmx^{n+m-1} \\
&= nax^{n-1}bx^m + ax^n mbx^{m-1} \\
&= \delta(f(x))g(x) + f(x)\delta(g(x))
\end{aligned}$$

5.6.6 Question 14

Assuming the result from problem 13 to be true, consider $\delta(x^m - x) = mx^{m-1} - 1 = -1$, so $\delta(x^m - x)$ must be relatively prime to $x^m - x$ and therefore $x^m - x$ has no roots with multiplicity greater than 1.

5.6.7 Question 15

(a) Let $f(x) \in F[x]$ be irreducible and let $f(x) = \sum_{i=0}^{n} f_i x^i$ with $n = \deg f(x)$. If $f(x)$ has a root with multiplicity then $f(x)$ and $\delta(f(x))$ share a divisor and as $\deg \delta(f(x)) < \deg f(x)$ and as $f(x)$ is irreducible then it must be that $\delta(f(x)) = 0$. We know that $f_n \neq 0$ as otherwise $n \neq \deg f(x)$, and as $\delta(f(x)) = 0$ then $nf_n = 0$. This means that F must have multiplicity p, where p is some prime divisor of n, as otherwise $nf_n \neq 0$.

(b) Now that we have established $\delta(f(x)) = 0$ and F has characteristic p, we can show there is some $g(x) \in F[x]$ such that $f(x) = g(x^p)$. Now for any $\deg f(x) \geq k > 0$, we have $kf_k = 0$ from $\delta(f(x)) = 0$ and therefore either $f_k = 0$ or $p|k$. This means we can rewrite $f(x)$ as

$$f(x) = f_0 + f_p x^p + f_{2p} x^{2p} + \cdots + a_{kp} a^{kp}$$

with $kp = n$ and therefore if we let $g(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{kp} a^k$ then we find $f(x) = g(x^p)$.