Solutions to Problems in Abstract Algebra by Dummit and Foote (Chapter 1)

Isaac Dobes

1

1.1

1.1.1

(a) $\star$ defined on $\mathbb{Z}$ as $a \star b = a - b$ is not associative since $(a - b) - c = [a + (-b)] - c = [a + (-b)] + (-c) = a + [(-b) + (-c)] = a + [-1(b + c)] = a - (b + c)$; in general $a - (b + c) \neq a - (b - c)$; e.g., $1 - (1 + 1) = -1 \neq 1 = 1 - (1 - 1)$

(b) $\star$ defined on $\mathbb{R}$ as $a \star b = a + b + ab$ is associative. Observe that

$$(a \star b) \star c = (a + b + ab) \star c = (a + b + ab) + c + (a + b + ab)c = a + b + c + ab + ac + bc + abc$$

and

$$a \star (b \star c) = a \star (b + c + bc) = a + (b + c + bc) + a(b + c + bc) = a + b + c + ab + ac + bc + abc$$

Therefore, $(a \star b) \star c = a \star (b \star c)$.

(c) $\star$ defined on $\mathbb{Q}$ as $a \star b = \frac{a+b}{5}$ is not associative. Observe that

$$(a \star b) \star c = \left(\frac{a + b}{5}\right) \star c = \frac{\frac{a+b}{5} + c}{5} = \frac{a + b + 5c}{25}$$

and

$$a \star (b \star c) = a \star \left(\frac{b + c}{5}\right) = \frac{a + \frac{b+c}{5}}{5} = \frac{5a + b + c}{25}$$

In general, $\frac{a+b+5c}{25} \neq \frac{5a+b+c}{25}$; e.g., if $a = 1$, $b = 0$, and $c = -1$, then $(a \star b) \star c = -\frac{4}{25} \neq \frac{4}{25} = a \star (b \star c)$.

(d) $\star$ defined on $\mathbb{Z} \times \mathbb{Z}$ as $(a, b) \star (c, d) = (ad + bc, bd)$ is associative, but it is tedious to verify and thus proof of fact is omitted.

(e) $\star$ defined on $\mathbb{Q} \setminus \{0\}$ as $a \star b = \frac{a}{b}$ is not associative. Observe that

$$(a \star b) \star c = \left(\frac{a}{b}\right) \star c = \frac{\frac{a}{b}}{c}$$

and

$$a \star (b \star c) = a \star \left(\frac{b}{c}\right) = \frac{a}{\frac{b}{c}}$$

In general, $\frac{\frac{a}{b}}{c} \neq \frac{a}{\frac{b}{c}}$; e.g., $(1 \star 2) \star 3 = \left(\frac{1}{2}\right) \frac{\frac{1}{2}}{3} = \frac{1}{6}$, but $1 \star (2 \star 3) = 1 \star \left(\frac{2}{3}\right) = \frac{1}{\frac{2}{3}} = \frac{3}{2}$.

1.1.2

(a) $\star$ is not commutative on $\mathbb{Z}$; e.g., $1 - 2 = -1 \neq 2 - 1 = 1$.

(b) $\star$ defined on $\mathbb{R}$ is commutative on $\mathbb{R}$ since addition and multiplication are commutative on $\mathbb{R}$, and $\star$ merely reduces to a combination the two operations.

(c) $\star$ defined on $\mathbb{Q}$ is commutative since $a \star b = \frac{a+b}{5} = \frac{b+a}{5} = b \star a$.

(d) $\star$ defined on $\mathbb{Z} \times \mathbb{Z}$ is commutative; proof omitted.

(e) $\star$ defined on $\mathbb{Q} \setminus \{0\}$ is not commutative on $\mathbb{Q} \setminus \{0\}$; e.g., $1 \star 2 = \frac{1}{2} \neq 2 = 2 \star 1$.

1.1.3

Addition of residue classes is associative in $\mathbb{Z}/_{n\mathbb{Z}}$ because $(\overline{a} + \overline{b}) + \overline{c} = \overline{(a+b)} + \overline{c} = \overline{(a+b)+c} = \overline{(a+(b+c)} = \overline{a} + \overline{(b+c)} = \overline{a} + (\overline{b} + \overline{c})$.

1.1.4

Multiplication of residue classes is associative in $\mathbb{Z}/_{n\mathbb{Z}}$ since $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}(\overline{bc}) = \overline{a} \cdot (\overline{b} \cdot \overline{c})$.

1.1.5

Assume for the sake of contradiction that for any integer $n > 1$, $\mathbb{Z}/_{n\mathbb{Z}}$ is a group under multiplication of residue classes. Then observe that for $0 \leq k \leq n-1$, $\overline{k} \cdot \overline{1} = \overline{1} \cdot \overline{k} = \overline{k}$ (because $\forall\, i, j \in \mathbb{Z}$, $(k+in) \cdot (1+jn) = k+in+jkn+ijn^2 \in \overline{k}$). Therefore, there exists $l \in \{0, 1, ..., n-1\}$ such that $\overline{0} \cdot \overline{l} = \overline{1}$; i.e., $\overline{0}$ must have an inverse. This, however, is impossible because for any $k \in \{0, 1, ..., n-1\}$, $\overline{0} \cdot \overline{k} = \overline{k} \cdot \overline{0} = \overline{0}$. Hence, $\mathbb{Z}/_{n\mathbb{Z}}$ is not a group under multiplication of residue classes.

1.1.6

(a) Let $S = \{x \in \mathbb{Q} :$ the denominator of x in lowest terms is odd$\}$ Then for any $a, b \in S$, say with $a = \frac{w}{x}$ and $b = \frac{y}{z}$, $a + b = \frac{w}{x} + \frac{y}{z} = \frac{wz+xy}{xz}$. Now, x, z odd implies that xz is odd $\Rightarrow (a+b) \in S$. The additive identity element $0 = \frac{0}{1} \in S$, and for any $a = \frac{w}{x} \in S$, $a^{-1} = -\frac{w}{x} \in S$. Moreover, since $S \subset \mathbb{Q}$, S inherits associativity of addition. Thus, S is a group.

(b) Let $S = \{x \in \mathbb{Q} :$ the denominator of x in lowest terms is even$\} \cup \{0\}$. Then $\frac{5}{6}, -\frac{1}{2} \in S$, but $\frac{5}{6} + \left(-\frac{1}{2}\right) = \frac{1}{3} \notin S \Rightarrow S$ is not a group under addition.

(c) Let $S = \{x \in \mathbb{Q} : |x| < 1\}$. Then $\sum\limits_{k=1}^{\infty} (\frac{1}{2})^k = \frac{1}{1-\frac{1}{2}} - 1 = 1 \notin S \Rightarrow S$ is not a group under addition.

(d) Let $S = \{x \in \mathbb{Q} : |x| \geq 1\} \cup \{0\}$. Then $\frac{3}{2}, -1 \in S$, but $\frac{3}{2} + (-1) = \frac{1}{2} \notin S \Rightarrow S$ is not a group under addition.

(e) Let $S = \{x \in \mathbb{Q} :$ the denominator of x (in lowest terms) is either 1 or $2\}$. Then S is a group, and the reasoning is analogous to that in part (a).

(f) Let $S = \{x \in \mathbb{Q} :$ the denominator is 1, 2, or $3\}$. Then $\frac{3}{2}, -\frac{2}{3} \in S$, but $\frac{3}{2} + \left(-\frac{2}{3}\right) = \frac{5}{6} \notin S \Rightarrow S$ is not a group under addition.

1.1.7

Observe that for any $x, y \in G$,

$$\lfloor x+y \rfloor \leq x+y < \lfloor x+y \rfloor + 1$$

$$\Rightarrow 0 \leq x+y+\lfloor x+y \rfloor < 1$$

$\Rightarrow x \star y \in G$. Thus, $\star$ is a well-defined binary operation on G. Since $G \subset \mathbb{R}$, G inherits associativity and commutivity under addition, which implies $\star$ is associative and commutative on G. Also, if $x \in G$, then $x \star 0 = x + 0 - \lfloor x+0 \rfloor = x + \lfloor x \rfloor = x \Rightarrow 0 \in G$ is the identity element. Lastly, if $x \in G \setminus \{0\}$, then $x \star (1-x) = x + (1-x) - \lfloor 1+x \rfloor = 1 - 1 = 0 \Rightarrow x^{-1} = (1-x) \in G$, and $0^{-1} = 0 \in G$. $\therefore G$ is an abelian group under $\star$.
NOTE: G is called the "real numbers mod 1".

1.1.8

(a) Since $G \subset \mathbb{C}$, G inherits associativity and commutivity of multiplication. Also, the multiplicative identity $1 \in \mathbb{C}$ is in G (because $1^1 = 1$). Now, if $z \in G$, then for some $n \in \mathbb{N}$, $z^n = 1$. Therefore, $z \cdot z^{n-1} = z^n = 1 \Rightarrow z^{-1} = z^{n-1}$; moreover, $(z^{n-1})^n = z^{n(n-1)} = (z^n)^{n-1} = 1^{n-1} = 1 \Rightarrow z^{-1} \in G$. Lastly, if $z_1, z_2 \in G$, then there exists $n_1, n_2 \in \mathbb{N}$ such that $z_1^{n_1} = 1 = z_2^{n_2} \Rightarrow (z_1 z_2)^{n_1 n_2} = z_1^{n_1 n_2} z_2^{n_1 n_2} = (z_1)^{n_2}(z_2)^{n_1} = 1^{n_2} 1^{n_1} = 1 \Rightarrow z_1 z_2 \in G$. Hence, G is an abelian group under multiplication.

(b) Observe that $1 \in G$, but $1 + 1 = 2 \notin G \Rightarrow G$ is not closed under addition; thus, G is not a group under addition.

NOTE: G, in part (a), is called the "n^{th} roots of unity."

1.1.9

(a) Since $G \subset \mathbb{R}$, G inherits associativity and commutivity of addition. Also, the additive identity $0 = 0 + 0\sqrt{2} \in G$. Now, if $a + b\sqrt{2} \in G$ and $c + \sqrt{d} \in G$, then $a + b\sqrt{2} + c + d\sqrt{2} = (a+c) + (b+d)\sqrt{2}$; since $a, b, c, d \in \mathbb{Q}$, this implies $(a+c) \in \mathbb{Q}$ and $(b+d) \in \mathbb{Q} \Rightarrow (a+c) + (b+d)\sqrt{2} \in G$. And lastly, if $a + b\sqrt{2} \in G$, then observe that $\left(a + b\sqrt{2}\right) + \left((-a) + (-b)\sqrt{2}\right) = (a + (-a)) + (b + (-b))\sqrt{2} = 0 \Rightarrow (a + b\sqrt{2})^{-1} = (-a) + (-b)\sqrt{2}$; now, $a, b \in \mathbb{Q} \Rightarrow (-a), (-b) \in \mathbb{Q} \Rightarrow (a + b\sqrt{2})^{-1} \in G$. Thus, G is an abelian group under addition.

(b) We now want to show that the nonzero elements of G form an abelian group under multiplication. First note that since $G \setminus \{0\} \subset \mathbb{R}$, $G \setminus \{0\}$ inherits associativity and commutivity of multiplication. Also, the multiplicative identity $1 = 1 + 0\sqrt{2} \in G \setminus \{0\}$. Now, if $a + b\sqrt{2} inG$ and $c + d\sqrt{2} \in G$, then $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2} \in G$, since $a, b, c, d \in \mathbb{Q} \Rightarrow (ac+2bd), (ad+bc) \in \mathbb{Q}$. And lastly, if $a + b\sqrt{2} \in G \setminus \{0\}$, then a or b is nonzero; therefore, $(a+b\sqrt{2}) \cdot \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a^2-2b^2}{a^2-2b^2} = 1 \Rightarrow (a+b\sqrt{2})^{-1} = \frac{a-b\sqrt{2}}{a^2-2b^2}$, and this is well defined since the a or b is nonzero implies that the denominator is nonzero. Moreover, $\frac{a-b\sqrt{2}}{a^2-2b^2} = \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{b}{a^2-2b^2}\right)\sqrt{2} \in G$ since $a, b, c, d \in \mathbb{Q} \Rightarrow \left(\frac{a}{a^2-2b^2}\right), \left(\frac{b}{a^2-2b^2}\right) \in \mathbb{Q}$. $\therefore G \setminus \{0\}$ is an abelian group under multiplication.

1.1.10

Given a finite group $G = \{x_1, x_2, ..., x_n\}$ with binary operation $\star$, we can represent it with its Cayley table as shown below:

$\star$	x_1	x_2	...	x_n
x_1	a_{11}	a_{12}	...	a_{1n}
x_2	a_{21}	a_{22}	...	a_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_n	a_{n1}	a_{n2}	...	a_{nn}

The Cayley table is symmetric $\iff \forall\, i, j \in [n], a_{ij} = a_{ji} \iff x_i \star x_j = x_j \star x_i$. $\therefore G$ is abelian if and only if its Cayley table is symmetric.

1.1.11

This problems requires only straightforward computation (boring!); recall, however, that since $\mathbb{Z}/_{12\mathbb{Z}}$ is an additive group, for $n \in \mathbb{N}$, $x^n = \sum_{k=1}^{n} x$. Thus, the orders of the elements are:

$$
\begin{aligned}
|0| &= 1 & |6| &= 2 \\
|1| &= 12 & |7| &= 12 \\
|2| &= 6 & |8| &= 3 \\
|3| &= 4 & |9| &= 4 \\
|4| &= 3 & |10| &= 6 \\
|5| &= 12 & |11| &= 12
\end{aligned}
$$

1.1.12

Another straightforward computation. Note, however, that this time for $n \in \mathbb{N}$, $x^n = \prod_{k=1}^{n} x$ since $(\mathbb{Z}/_{12\mathbb{Z}})^{\times}$ is a group under multplication (of residue classes). Thus, the order of the elements are:

$$
\begin{aligned}
|1| &= 1 & |7| &= 2 \\
|-1| &= 2 & |-7| &= 2 \\
|5| &= 2 & |13| &= 1 \text{ since } 13 \equiv 1 \pmod{13}
\end{aligned}
$$

1.1.13

Omitted because it is analogous to 1.1.11.

1.1.14

Omitted because it is analogous to 1.1.12.

1.1.15

Let $e \in G$ be the identity element.

$$
\begin{aligned}
(a_1 \cdot ... \cdot a_{n-1}a_n)(a_n^{-1}a_{n-1}^{-1} \cdot ...a_1^{-1}) &= (a_1 \cdot ... \cdot a_{n-1})(a_n a_n^{-1})(a_{n-1}^{-1} \cdot ...a_1^{-1}) \\
&= (a_1 \cdot ... \cdot a_{n-1})e(a_{n-1}^{-1} \cdot ... \cdot a_1^{-1}) \\
&= (a_1 \cdot ... \cdot (a_{n-1}a_{n-1}^{-1}) \cdot ... \cdot a_1^{-1}) \\
&= (a_1 \cdot ... \cdot)e(\cdot ... \cdot a_1^{-1}) \\
&\vdots \\
&= (a_1 a_1^{-1}) \\
&= e
\end{aligned}
$$

$\Rightarrow (a_1 \cdot ... \cdot a_{n-1}a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \cdot ...a_1^{-1}$

1.1.16

In this problem, 1 denotes the identity element of G.

Now, if $x^2 = 1$, then this implies $|x| \le 2$. By definition, the order of an element $x \in G$ is a positive integer; therefore, $|x| = 1$ or $|x| = 2$.

Conversely, if $|x| = 1$, then $x^1 = x = 1 \Rightarrow x$ is the identity element $\Rightarrow x^2 = x \cdot x = x = 1$. If, however, $|x| = 2$, then by definition $x^2 = 1$.

1.1.17

Observe that $|x| = n \Rightarrow x^n = 1 \Rightarrow (x^n)^{n-1} = 1^{n-1} \iff x^{n(n-1)} = 1 \iff x^n x^{n-1} = 1 \Rightarrow x^{-1} = x^{n-1}$.

1.1.18

Trivial.

1.1.19

This problem is not particularly illuminating and tedious, so it is omitted; nonetheless we will take the results for granted.

1.1.20

Let e be the identity element in G and $n \in \mathbb{N}$. Then if $|x| = n$, then $x^n = e \Rightarrow (x^{-1})^n = x^{-n} = (x^n)^{-1} = e^{-1} = e$, since $e \cdot e = e$. Therefore, $|x^{-1}| \le n$. Substituting x^{-1} for x, and vice versa, we obtain the result $|x^{-1}| = n \Rightarrow |x| \le n$; hence, for finite order, $|x| = |x^{-1}|$.

Now, suppose $|x| = \infty$ and assume for the sake of contradiction that $|x^{-1}| < \infty$. Then there exists $m \in \mathbb{N}$ such that $(x^{-1})^m = e \iff x^{-m} = e \Rightarrow x^m x^{-m} = x^m \iff x^{m-m} = x^m \iff x^0 = x^m \iff e = x^m \Rightarrow |x| < \infty$, a contradiction. Thus, $|x| = \infty \Rightarrow |x^{-1}| = \infty$; subsituting x^{-1} for x, and vice versa, we see that $|x^{-1}| = \infty \Rightarrow |x| = \infty$.

Consequently, for any element $x \in G$, x and x^{-1} have the same order.

1.1.21

Let e be the identity element of G. Suppose $x \in G$ has order n, where n is an odd number. Then $n = 2k - 1$ for some integer $k \ge 1$, and we thus have:

$$x^n = e \iff x^{2k-1} = e \iff x^{2k}x^{-1} = e$$

$$\Rightarrow x^{2k} = x \iff (x^2)^k = x$$

1.1.22

Let e be the identity element in G. I claim that for any $n \in \mathbb{N}$, $y = gxg^{-1} \Rightarrow y^n = g{-}1x^n g$. We use induction to prove this claim.

Base Case: Suppose $y = g^{-1}xg$. Then $y^2 = y \cdot y = g^{-1}xg \cdot g^{-1}xg = g^{-1}x(gg^{-1})xg = g^{-1}xexg = g^{-1}x^2g$.

Induction Hypothesis: Suppose for $n \in \mathbb{N}$, $y = g^{-1}xg \Rightarrow y^n = g^{-1}x^n g$.

Induction Step: Observe that $y^{n+1} = y^n \cdot y = g^{-1}x^n g \cdot g^{-1}xg = g^{-1}x^n(gg^{-1})xg = g^{-1}x^n exg = g^{-1}x^{n+1}g$.

Now, let $n \in \mathbb{N}$. Suppose $|x| = n$. Then $(g^{-1}xg)^n = g^{-1}x^n g = g^{-1}eg = e \Rightarrow |g^{-1}xg| \le n$. On the other hand, suppose $|g^{-1}xg| = n$. Then $(g^{-1}xg)^n = e \iff g^{-1}x^n g = e \Rightarrow gg^{-1}x^n gg^{-1} = geg^{-1} \Rightarrow x^n = e \Rightarrow |x| \le n$. Therefore, for finite order, $|x| = |g^{-1}xg|$.

Suppose $|x| = \infty$, and assume for the sake of contradiction that $|g^{-1}xg| < \infty$. Then there exists $m \in \mathbb{N}$ such that $(g^{-1}xg)^m = e \iff g^{-1}x^n g = e \Rightarrow gg^{-1}x^n gg^{-1} = geg^{-1} \Rightarrow x^n = e$, which contradicts the assumption that $|x| = \infty$. Therefore, $|x| = \infty \Rightarrow |g^{-1}xg| = \infty$. On the other hand, suppose that $|g^{-1}xg| = \infty$, and assume for the sake of contradiction that $|x| < \infty$. Then there exists $m \in \mathbb{N}$ such that $x^m = e$. Consequently, $(g^{-1}xg)^m = g^{-1}x^m g = g^{-1}eg = e$, which contradicts the assumption that $|g^{-1}xg| = \infty$. Therefore, $|g^{-1}xg| = \infty \Rightarrow |x| = \infty$.

Thus, given any two elements x and g in the group G, $|x| = |g^{-1}xg|$. Now, set $x := ab$ and $g := a$. Then $|ab| = |x| = |g^{-1}xg| = |a^{-1}aba| = |ba|$; hence we conclude that for any $a, b \in G$, $|ab| = |ba|$.

1.1.23

Let e be the identity element of G. Then $|x| = n = st \Rightarrow x^{st} = e \iff (x^s)^t = e \Rightarrow |x^s| \leq t$. Now, if $|x^s| = k < t$, then $(x^s)^k = e \iff x^{sk} = e \Rightarrow |x| \leq sk < st$, which contradicts the assumption that $|x| = n = st$. $\therefore |x| = st \Rightarrow |x^s| = t$.

1.1.24

Let e be the identity element of G. We are told that $a, b \in G$ commute. First we use induction to prove that for any nonnegative integer n, $(ab)^n = a^n b^n$.
<u>First Base Case $(n = 0)$</u>: Observe that $(ab)^0 = e = a^0 b^0$
<u>Second Base Case $(n = 1)$</u>: Observe that $(ab)^1 = ab = a^1 b^1$.
<u>Induction Hypothesis $(n = k)$</u>: Suppose for some positive integer $k \geq 2$ we have $(ab)^k = a^k b^k$.
<u>Induction Step $(n = k + 1)$</u>: Observe that $(ab)^{k+1} = (ab)^k (ab)^1 = a^k b^k (ab) = a^{k+1} b^{k+1}$, since the a can commute with each of the k-many b's, one at a time.

To prove that for any arbitrary integer n, $(ab)^n = a^n b^n$, we prove the following lemma:

Lemma 1. *Let G be a group. If $a, b \in G$ commute, then $a^{-1}, b^{-1} \in G$ commute.*

Proof. $ab = ba \iff a^{-1}ab = a^{-1}ba \iff b = a^{-1}ba \iff b^{-1}b = b^{-1}a^{-1}ba \iff e = b^{-1}a^{-1}ba \Rightarrow (ba)^{-1} = b^{-1}a^{-1}$. On the other hand, by proposition 1, $(ab)^{-1} = b^{-1}a^{-1}$ and $(ba)^{-1} = a^{-1}b^{-1}$. Therefore,

$$(ab)^{-1} = b^{-1}a^{-1} = (ba)^{-1} = a^{-1}b^{-1}$$

That is, $a^{-1}b^{-1} = b^{-1}a^{-1}$. □

We can now use the above lemma to prove that for any integer n, n $(ab)^n = a^n b^n$. We prove this identity using induction in a manner completely analogous to that above, with k being subsitituted with $-k$ and with $k + 1$ being substituted with $-k - 1$.

1.1.25

Let e be the identity element of G, and let $x \in G$. Then $x^2 = e$; this implies that $x = x^{-1}$. Therefore, if $a, b \in G$, then

$$ab = a^{-1}b^{-1} = (ba)^{-1} = ba$$

Thus, for any $a, b \in G$, $ab = ba$; i.e., G is abelian.

1.1.26

Let e be the identity element of the group G with binary operation $\star$. The since $H \subset G$, H inherits associativity of elements under $\star$. Also, we are told that H is closed under $\star$ and under inverses. Thus, $h \in H \Rightarrow h^{-1} \in H \Rightarrow h \star h^{-1} = e \in H$. Hence, H is a group under $\star$.

1.1.27

Let e be the identity element in G equipped with binary operation $\star$. Observe that if $x \in G$, then for any integer n, $x^n \in G$ (since groups are closed under their binary operation and inverses); thus, $\{x^n : n \in \mathbb{Z}\} \subset G$. Due to previous exercise, it thus suffices to show that H is closed under $\star$ and under inverses; i.e., we want to show that $h, k \in \{x^n : n \in \mathbb{Z}\} \Rightarrow hk \in \{x^n : n \in \mathbb{Z}\}$ and $h^{-1}, k^{-1} \in \{x^n : n \in \mathbb{Z}\}$. Accordingly, let $h, k \in \{x^n : n \in \mathbb{Z}\}$. Then there exist integers $m, n \in \mathbb{Z}$ such that $h = x^m$ and $k = x^n$. Therefore, $hk = x^m x^n = x^{m+n} \in \{x^n : n \in \mathbb{Z}\}$; moreover, $h^{-1} = (x^m)^{-1} = x^{-m} \in \{x^n : n \in \mathbb{Z}\}$, and likewise $k^{-1} = (x^n)^{-1} = x^{-n}\{x^n : n \in \mathbb{Z}\}$.

1.1.28

(a) Recall that is A and B are groups equipped (respectively) with the binary operations $\star$ and $\diamond$, then $A \times B = \{(a, b) : a \in A \wedge b \in B\}$ and for any $(a_1, b_1), (a_2, b_2) \in A \times B$, $(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$. Let e_A and e_B be the identity elements (respectively) of A and B. Then note that $(e_A, e_B) \in A \times B$ (since $e_A \in A \wedge e_B \in B$) and observe that for any $(a, b) \in A \times B$, $(e_A, e_B)(a, b) = (e_A \star a, e_B \diamond b) = (a, b) \Rightarrow A \times B$ has an identity element. Also, if $(a, b) \in A \times b$, then note that $(a^{-1}, b^{-1}) \in A \times B$ (since $a^{-1} \in A \wedge b^{-1} \in B$) and observe that $(a, b)(a^{-1} b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (e_A, e_B) \Rightarrow (a, b)^{-1} \in A \times B$; i.e., $A \times B$ is closed under inverses. Moreover, for any $(a_1, b_1), (a_2, b_2) \in A \times B$, observe that $(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2) \in A \times B$ since $(a_1 \star a_2) \in A$ and $b_1 \diamond b_2 \in B$; i.e., $A \times B$ is closed under its binary operation. Lastly, observe that for any $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B$, then $\big((a_1, b_1)(a_2, b_2)\big)(a_3, b_3) = (a_1 \star a_2, b_1 \diamond b_2)(a_3, b_3) = \big((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3)\big) = \big(a_1(a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3)\big) = (a_1, b_1)\big((a_2, b_2)(a_3, b_3)\big) \Rightarrow$ associativity holds.

(b) In part (a) we showed that the identity element is (e_A, e_B).

(c) In part (a) we showed that the inverse of (a, b) is (a^{-1}, b^{-1})

1.1.29

Let $(a_1, b_1), (a_2, b_2) \in A \times B$. Then A and B abelian implies that:

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2) = (a_2 \star a_1, b_2 \diamond b_1) = (a_2, b_2)(a_1, b_1)$$

$\Rightarrow A \times B$ is an abelian group.

1.1.30

As before we denote the identity element of A as e_A and the identity element of B as e_B. Observe that

$$(a, e_B)(e_A, b) = (a \star e_A, e_B \diamond b) = (a, b)$$

and

$$(e_A, b)(a, e_A) = (1 \star a, b \diamond e_B) = (a, b)$$

$\therefore (a, e_B)$ and (e_A, b) commute.

Now, if for some $n \in \mathbb{N}$, $|(a, b)| = n$, then n is the smallest positive integer such that

$$
\begin{aligned}
(a, b)^n &= (e_A, e_B) \\
\Rightarrow \prod_{k=1}^{n} (a, b) &= (e_A, e_B) \\
\iff \prod_{k=1}^{n} (a, e_B)(e_A, b) &= (e_A, e_B) \qquad (\triangle)
\end{aligned}
$$

Since (a, e_B) and (e_A, b) commute, $(\triangle)$ implies that n must be so that $a^n = e_A$ and $b^n = e_B$; that is, n must be a multple of $|a|$ and $|b|$. Since by definition of order, n must also be the smallest such n, we conclude that n must be the least common multiple of $|a|$ and $|b|$.

1.1.31

Let e be the identity element in G, a finite group of even order, and let $t(G) := \{g \in G : g \neq g^{-1}\}$. Note that $t(G) = \{g \in G : |g| > 2\}$ since $|g| = 2 \Rightarrow g^2 = e \iff g = g^{-1}$, and the only element in G with order 1, e, is of course its own inverse. Now, we want to show that G contains an element of order 2.

Assume for the sake of contradiction that G does not contain any elements of order 2. Then $G = e \cup t(G)$. Necessarily $t(G)$ is non-empty since $G \ni e$ and $|G| \geq 2$. Now, if $g \in t(G)$, then also $g^{-1} \in t(G)$ since $(g^{-1})^{-1} = g \neq g^{-1}$; i.e., $g^{-1} \neq (g^{-1})^{-1}$. Thus for each element $g \in t(G)$, we may pair it with its inverse in $t(G)$, which is distinct from itself (as shown above) and distinct from all other inverses in $t(G)$ (because if $g, h \in t(G)$ have the same inverse a, then $ga = e = ha \Rightarrow g = h$). Therefore, $t(G)$ has even order. This, however, is a contradiction since $G = e \cup t(G)$ implies that $|G|$ has odd order. Hence, there must be some element $\hat{g} \in G$ such that $\hat{g} \notin e \cup t(G)$; i.e., G must contain an element of order 2.

1.1.32

Let e be the identity element. We are told that $x \in G$ has order n, and we want to show that $\{e, x, ..., x^{n-1}\}$ are distinct.

Assume for the sake of contradiction that not all elements in $\{e, x, ..., x^{n-1}\}$ are distinct; i.e., suppose there exists integers i, j such that $0 \leq i, j \leq n-1$ such that $x^i = x^k$. Without loss of generality we may assume that $i > j$. Then

$$x^i = x^j \iff x^i \cdot x^{-j} = x^j \cdot x^{-j} \iff x^{i-j} = e$$

Now, $0 < i - j < n$, which contradicts the assumption that $|x| = n$.

Thus, each of the n elements in the set $\{e, x, ..., x^{n-1}\}$ are distinct; moroever, closure of groups implies that $\{e, x, ..., x^{n-1}\} \subseteq G \Rightarrow |G| \geq n$.

1.1.33

Let e be the identity element of G.

(a) x has odd order implies that there exists a positive integer k such that $x^{2k+1} = e$. Now, assume for the sake of contradiction that there exists and integer $i \in \{1, 2, ..., n-1\}$ such that $x^i = x^{-i}$. Then

$$x^i = x^{-i} \Rightarrow x^i \cdot x^i = x^{-i} \cdot x^i \iff x^{2i} = e$$

Necessarily, $2i > 2k+1$ since $|x| = 2k+1 \neq 2i$, and note that $2i < 2(2k+1)$. Consequently, $0 < 2i - (2k+1) = 2(i-k) + 1 < 2k+1$, which implies:

$$e = x^{2i} = x^{2(i-k)+1} \cdot x^{2k+1} = x^{2(i-k)+1} \cdot e = x^{2(i-k)+1}$$

which contradicts the assumption that $|x| = 2k+1$. Hence, $x^i \neq x^{-i}$ for all $i = 1, 2, ..., n-1$.

(b) $|x| = n = 2k$, for some positive integer k. Now, observe that for an integer $i \in \{1, 2, ..., n-1\}$,

$$x^i = x^{-i} \iff x^i \cdot x^i = x^{-i} \cdot x^i \iff x^{2i} = e$$

Necessarily, $2i \geq 2k$ since $|x| = 2k$, and note that $2i < 2(2k)$. Now, if $2i > 2k$, then $0 < 2i - 2k = 2(i-k) < 2k$, which implies:

$$e = x^{2i} = x^{2(i-k)} \cdot x^{2k} = x^{2(i-k)} \cdot e = x^{2(i-k)}$$

which contradicts the assumption that $|x| = 2k$. Hence, $2i \leq 2k \Rightarrow i = k$.

Conversely, observe that if $i = k$, then

$$(x^i)^2 = (x^k)^2 = x^{2k} = e$$

$\Rightarrow x^i = (x^i)^{-1} = x^{-i}$

1.1.34

Let e be the identity element of G. $|x| = \infty \Rightarrow \forall\ n \in \mathbb{N}$, $x^n \neq e$. It thus follows that $\forall\ n \in \mathbb{N}$, $x^{-n} \neq e$. Hence, the only integer m such that $x^m = e$ is $m = 0$. Now, assume for the sake of contradiction that there exists integers $i, j \in \mathbb{Z} \setminus \{0\}$ such that $x^i = x^j$. Without loss of generality we may assume that $i > j$. Then $x^i = x^j \iff x^{i-j} = e \Rightarrow |x| \leq i - j < \infty$, which contradicts the assumption that $|x| = \infty$.

1.1.35

Let e be the identity element of G. We are told that $|x| = n < \infty$. Let $k \in \mathbb{Z}$. Then by the division algorithm, there exists integers q and r, with $0 \leq r < n$, such that $k = nq + r$. Hence,

$$x^k = x^{nq+r} = x^{nq} \cdot x^r = (x^n)^q \cdot x^r = e^q \cdot x^r = x^r$$

$\Rightarrow x^k \in \{e, x, x^2, ..., x^{n-1}\}$.

1.1.36

We are told that $G = \{1, a, b, c\}$, where 1 is the identity element of G, and every element in G has order ≤ 3. Suppose a has order 3. Then $a \neq a^2$, otherwise that would imply that $a = e$. Thus, $a^2 = b$ or $a^2 = c$.

If $a^2 = b$, then $b^2 = (a^2)^2 = a^4 = a^3 \cdot a = e \cdot a = a$. Now, consider ca. Then $ca \neq e$ since $a^{-1} = a^2 = b \neq c$, $ca \neq a$ since $c \neq e$, $ca \neq c$ since $a \neq e$; and lastly, $ca \neq b$ since $b = a^2$, which would imply $ca = a^2 \Rightarrow c = a$ which is impossible. Thus, $ca \notin G$, contradicting closure of groups. Therefore, $a^2 \neq b$. An analogous argument shows that $a^2 \neq c$. Hence, a cannot have order 3; i.e., a has an order of 2.

Since we arbitrarily picked a in the above argument, we conclude that b and c also have order 2. Thus, we have the following table: Thus, it is clear (atleast upon some inspection) that there is only one unique way to finish this table,

G	1	a	b	c
1	1	a	b	c
a	a	1		
b	b		1	
c	c			1

and it is the following configuration:

G	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Since the Cayley table is symmetric, by exercise 1.1.10 we deduce that G is abelian.

1.2

1.2.1

(a) The order of elements in D_6 are:

$$|1| = 1 \qquad |s| = 2$$
$$|r| = 3 \qquad |sr| = 2$$
$$|r^2| = 3 \qquad |sr^2| = 2$$

(b) The order of elements in D_8 are:

$$\begin{aligned} |1| &= 1 & |s| &= 2 \\ |r| &= 4 & |sr| &= 2 \\ |r^2| &= 2 & |sr^2| &= 2 \\ |r^3| &= 4 & |sr^3| &= 2 \end{aligned}$$

(c) The order of elements in D_{10} are:

$$\begin{aligned} |1| &= 1 & |s| &= 2 \\ |r| &= 5 & |sr| &= 2 \\ |r^2| &= 5 & |sr^2| &= 2 \\ |r^3| &= 5 & |sr^3| &= 2 \\ |r^4| &= 5 & |sr^4| &= 2 \end{aligned}$$

1.2.2

We are given the presentation of the Dihedral group of order $2n$:

$$D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$$

Therefore, if $x \in D_{2n}$ is not a power of r, then $x = sr^i$, where $i \in \{0, 1, ..., n-1\}$. Therefore, $rx = rsr^i = sr^{-1}r^i = sr^{i-1}$, and $xr^{-1} = sr^i r^{-1} = sr^{i-1}$. Hence, $rx = xr^{-1}$.

1.2.3

As before, if $x \in D_{2n}$ is not a power of r, then $x = sr^i$ where $i \in \{0, 1, ..., n-1\}$.

Suppose $i = 0$. Then $x = s \Rightarrow x^2 = s^2 = 1 \Rightarrow |x| \leq 2$. Moreover, $s \neq 1$ and only $1 \in D_{2n}$ has order 1; hence, $|s| = 2$.

Now suppose $i \in \{0, 1, ..., n-1\}$ is nonzero. Then,

$$x^2 = (sr^i)^2 = sr^i sr^i = sr^{i-1} rsr^i = sr^{i-1} sr^{-1} r^i = sr^{i-1} sr^{i-1}$$

Repeating this algebraic manipulation at most finitely many times (eventually) yields the equality: $x^2 = sr^0 sr^0 = s^2 = 1 \Rightarrow |x| \leq 2$. Again, $sr^i \neq 1$ and only $1 \in D_{2n}$ has order 1; hence, $|x| = 2$.

Observe that $s \circ sr = s^2 r = r \Rightarrow \{s, sr\}$ generates $\{r, s\} \subset D_{2n}$. Since $\{r, s\}$ generates D_{2n}, this implies that $\{s, sr\}$ generates D_{2n}.

1.2.4

We are told $D_{2n} = D_{2(2k)}$ for $k \geq 1$. Let $z = r^k$. Then since $1 \geq k < n$, $z \neq 1$; hence, $|z| > 1$. Now, observe that:

$$z^2 = (r^k)^2 = r^{2k} = r^n = 1$$

$\Rightarrow |z| \leq 2 \Rightarrow |z| = 2$.

Observe that if $i \in \{0, 1, ..., n-1\}$, then $r^k r^i = r^{k+i} = r^{i+k} = r^i r^k$; hence, r^k commutes with the rotations in D_{2n}. Also, observe that $r^k s = r^k - 1rs = r^{k-1} sr^{-1} = ... = sr^{-k}$; since $|r^k| = 2 \Rightarrow (r^k)^{-1} = r^k \Rightarrow sr^{-k} = s(r^k)^{-1} = sr^k$. Therefore, for any $i \in \{0, 1, ..., n-1\}$, $r^k sr^i = sr^k r^i = sr^{k+i} = sr^{i+k} = sr^i r^k$. Thus, r^k commutes with every element in D_{2n}.

Now, suppose $x \in D_{2n}$ and x commutes with every element in D_{2n}. Then, if $x = r^i$ or $x = sr^j$ for $i, j \in \{0, 1, ..., n-1\}$. Suppose $x = r^i$. Then,

$$r^i s = r^{i-1} rs = r^{i-1} sr^{-1} = ... = sr^{-i}$$

$\Rightarrow sr^{-i} = sr^i \iff r^{-i} = r^i \iff 1 = r^{2i} \Rightarrow i = 0$ or $i = k$. Now, suppose $x = sr^j$ with $j \in \{0, 1, ..., n-1\}$. Then,

$$(sr^j)r = r(sr^j) \iff sr^{j+1} = rsr^j \iff sr^{j+1} = sr^{-1}r^j \iff sr^{j+1} = sr^{j-1} \iff r^{j+1} = r^{j-1}$$

$\Rightarrow j = 0$ since for each $j \in \{1, ..., n-1\}$, r^{j+1} and r^{j-1} are distinct; however, $r = r^{-1}$. Therefore, r^k is the only non-identity element in D_{2n} to commute with every other element.

1.2.5

Assume for the sake of contradiction that there exists a non-identity element $x \in D_{2n}$, where $n \geq 3$ is odd, which commutes with every element in D_{2n}. Then, $x = r^i$ for $i \in \{1, ..., n-1\}$ or $x = r^j$ for $j \in \{0, 1, ..., n-1\}$.

Suppose $x = r^i$. Then, $r^i s = sr^i$ and $r^i s = r^{i-1}rs = r^{i-1}sr^{-1} = ... = sr^{-i}$. Hence, $sr^{-i} = sr^i \iff r^i = r^i \iff 1 = r^{2i}$. Now, $1 \leq i < n \Rightarrow i$ is not a multiple of n, and n is odd $\Rightarrow 2i \neq n$; thus, we have a contradiction since only r^{kn}, where $k \in \mathbb{Z}$, equals 1.

Now, suppose $x = sr^j$. Then, $(sr^j)r = r(sr^j)$ and $r(sr^j) = rsr^j = sr^{-1}r^j = sr^{j-1}$

$$\Rightarrow (sr^j)r = sr^{j-1} \iff sr^{j+1} = sr^{j-1} \iff r^{j+1} = r^{j-1}$$

$\Rightarrow j = 0$. Hence, $x = s$. But then this implies that $sr = rs$; $rs = sr^{-1} \Rightarrow sr = sr^{-1} \iff sr^2 = s \iff r^2 = 1$ which is impossible since, again, only r^{kn}, where $k \in \mathbb{Z}$, equals 1 and $n \geq 3$.

Therefore, only the identity commutes with every element in D_{2n} for $n \geq 3$ odd.

1.2.6

Since x and y have order 2, this implies that $x = x^{-1}$ and $y = y^{-1}$. Morover, since $t = xy \Rightarrow t^{-1} = (xy)^{-1} = y^{-1}x^{-1}$. Hence,

$$tx = (xy)x = xyx = xy^{-1}x^{-1} = x(xy)^{-1} = xt^{-1}$$

1.2.7

We want to show that $\langle a, b | a^2 = b^2 = (ab)^n = 1 \rangle = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$, where $a = s$ and $b = sr$. Recall from exercise 1.2.3 that s and sr generate D_{2n}; hence, it suffices to show that the relations of the two group presentations are equivalent. Observe that

$$a^2 = (ab)^n = 1 \iff s^2 = [s(sr)]^n = 1 \iff s^2 = (s^2 r)^n = 1 \iff s^2 = r^n = 1$$

and

$$b^2 = 1 \iff (sr)^2 = 1 \iff srsr = 1 \iff rs = s^1 r^{-1} \iff rs = sr^{-1}$$

since $|s| = 2$, i.e. $s = s^{-1}$. Therefore, $\langle a, b | a^2 = b^2 = (ab)^n = 1 \rangle$, where $a = s$ and $b = sr$, gives a presentation for D_{2n}.

1.2.8

Since $r^0 = r^n = 1$, $|\langle r \rangle| = \{1, r^1, ..., r^{n-1}\} \Rightarrow |\langle r \rangle| = n$.

For problems 1.2.9-1.2.13, we find the order of the group G of rigid motions in $\mathbb{R}^3$ of a given Platonic solid by finding the number of places to which a given face may be sent to, and once a face is fixed, the number of positions to which a vertex on that face may be sent.

1.2.9

In this problem, G is the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. A tetrahedron has 4 faces, where each face is triangle $\Rightarrow$ there are 3 different positions that a vertex on a face may be sent; hence, the order of G is 12.

1.2.10

In this problem, G is the group of rigid motions in $\mathbb{R}^3$ of a cube. A cube has 6 faces, where each face is a square $\Rightarrow |G| = 6 \cdot 4 = 24$.

1.2.11

In this problem, G is the group of rigid motions in $\mathbb{R}^3$ of a octahedron. An octahedron has 8 faces, where each face is a triangle $\Rightarrow |G| = 8 \cdot 3 = 24$.

1.2.12

In this problem, G is the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. A dodecahedron has 12 faces, where each face is a pentagon $\Rightarrow |G| = 12 \cdot 5 = 60$.

1.2.13

In this problem, G is the group of rigid motions in $\mathbb{R}^3$ of a icosahedron. An icosahedron has 202 faces, where each face is a triangle $\Rightarrow |G| = 20 \cdot 3 = 60$.

1.2.14

For any positive integer n, $\sum\limits_{k=1}^{n} 1 = n \Rightarrow 1$ generates all positive integers $\mathbb{N}$. Similarly, -1 generates all negative integers, $(1)^{-1} = (-1)$, and $1 + (-1) = 0$; hence, $\langle 1 \rangle = (\mathbb{Z}, +)$.

1.2.15

For any integer $m \in [n-1]$, $\sum\limits_{k=1}^{m} 1 = m$, and $\sum\limits_{k=1}^{n} 1 = n \equiv 0 \pmod{n}$; hence, $\langle 1 \rangle = (\mathbb{Z}/_{n\mathbb{Z}}, +)$. The only relation one would need to know to generate $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ is $n = 0$. Hence, the presentation of $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ is:

$$\langle 1 | n = 0 \rangle$$

1.2.16

We want to show that $D_4 = \langle r, s | r^2 = s^2 = (rs)^2 = 1 \rangle$. Recall that $D_4 = \langle r, s | r^2 = s^2 = 1, rs = sr^{-1} \rangle$; thus, it suffices to show that $(rs)^2 = 1 \Rightarrow rs = sr^{-1}$. Observe that:

$$(rs)^2 = 1 \iff rsrs = 1 \iff rs = s^{-1}r^{-1} = sr^{-1}$$

since $|s| = 2$. Hence, $D_4 = \langle r, s | r^2 = s^2 = (rs)^2 = 1 \rangle$.

1.2.17

(a) We are given the group presentation $X_{2n} = \langle x, y | x^n = y^2 = 1, xy = yx^2 \rangle$, and told that $n = 3k$ for some $k \in \mathbb{N}$. We want to show $|X_{2n}| = 6$. $n = 3k$ implies that $x, x^2 \in X_{2n}$ are distinct elements and $x, x^2 \neq 1$;

$y^2 = 1 \Rightarrow y = y^{-1}$. Therefore, observe that:

$$\begin{aligned}
xy &= yx^2 \\
\Rightarrow yxy &= x^2 \\
\Rightarrow (yxy)^2 &= (x^2)^2 \\
\iff yxyyxy &= x^4 \\
\iff yx^2y &= x^4 \\
\iff xyy &= x^4 \\
\iff x &= x^4 \\
\Rightarrow 1 &= x^3
\end{aligned}$$

Furthermore, note that

$$\begin{aligned}
xy &= yx^2 \\
\Rightarrow xyx^{-1} &= yx \\
\iff xyx^2 &= yx \\
\iff xxy &= yx \\
\iff x^2y &= yx
\end{aligned}$$

$\therefore X_{2n} = \{1, x, x^2, y, xy, x^2y\} \Rightarrow |X_{2n}| = 6$.

Now, letting $x = r$ and $y = s$, we have the relations $r^3 = s^2 = 1$ and $rs = sr^2 \iff rs = sr^{-1}$, which are the exact same relations in D_6.

(b) From part (a) we know that $x^n = x^3 = 1$, and we are told that $\gcd(3, n) = 1 \Rightarrow \exists x \in \mathbb{Z}$ s.t. $n = 3x + 1$ or $n = 3x + 2 = 3(x + 1) - 1 \Rightarrow n = 3k \pm 1$ for some $k \in \mathbb{Z}$. Therefore,

$$x^n = 1 \iff x^{3k\pm1} = 1 \iff (x^3)^k x^{\pm1} = 1 \iff x^{\pm1} = 1$$

$\Rightarrow x = 1$. Hence, $X_{2n} = \{1, y\} \Rightarrow |X_{2n}| = 2$.

1.2.18

Omitted.

1.3

1.3.1

$$\begin{aligned}
\sigma &= (1,3,5)(2,4) \\
\tau &= (1,5)(2,3) \\
\sigma^2 &= (1,3,5)(2,4)(1,3,5)(2,4) \\
&= (1,5,3) \\
\sigma\tau &= (1,3,5)(2,4)(1,5)(2,3) \\
&= (2,5,3,4) \\
\tau\sigma &= (1,5)(2,3)(1,3,5)(2,4) \\
&= (1,2,4,3) \\
\tau^2\sigma &= \tau(\tau\sigma) = (1,5)(2,3)\big((1,5)(2,3)(1,3,5)(2,4)\big) \\
&= (1,5)(2,3)(1,2,4,3) \\
&= (1,3,5)(2,4)
\end{aligned}$$

1.3.2

Omitted because it analogous to the previous exercise.

1.3.3

Recall that the order of a permutation in S_n is the least common multiple of its cycle lengths in its cycle decomposition. Therefore,

$$\begin{aligned} |\sigma| &= 6 & \qquad |\sigma\tau| &= 4 \\ |\tau| &= 2 & |\tau\sigma| &= 4 \\ |\sigma^2| &= 3 & |\tau^2\sigma| &= 6 \end{aligned}$$

1.3.4

(a) $S_3 = \{(1), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$. Thus,

$$\begin{aligned} |(1)| &= 1 & \qquad |(2,3)| &= 2 \\ |(1,2)| &= 2 & |(1,2,3) &= 3 \\ |(1,3)| &= 2 & |(1,3,2)| &= 3 \end{aligned}$$

(b) $S_4 = \{(1), (1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,3), (1,3,2), (1,2,4), (1,4,2), (2,3,4), (2,4,3), (1,2,3,4), (1,2,4,3), (1,3,2,4), (1,3,4,2), (1,4,2,3), (1,4,3,2)\}$. Thus,

$$\begin{aligned} |(1)| &= 1 & \qquad |(1,3)(2,4)| &= 2 & \qquad |(2,3,4)| &= 3 \\ |(1,2)| &= 2 & |(1,4)(2,3)| &= 2 & |(2,4,3)| &= 3 \\ |(1,3)| &= 2 & |(1,2,3)| &= 3 & |(1,2,3,4)| &= 4 \\ |(1,4)| &= 2 & |(1,3,2)| &= 3 & |(1,2,4,3)| &= 4 \\ |(2,3)| &= 2 & |(1,2,4)| &= 3 & |(1,3,2,4)| &= 4 \\ |(2,4)| &= 2 & |(1,4,2)| &= 3 & |(1,3,4,2)| &= 4 \\ |(3,4)| &= 2 & |(1,3,4)| &= 3 & |(1,4,2,3)| &= 4 \\ |(1,2)(3,4)| &= 2 & |(1,4,3) &= 3 & |(1,4,3,2)| &= 4 \end{aligned}$$

1.3.5

$|(1,12,8,10,4)(2,13)(5,11,7)(6,9)| = \text{lcm}(5,2,3) = \frac{5\cdot 2\cdot 3}{\text{gcd}(5,2,3)} = 30.$

1.3.6

The elements of order 4 in S_4 (in cycle decomposition) are: $(1,2,3,4), (1,2,4,3), (1,3,2,4), (1,3,4,2), (1,4,2,3), (1,4,3,2)$.

1.3.7

The elements of order 2 in S_4 (in cycle decomposition) are: $(1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$.

1.3.8

Let $\Omega = \{1,2,3,...\}$. Then S_Ω is the set of all bijections from $\mathbb{N}$ to $\mathbb{N}$. Let $\sigma \in S_\Omega$. Then σ maps 1 to m, where m may be any arbitrary natural number. Since there are infinitely many options for σ to map 1, there are infinitely permutations in $S_\Omega \Rightarrow S_\Omega$ is an infinite group.

1.3.9

Ommitted because it is tedious and a result from exercises 1.3.11 can be used to easily find such powers.

1.3.10

Given the $m-$cycle $\sigma = (a_1, a_2, ..., a_m)$, we want to show that for all $i \in \{1, 2, ..., m\}$, $\sigma^i(a_k) = a_{k+i \text{ mod m}}$, with $a_0 := a_m$ (i.e., $k + i$ is replaced with the smallest *positive* residue class mod m). We prove this by induction:
Base Case: $\sigma^1 = \sigma = (a_1, a_2, ..., a_m) \Rightarrow \sigma^1(a_k) = a_{k+1 \text{ mod m}}$, with $a_0 := a_m$.
Induction Hypothesis: Suppose that for some $i \in \{1, 2, ..., m-1\}$, $\sigma^i(a_k) = a_{k+i \text{ mod m}}$, with $a_0 := a_m$.
Induction Step: Observe that $\sigma^{i+1}(a_k) = \sigma^i\big(\sigma^1(a_k)\big) = \sigma^i(a_{k+1 \text{ mod m}}) = a_{k+1+i \text{ mod m}}$, with $a_0 := a_m$.

Therefore, $\sigma^i(a_k) = a_{k+i \text{ mod m}}$, with $a_0 := a_m$. Hence, for $1 \leq i \leq m-1$, $\sigma^i(a_1) = a_{1+i \text{ mod m}} = a_{1+i} \neq a_1 \Rightarrow |\sigma| > m-1$; yet, $\sigma^m(a_1) = a_{1+m \text{ mod m}} = a_1$, $\sigma^m(a_2) = a_{2+m \text{ mod m}} = a_2$,..., $\sigma^m(a_m) = a_{m+m \text{ mod m}} = a_0 = a_m \Rightarrow |\sigma| \leq m$. Thus, $|\sigma| = m$.

1.3.11

Let e be the identity permutation. Given that $\sigma = (1, 2, ..., m)$, we want to prove that σ^i is an $m-$cycle if and only if $\gcd(i, m) = 1$.

($\Rightarrow$) We prove by contrapositive; i.e., we show that if $\gcd(i, m) \neq 1$, then σ^i cannot be an $m-$cycle. Suppose $\gcd(i, m) = d > 1$. Then there exists $x, y \in \mathbb{N}$ such that $i = xd$ and $m = yd$; in particular, $x < i$ and $y < m$. Thus, observe that:

$$(\sigma^i)^y = (\sigma^{xd})^y = \sigma^{x(dy)} = (\sigma^m)^x = e^x = e$$

$\Rightarrow |\sigma^i| \leq y < m \Rightarrow \sigma^i$ cannot be an $m-$cycle (since in the previous exercise we showed that $m-$cycles have order m).

($\Leftarrow$) We want to show that if $\gcd(i, m) = 1$, then σ^i is an $m-$cycle. Note, from the previous exercises, $\sigma^i = (1 + i, 2 + i, ..., m + i)$. Now, suppose for the sake of contradiction that $\gcd(i, m) = 1$, but σ^i is not an $m-$cycle. Then this implies that there exists distinct $x, y \in \{1, 2, ..., m\}$ such that $x + i \equiv y + i$ (mod m). Then $m|(y - x) \Rightarrow\Leftarrow$ since $y - x < y \leq m$. Therefore, $\gcd(i, m) = 1$ implies that σ^i is an $m-$cycle.

1.3.12

(a) Given that $\tau = (1, 2)(3, 4)(5, 6)(7, 8)(9, 10)$, we want to determine whether or not there exists and $n-$cycle ($n \geq 10$) such that $\sigma^k = \tau$ for some $k \in \mathbb{Z}$. Let $\hat{\sigma} = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$. Then observe that

$$\begin{aligned}
\hat{\sigma}^2 &= (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)(1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \\
&= (1, 3, 5, 7, 9)(2, 4, 6, 8, 10) \\
\Rightarrow \hat{\sigma}^3 &= \hat{\sigma}^2(1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \\
&= (1, 4, 7, 10, 3, 6, 9, 2, 5, 8) \\
\Rightarrow \hat{\sigma}^4 &= \hat{\sigma}^3(1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \\
&= (1, 5, 9, 3, 7)(2, 6, 10, 4, 8) \\
\Rightarrow \hat{\sigma}^5 &= (1, 6)(2, 7)(3, 8)(4, 9)(5, 10)
\end{aligned}$$

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

$$\begin{aligned}\sigma^2 &= (1,3,5,7,9,2,4,6,8,10)(1,3,5,7,9,2,4,6,8,10)\\ &= (1,5,9,4,8)(2,6,10,3,7)\\ \Rightarrow \sigma^3 &= \sigma^2(1,3,5,7,9,2,4,6,8,10)\\ &= (1,7,4,10,5,2,8,3,9,6)\\ \Rightarrow \sigma^4 &= \sigma^3(1,3,5,7,9,2,4,6,8,10)\\ &= (1,9,8,5,4)(2,10,7,6,3)\\ \Rightarrow \sigma^5 &= (1,2)(3,4)(5,6)(7,8)(9,10)\end{aligned}$$

(b) Since this is similar to part (a) $-$which wasted way too much of my time$-$ this part is ommitted.

1.3.13

Let e be the identity permutation. We want to prove that $\sigma \in S_n$ has order 2 if and only if σ is the product of disjoint $2-$cycles.

($\Leftarrow$) First we prove the converse; that is, suppose that σ is the product of disjoint $2-$cycles. Then since disjoint cycles commute, we can write σ^2 as the product of squared $2-$cycles. Since the order of any $2-$cycle is 2, this implies that $\sigma^2 = e \Rightarrow |\sigma| \leq 2$; since only the identity permutation has order < 2, this implies that $|\sigma| = 2$

($\Rightarrow$) Now, proving the forward direction, suppose $|\sigma| = 2$. Assume for the sake of contradiction that the cycle decomposition of σ contains a $k-$cycle, for some $k \in \{3, ..., n\}$. Then since disjoint cycles commute, σ^2 may be expressed as the product of the square of the disjoint cycles in the cycle decomposition of σ; i.e., if

$$\sigma = (a_1, a_2)(a_3, a_4) \cdot ... \cdot (a_m, a_{m+1}, ..., a_{m+(k-1)})$$

then

$$\sigma^2 = (a_1, a_2)^2(a_3, a_4)^2 \cdot ... \cdot (a_m, a_{m+1}, ..., a_{m+(k-1)})^2$$

The squared $2-$cycles will equal the identity permutation, but the squared $k-$cycle will equal some non-identity permutation since $k-$cycles have order k. This, however, contradicts the fact that $|\sigma| = 2$. Therefore, the cycle decompostion of σ must consist of only disjoint $2-$cycles.

1.3.14

In this problem, we are asked to prove that for a prime number p, $\sigma \in S_n$ has order p if and only if σ is the product of disjoint $p-$cycles. Suppose σ has the cycle decomposition: $\sigma = c_1, c_2, ..., c_m$, where c_i are disjoint cycles for $i = 1, 2, ..., m$.

($\Leftarrow$) Suppose that each of the cycles in the cycle decomposition of σ are $p-$cycles. Then

$$\sigma^p = (c_1, c_2, ..., c_m)^p = c_1^p c_2^p \cdot ... \cdot c_m^p = e$$

since disjoint cycles commute. Therefore, $|\sigma| \leq p$; moreover, $|\sigma| \geq p$, since for any positive integer a such that $a < p$, $c_i^a \neq e$ for $i = 1, 2, ..., m$ (since $p-$cycles have order p). Thus, $|\sigma| = p$.

($\Rightarrow$) Now suppose $|\sigma| = p$. Assume for the sake of contradiction the cycle decomposition of σ contains a $k-$cycle, where $k \neq p$; without loss of generality, suppose c_1 is the $k-$cycle. Then, either

- $|c_1| = k > p$, in which case $c_1^p \neq e$; or,
- $|c_1| = k < p$, in which case p prime implies that $k \not| \, p \Rightarrow p = kq + r$ where $q, r \in \mathbb{Z}$ and $1 \leq r < k \Rightarrow c_1^p = c_1^{kq+r} = (c_1^k)^q c_1^r = c_1^r \neq e$

In either case, $\sigma^p \neq e \Rightarrow |\sigma| \neq p$. Thus, $|\sigma| = p$ implies that the cycle decomposition of σ consists only of the product of disjoint $p-$cycles.

Note: If, however, p is not prime, then the forward direction of the above result does not necessarily hold. That is, if m is a non-prime integer, then $|\sigma| = m$ does not imply that the cycle decomposition of σ is the product of disjoint $m-$cycles. For example, let $\sigma = (1,2)(3,4,5) \in S_5$. Then, $|\sigma| = 6$, but the cycle decomposition of σ is not a product of disjoint $6-$cycles (it is in fact as we expressed it above).

1.3.15

Suppose $\sigma \in S_n$ has the cycle decomposition: $\sigma = c_1 c_2 \cdot ... \cdot c_m$, where c_i are disjoint cycles for $i = 1, 2, ..., m$. Suppose also that $|c_1| = n_1$, $|c_2| = n_2$,...,$|c_m| = n_m$. Let $k := \text{lcm}(n_1, n_2, ...n_m)$. Then,

$$\begin{aligned}
\sigma^k &= (c_1 c_2 \cdot ... \cdot c_m)^k \\
&= c_1^k c_2^k \cdot ... \cdot c_m^k \qquad \text{(since disjoint cycles commute)} \\
&= (c_1^{n_1})^{k_1} (c_2^{n_2})^{k_2} \cdot ... \cdot (c_m^{n_m})^{k_m} \qquad \left(\text{where } k_i = \frac{k}{n_i} \text{ for } i = 1, 2, ..., m\right) \\
&= e^{k_1} e^{k_2} \cdot ... \cdot e_m^{k_m} \\
&= e
\end{aligned}$$

$\Rightarrow |\sigma| \leq k$.

Now, assume for the sake of contradiction that $|\sigma| = k' < k$. Then, $\sigma^{k'} = c_1^{k'} c_2^{k'} \cdot ... \cdot c_m^{k'}$, and since $k' < k$, k' is not a multiple of each of the n_i $(1 \leq i \leq m)$, which implies that there exists $j \in \{1, 2, ..., m\}$ such that $k' = n_j q + r$ where $q, r \in \mathbb{Z}$ and $1 \leq r < n_j \Rightarrow c_j^{k'} = (c_j^{n_j})^q c_j^r = c_j^r \neq e \Rightarrow \Leftarrow$. Thus, $|\sigma| \geq k \Rightarrow |\sigma| = k$.

1.3.16

Let $\sigma \in S_n$ be an $m-$cycle, where $m \leq n$. Then

$$\begin{aligned}
\sigma(1) &= k_1, \text{ for } k_1 \in \{1, 2, ..., n\}, \\
\sigma(2) &= k_2, \text{ for } k_2 \in \{1, 2, ..., n\} \setminus \{k_1\}, \\
&\vdots \\
\sigma(m) &= k_2, \text{ for } k_2 \in \{1, 2, ..., n\} \setminus \{k_1, k_2, ..., k_{m-1}\}
\end{aligned}$$

Therefore, there are n possible elements $\sigma(1)$ may be, $n-1$ possible elements $\sigma(2)$ may be,..., and $n-(m-1) = n-m+1$ possible elements $\sigma(m)$ may be. Note, however, that cycles cyclically permute their own elements, hence there are m equivalent ways to represent the same $m-$cycle. Thus, the total number of distinct permutations σ may be is:

$$\frac{n(n-1) \cdot ... \cdot (n-m+1)}{m} = \frac{n^{\underline{m}}}{m}$$

1.3.17

Let $\sigma \in S_n$, where $n \geq 4$, be a product of two disjoint $2-$cycles.

$$\begin{aligned}
\sigma(1) &= k_1, \text{ for } k_1 \in \{1, 2, ..., n\}, \\
\sigma(2) &= k_2, \text{ for } k_2 \in \{1, 2, ..., n\} \setminus \{k_1\}, \\
\sigma(3) &= k_3, \text{ for } k_2 \in \{1, 2, ..., n\} \setminus \{k_1, k_1\}, \\
\sigma(4) &= k_2, \text{ for } k_2 \in \{1, 2, ..., n\} \setminus \{k_1, k_2, k_3\},
\end{aligned}$$

Therefore, there are n possible elements $\sigma(1)$ may be, $n-1$ possible elements $\sigma(2)$ may be, $n-2$ possible elements $\sigma(3)$ may be, and $n-3$ possible elements $\sigma(4)$ may be. Note, however, that cycles cyclically permute their own elements, hence there are 2 equivalent ways to represent the same first cycle and 2 equivalent ways to represent the same second cycle; morover, disjoint cycles commute, which implies that there are 2 equivalent ways to write σ as the product of the same disjoint $2-$cycles. Thus, the total number of distinct permutations σ may be is:

$$\frac{n(n-1)(n-2)(n-3)}{2 \cdot 2 \cdot 2} = \frac{n^{\underline{4}}}{8}$$

1.3.18

Non-identity permutations in S_5, expressed as their cycle decomposition, may be $2, 3, 4,$ or $5-$cycles, the product of two $2-$cycles, or the product of a 2 and $3-$cycle. Therefore, elements in S_5 may have orders: $1, 2, 3, 4, 5,$ or 6.

1.3.19

Non-identity permutations in S_7, expressed as their cycle decomposition, may be $2, 3, 4, 5, 6,$ or $7-$cycles, the product of two or three $2-$cycles, the product of two $3-$cycles, the product of a $2-$cycle and a $4-$cycle, the product of a $3-$cycle and a $4-$cycle, or the product of a $2-$cycle and $5-$cycle. Therefore, elements in S_7 may have orders: $1, 2, 3, 4, 5, 6, 7, 10,$ or 12.

1.3.20

Omitted.

1.4

1.4.1

Recall that $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$. Since $|\mathbb{F}_2| = 2$, this implies that $|GL_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = (3)(2) = 6$.

1.4.2

Observe that the following set of 2×2 matrices with entries in $\mathbb{F}_2$ (where the overline has been ommitted for convenience) have non-zero determinants:

$$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

Therefore, $S \subseteq GL_2(\mathbb{F}_2)$; since $|GL_2(\mathbb{F}_2)| = 6 = |S| \Rightarrow GL_2(\mathbb{F}_2) = S$.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of $GL_2(\mathbb{F}_2)$, so it has order 1. As for the others, we have:

$$\left|\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right| = 2$$
$$\left|\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right| = 2$$
$$\left|\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right| = 2$$
$$\left|\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right| = 3$$
$$\left|\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right| = 3$$

1.4.3

Observe that for elements $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in $GL_2(\mathbb{F}_2)$, we have

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

but,

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

Thus, $AB \neq BA \Rightarrow GL_2(\mathbb{F}_2)$ is not an abelian group.

1.4.4

Let $n \in \mathbb{N}$ be composite, and assume for the sake of contradiction that $\mathbb{Z}/_{n\mathbb{Z}}$ is a field. Then since n is composite, this implies that there exists integers $a, b > 1$ such that $n = ab$. Necessarily, $a, b < n$, and

$$\begin{aligned} ab &\equiv 0 \text{ (mod n)} \\ \Rightarrow a^{-1}ab &\equiv a^{-1}0 \text{ (mod n)} \\ \iff b &\equiv 0 \text{ (mod n)} \end{aligned}$$

$\Rightarrow\Leftarrow$ since $1 < b < n$.

1.4.5

We want to show that $GL_n(F)$ is a finite group if and only if F is a finite field.

($\Leftarrow$) Suppose F is finite. Then there exists $m \in \mathbb{N}$ such that $|F| = m$. Thus, there are m^{n^2} many $n \times n$ matrices whose entries are in $F \Rightarrow |GL_n(F)| \leq m^{n^2} < \infty$; i.e., $GL_n(F)$ is a finite group.

($\Rightarrow$) We prove the contrapositive. That is, suppose F is an infinite field; then we want to show that $GL_n(F)$ is an infinite group. Let I_n be the $n \times n$ identity matrix and let $a \in F \setminus \{0\}$. Then aI_n is a diagonal matrix $\Rightarrow \det(aI_n) = a^n \neq 0$, since $a \neq 0$ and fields do not have zero divisors. Thus, aI_n is invertible $\Rightarrow aI_n \in GL_n(F)$. Since there are infinitely many such a to choose from, it follows that $GL_n(F)$ is an infinite group.

1.4.6

If $|F| = q < \infty$, and if $M_n(F)$ denotes the set of all $n \times n$ matrices whose entries are elements of F, then I claim that $|M_n(F)| = q^{n^2}$. To see this, note that if A is a matrix in $M_n(F)$, then each of the n^2 many elements in A may be any of the q elements in F. Thus, there are q^{n^2}−many of such matrices $A \in M_n(F)$. Hence, $|GL_n(F)| < |M_n(F)| = q^{n^2}$.

Note: The inequality in the last sentence is strict since $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_n(F)$ is not invertible.

1.4.7

Let $M_2(\mathbb{F}_p)$ denote the set of all 2×2 matrices whose entries are elements of $\mathbb{F}_p$. We recall two facts from matrix theory:

1. $A \in M_2(\mathbb{F}_p)$ is not invertible $\iff$ a row in A is a multiple of the other row in A, and
2. $A \in M_2(\mathbb{F}_p)$ is not invertible $\iff$ A contains a column whose entries are both 0.

Since $|\mathbb{F}_p| = p$ and each of the four entries of a matrix in $M_2(\mathbb{F}_p)$ may be any element of $\mathbb{F}_p$, it follows that $|M_2(\mathbb{F}_p)| = p^4$. Now, we want to subtract from $M_2(\mathbb{F}_p)$ all non-invertible matrices. There are p^2 possibly many rows a matrix in $M_2(\mathbb{F}_p)$ may have. Given a row A_1 in a matrix $A \in M_2(\mathbb{F}_p)$, there are p many multiples of $A_1 \Rightarrow$ there are atleast $p^2 \cdot p = p^3$ many non-invertible matrices in $M_2(\mathbb{F}_p)$. Now, if $A \in M_2(\mathbb{F}_p)$ is a matrix with a column whose entries are both 0, then A is not invertible; since the other 2 entries in A may be any element in $\mathbb{F}_p$, there are p^2 many such matrices. However, if a matrix $A \in M_2(\mathbb{F}_p)$ contains a column whose entries are both 0, and (atleast) one of the other elements in its other column are 0, then its rows are scalar multiples and were already counted in the first p^2 subtracted matrices; in this case, since there are p possible many entries for the other element, we must add back p many matrices to avoid double counting. Thus, there are $p^4 - p^3 - p^2 + p$ invertible matrices in $M_2(\mathbb{F}_p)$; i.e., $|GL_n(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p$.

1.4.8

As before in exercise 1.4.3., let $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then $AB = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $BA = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, hence, $AB \neq BA$.

Now, let $X, Y \in GL_n(F)$, where we define $X := \begin{pmatrix} A & 0_{n-2\times n-2} \\ 0_{n-2\times n-2} & I_2 \end{pmatrix}$ and $Y := \begin{pmatrix} B & 0_{n-2\times n-2} \\ 0_{n-2\times n-2} & I_2 \end{pmatrix}$. Then

$$XY = \begin{pmatrix} AB & 0_{n-2\times n-2} \\ 0_{n-2\times n-2} & I_2 \end{pmatrix} \neq \begin{pmatrix} BA & 0_{n-2\times n-2} \\ 0_{n-2\times n-2} & I_2 \end{pmatrix} = YX$$

Hence, for any integer $n \geq 2$, $GL_n(F)$ is non-abelian.

1.4.9

This problem is ommitted because it only requires a straightforward (but tedious) computation; nonetheless, we will accept and use the result in future problems.

1.4.10

We are told that $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}$.

(a) Observe that

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

Since $a_1, c_1, a_2, c_2 \neq 0$, this implies that a_1a_2 and c_1c_2 are nonzero, hence $\begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix} \in G$. That is, G is closed under matrix multiplication.

(b) Recall from linear algebra, that given a 2×2 matrix of the form

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

A is invertible if and only if $\det(A) = ad - bc \neq 0$, and if A is invertible, then

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

If a matrix $B \in G$, then B is of the form

$$B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

for some real numbers a, b, c with $a, c \neq 0$. Therefore, $\det(B) = ac - b \cdot 0 = ac \neq 0 \Rightarrow B$ is invertible, and

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

Since $a, c \neq 0$, this implies that $\frac{1}{a}$ and $\frac{1}{c}$ are nonzero, hence $B^{-1} \in G$. That is, G is closed under inverses.

(c) From the previous sub-problem, we have shown that every element in G is invertible, hence, $G \subset GL_2(\mathbb{R})$. Moreover, we have shown that G is closed under matrix multiplication and closed under inverses. Therefore, G is a subgroup of $GL_2(\mathbb{R})$.

(d) It suffices to show that the set $S = \left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R} \text{ and } a \neq 0\right\}$ is closed under matrix multiplication and closed under inverses. Observe that for real numbers a_1, a_2, b, with $a_1, a_2 \neq 0$, we have:

$$\begin{pmatrix} a_1 & b \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b + ba_2 \\ 0 & a_1a_2 \end{pmatrix}$$

Thus, S is closed under matrix multiplication. Also, if $A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ is a matrix in S, then $\det(A) = a^2 \neq 0 \Rightarrow A$ is invertible; moreover,

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

$a \neq 0 \Rightarrow \frac{1}{a} \neq 0 \Rightarrow S$ is closed under invereses. Thus, S is also a subgroup of $GL_2(\mathbb{R})$.

1.4.11

The Heisenburg group over the field F is defined as

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

(a)

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

and

$$YX = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & b+dc+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} \in H(F)$$

Hence, $H(F)$ is closed under matrix multiplication. Letting $a = f = 1$ and $b = c = d = e = 0$, we have:

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

and

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

Therefore, in general, $XY \neq YX$, hence $H(F)$ is not commutative.

(b) Let $A \in H(F)$. Note that since A is a triangular matrix with nonzero entries in its diagonal, its determinant is nonzero and is thus invertible. Now, consider the augmented matrix

$$[A|I_3] = \left(\begin{array}{ccc|ccc} 1 & a & b & 1 & 0 & 0 \\ 0 & 1 & c & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Using elementary row operations, we reduce the left-side of the augmented matrix to the identity matrix I_3, and obtain the inverse of A:

$$[I_3|A^{-1}] = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -a & -b+ac \\ 0 & 1 & 0 & 0 & 1 & -c \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Therefore, $A^{-1} \in H(F)$.

(c) It requires only a straightforward (but tedious) computation to verify the associative law for $H(F)$, so I will not bother.

Now, given that $H(F)$ is closed under multiplication, closed under inverses, contains an identity element (the matrix I_3), and satisfies associativity, we conclude $H(F)$ is a group. Moreover, it follows from the product rule that the order of $H(F)$ is $|F|^3$ since each matrix in $H(F)$ is uniquely determined by its three entries above the diagonal, each of which may be any element in F.

(d) This is straightforward but tedious, so for the sake of time is ommitted.

(e) If $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in H(\mathbb{R})$, then it is easily shown by induction that for any $n \in \mathbb{N}$, $A^n = \begin{pmatrix} 1 & na & \star \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$, where $\star \in \mathbb{R}$. Therefore, if a or c is nonzero, then $A^n \neq 0_{3\times 3}$. If, on the other hand, $a = c = 0$, then $A^n = \begin{pmatrix} 1 & 0 & nb \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq 0_{3\times 3}$. Hence, every non-identity matrix in $H(\mathbb{R})$ has infinite order.

1.5

1.5.1

The order of the elements in Q_8 are:

$$\begin{aligned} |1| &= 1 & |k| &= 4 \\ |-1| &= 2 & |-i| &= 4 \\ |i| &= 4 & |-j| &= 4 \\ |j| &= 4 & |-k| &= 4 \end{aligned}$$

1.5.2

Below are the Cayley tables for S_3, D_8, and Q_8:

S_3	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(132)	(123)	(23)	(13)
(13)	(13)	(123)	e	(132)	(12)	(23)
(23)	(23)	(132)	(123)	e	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	e
(132)	(132)	(23)	(12)	(13)	e	(123)

D_8	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	a	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	1	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

Q_8	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	j	k	$-i$	$-j$	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	1	-1
$-k$	$-k$	k	$-j$	j	i	$-i$	-1	1

1.5.3

Note that $i^2 = j^2 = k^2 = -1 \Rightarrow i(-i) = j(-j) = k(-k) = 1 \Rightarrow i^{-1} = -i$, $j^{-1} = -j$, and $k^{-1} = -k$ Therefore, all equations satisfied by elements of Q_8 follow from the relations below:

$$(-1)^2 = 1,\ i^2 = j^2 = k^2 = -1, \text{ and } ijk = -1 \qquad (\star)$$

Now, since $i^2 = -1$ and $ij = k$, it follows that i and j generate Q_8. So, to find a presentation of Q_8 with generators i and j, we need to find the relations that i and j satisfy so that the equations in $(\star)$ follow. We do this by starting with the equations in $(\star)$, and reformulating them so that they involve only i, j, and their inverses.

Observe that multiplying both sides of the third equation by k yields $ijk^2 = -k \Rightarrow ij = k$. Therefore, the second relation is equivalent to $i^2 = j^2 = (ij)^2 = -1$. Thus we have:

$$(-1)^2 = 1,\ i^2 = j^2 = (ij)^2 = -1, \text{ and } ij(ij) = -1$$

The third equation is reduntant, so we thus have:

$$(-1)^2 = 1 \text{ and } i^2 = j^2 = (ij)^2 = -1$$

Now, to get rid of -1 in the above equations, we define $i^2 := -1$. Thus, the above relations reduce to:

$$i^4 = 1 \text{ and } i^2 = j^2 = (ij)^2$$

Lastly, we can rewrite $j^2 = (ij)^2$ as $ij = ji^{-1}$, which let's us know how we can commute elements in a product of elements in Q_8. Therefore, we have the following presentation:

$$Q_8 = \langle i, j | i^4 = 1, i^2 = j^2, ij = ji^{-1} \rangle$$

1.6

1.6.1

Let $(G, \star)$ and $(H, \diamond)$ be groups, $\phi : G \to H$ be a homomorphism, and $x \in G$.

(a) We use induction to prove that given any $x \in G$, $\phi(x^n) = [\phi(x)]^n \ \forall n \in \mathbb{N}$.
Base Case: Trivially $\phi(x^1) = \phi(x) = [\phi(x)]^1 \Rightarrow \phi(x^1) = [\phi(x)]^1$.
Induction Hypothesis: Suppose that for any $k \in \mathbb{N}$ that $\phi(x^k) = [\phi(x)]^k$.
Induction Step: Observe that $\phi(x^{k+1}) = \phi(x \star x^k) = \phi(x) \diamond \phi(x^k) = \phi(x) \diamond [\phi(x)]^k = [\phi(x)]^{k+1}$. Therefore, for any $x \in G$, $\phi(x^n) = [\phi(x)]^n \ \forall n \in \mathbb{N}$.

(b) Note that if 1 is the identity element in G and if x is any element in G, then $\phi(x) = \phi(1 \star x) = \phi(1) \diamond \phi(x) \Rightarrow \phi(1)$ is the identity element of H. Now we want to show that for any $x \in G$, $\phi(x^n) = [\phi(x)]^n \ \forall n \in \mathbb{Z}$; we proceed by using induction.
Base Cases: Trivially $\phi(x^0) = \phi(1) = [\phi(x)]^0 \Rightarrow \phi(x^0) = [\phi(x)]^0$. Also, observe that $\phi(1) = \phi(x \star x^{-1}) = \phi(x) \diamond \phi(x^{-1}) \Rightarrow \phi(x^{-1}) = [\phi(x)]^{-1}$.
Induction Step: Suppose that for any $k \in \mathbb{N}$, that $\phi(x^{-k}) = [\phi(x)]^{-k}$.
Induction Step: Observe that $\phi(x^{-k-1}) = \phi(x^{-k} \star x^{-1}) = \phi(x^{-k}) \diamond \phi(x^{-1}) = [\phi(x)]^{-k} \diamond [\phi(x)]^{-1} = [\phi(x)]^{k-1}$. Therefore, we conclude that for any $x \in G$, $\phi(x^n) = [\phi(x)]^n \ \forall n \in \mathbb{Z}$.

1.6.2

We are told that $\phi : G \to H$ is a homomorphism and we want to show that $|x| = |\phi(x)|$ for all $x \in G$. Before we prove this, recall that from the previous exercises we showed that $\phi(1)$ is the identity element of H.

Suppose that $|x| = n$. Then $x^n = 1 \Rightarrow \phi(1) = \phi(x^n) = [\phi(x)]^n \Rightarrow |\phi(x)| \leq n$.

Alternatively, suppose $|\phi(x)| = m$. Then $[\phi(x)]^m = \phi(1) \Rightarrow \phi(1) = [\phi(x)]^m = \prod_{i=1}^{m} \phi(x) = \phi(x^m) \Rightarrow x^m = 1 \Rightarrow |x| \leq |\phi(x)|$.

Therefore, $|x| = |\phi(x)|$.

1.6.3

Let $\phi : G \to H$ be an isomorphism. Then for any element $h \in H$, there exists $x \in G$ such that $\phi(x) = h$; therefore, we can express elements in H in terms images, under ϕ, of elements in G.

Now, G is abelian $\iff$ $xy = yx$ for all $x, y \in G$. Hence,

$$\phi(x)\phi(y) = \phi(xy) = \phi(yx) = \phi(y)\phi(x)$$

$\Rightarrow H$ is abelian.

Similarly, H abelian $\iff$ $\phi(x)\phi(y) = \phi(y)\phi(x)$ for all $\phi(x), \phi(y) \in H$. Hence,

$$\phi(xy) = \phi(x)\phi(y) = \phi(y)\phi(x) = \phi(yx)$$

$\Rightarrow G$ is abelian.

1.6.4

Assume for the sake of contradiction that $(\mathbb{R} \setminus \{0\}, \times)$ is isomorphic to $(\mathbb{C} \setminus \{0\}, \times)$. Then since $i \in \mathbb{C} \setminus \{0\}$ has order 4, there must exist some number $x \in \mathbb{R} \setminus \{0\}$ of order 4. Assuming such an $x \in \mathbb{R} \setminus \{0\}$ exists, then $x^4 = 1 \iff x^4 - 1 = 0$. Observe that

$$x^4 - 1 = (x^2 + 1)(x^2 - 1) = (x - i)(x + i)(x - 1)(x + 1)$$

$\Rightarrow x = i, -i, 1$, or -1. Now, i and $-i$ are not in $\mathbb{R} \setminus \{0\}$, which implies $x = 1$ or $x = -1$. However, 1 and -1 both have order less than 4, which implies that $x \neq 1$ and $x \neq -1$. Consequently, there is no element of order 4 in $(\mathbb{R} \setminus \{0\}, \times)$, so we conclude that $(\mathbb{R} \setminus \{0\}, \times)$ is not isomorphic to $(\mathbb{C} \setminus \{0\}, \times)$.

1.6.5

Recall that $\mathbb{Q}$ is countably infinite, whereas $\mathbb{R}$ is uncountably infinite. Therefore, there does not exists a bijection between $\mathbb{Q}$ and $\mathbb{R}$, which implies that $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{R}, +)$.

1.6.6

Assume for the sake of contradiction that there exists an isomorphism $\phi : (\mathbb{Z}, +) \to (\mathbb{Q}, +)$. Then note that 1 generates $\mathbb{Z}$; that is, $\forall n \in \mathbb{Z}$, $n = \pm \sum_{i=1}^{n} 1$. Therefore, for every $a \in \mathbb{Q}$, there exists $m \in \mathbb{Z}$ such that $a = \phi\left(\pm \sum_{i=1}^{m} 1\right) = \pm \sum_{i=1}^{m} \phi(1) \Rightarrow \mathbb{Q}$ is generated by $\phi(1)$. Hence, $\mathbb{Q} = \langle \phi(1) \rangle = \{n\phi(1) : n \in \mathbb{Z}\}$. This implies that $\frac{1}{2} \cdot \phi(1) = \frac{\phi(1)}{2} \notin \mathbb{Q} \Rightarrow\Leftarrow$ since non-zero rational numbers are closed under multiplication.

1.6.7

In Q_8 there is only one element that has order 2; namely, -1. However, in D_8, there are four elements which have order 2; namely, s, sr, sr^2, and sr^3. Therefore, there cannot be an isomorphism between Q_8 and D_8.

1.6.8

If $n, m \in \mathbb{N}$ such that $n \neq m$, then $n! \neq m! \Rightarrow |S_n| = n! \neq m! = |S_m| \Rightarrow S_n$ and S_m are not isomorphic.

1.6.9

$r \in D_{24}$ has order 12, but every non-dentity element in S_4 is of the form (ab), (abc), $(abcd)$, or $(ab)(cd)$, for some distinct integers $a, b, c, d \in \{1, 2, 3, 4\}$; these elements in S_4 have orders $2, 3, 4$, and 2, respectively. Therefore, no element in S_4 has order 12, which implies that D_{24} and S_4 are not isomorphic.

1.6.10

(a) Given that σ is a permutation on Δ, we want to show that $\phi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$ is a permuation in on Ω. Since $\theta : \Delta \to \Omega$ is a bijection, there is an inverse $\theta^{-1} : \Omega \to \Delta$, which is also a bijection; moreover, σ is a permutation on Δ means that $\sigma : \Delta \to \Delta$ is a bijection. Therefore, $\theta \circ \sigma \circ \theta^{-1}$ is a composition of bijective functions, and thus a bijection; moreover, maps elements from Ω to Ω since:

$$\Omega \xrightarrow{\theta^{-1}} \Delta \xrightarrow{\sigma} \Delta \xrightarrow{\theta} \Omega$$

Thus, $\phi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$ is a permutation on Ω.

(b) Define the function $\chi : S_\Omega \to S_\Delta$ as $\chi(\tau) = \theta^{-1} \circ \tau \circ \theta$, where θ is the bijection given in part (a). Then χ is well defined because if τ is a permutation on Ω, then $\chi(\tau)$ is a composition of bijections $-$ and thus a bijection$-$ and

$$\Delta \xrightarrow{\theta} \Omega \xrightarrow{\tau} \Omega \xrightarrow{\theta^{-1}} \Delta$$

$\Rightarrow \chi(\tau)$ is a permuation on Δ.

Now, if $\sigma \in S_\Delta$, observe that

$$\chi(\phi(\sigma)) = \chi(\theta \circ \sigma\theta^{-1}) = \theta^{-1}(\theta \circ \sigma \circ \theta^{-1}) \circ \theta = \theta^{-1} \circ \theta \circ \sigma \circ \theta^{-1} \circ \theta = \sigma$$

$\Rightarrow \chi \circ \phi = id_{S_\Delta}$, hence χ is a left inverse for ϕ. Moreover, if $\tau \in S_\Omega$, observe that

$$\phi(\chi(\tau)) = \phi(\theta^{-1} \circ \tau \circ \theta) = \theta(\theta^{-1} \circ \tau \circ \theta) \circ \theta^{-1} = \tau$$

$\Rightarrow \phi \circ \chi = id_{S_\Omega}$, hence χ is a right inverse for ϕ. Therefore, χ is the inverse for ϕ, which implies that ϕ is a biejction from S_Δ to S_Ω.

(c) Let e be the identity element of S_Δ, and let $\sigma, \tau \in S_\Delta$. Then, observe that

$$\begin{aligned}\phi(\sigma \circ \tau) &= \theta \circ (\sigma \circ \tau) \circ \theta^{-1}\\ &= \theta \circ \sigma \circ e \circ \tau \circ \theta^{-1}\\ &= \theta \circ \sigma \circ (\theta^{-1} \circ \theta) \circ \tau \circ \theta^{-1}\\ &= (\theta \circ \sigma \circ \theta^{-1}) \circ (\theta \circ \tau \circ \theta^{-1})\\ &= \phi(\sigma) \circ \phi(\tau)\end{aligned}$$

$\Rightarrow \phi$ is a homomorphism.

Therefore, we conclude that if $|\Delta| = |\Omega|$, then $S_\Delta \cong S_\Omega$.

1.6.11

Let $(A, \star)$ and $(B, \diamond)$ be groups. Then recall that $A \times B = \{(a, b) : a \in A,\ b \in B$ forms a group with the binary operation $\cdot : (A \times B) \times (A \times B) \to A \times B$ defined as $(a_1, b_1) \cdot (a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$, and similarly $B \times A\{(b, a) : b \in B,\ a \in A$ forms a group with the binary operation $\cdot : (B \times A) \times (B \times A) \to B \times A$ defined as $(b_1, a_1) \cdot (b_2, a_2) = (b_1 \diamond b_2, a_1 \star a_2)$. We want to show that $A \times B \cong B \times A$.

Define $\phi : (A \times B) \to (B \times A)$ as $\phi(a, b) = (b, a)$. Then ϕ is bijection: note that $\phi(a_1, b_1) = \phi(a_2, b_2) \Rightarrow (b_1, a_1) = (b_2, a_2)$, hence ϕ is one-to-one; moreover, if $(b, a) \in B \times A$, then $(a, b) \in A \times B$ and $\phi(a, b) = (b, a) \Rightarrow \phi$ is onto. Lastly, observe that

$$\phi[(a_1, b_1) \cdot (a_2, b_2) = \phi[(a_1 \star a_2, b_1 \diamond b_2)] = (b_1 \diamond b_2, a_1 \star a_2)$$

and

$$\phi(a_1, b_1) \cdot \phi(a_2, b_2) = (b_1, a_a) \cdot (b_2, a_2) = (b_1 \diamond b_2, a_1 \star a_2)$$

$\therefore \phi[(a_1, b_1) \cdot (a_2, b_2)] = \phi(a_1, b_1) \cdot \phi(a_2, b_2) \Rightarrow A \times B \cong B \times A$.

1.6.12

We are told that A, B, and C are groups, $G := A \times B$, and $H := B \times A$; we want to show that $G \cong H$. First, we need the following lemma:

Lemma 2. *The finite direct product of groups is a group.*

Proof. We use induction.
Base Case: Earlier in exercise 1.1.28, we showed that if A_1 and A_2 are groups, then $A_1 \times A_2$ is a group.
Induction Step: Suppose that for any positive integer $n \geq 2$, $\prod_{i=1}^{n} A_i$ is a group.
Inudction Step: Observe that $\prod_{i=1}^{n+1} = \left(\prod_{i=1}^{n} A_i \right) \times A_{n+1}$, which by the induction hypothesis is a product to two groups, hence by the base case is a group. $\square$

Since the finite direct product of groups is a group, associativity holds for any finite direct product of groups. Therefore, we have:

$$G \times C = (A \times B) \times C = A \times (B \times C) = A \times H$$

$\Rightarrow G \times C = A \times H$; every group is isomorphic to itself (such an isomorphism is called and automorphism), hence $G \times C \cong A \times H$.

1.6.13

We are told that $(G, \star)$ and $(H, \diamond)$ are groups and that $\phi : G \to H$ is a homomorphism. We want to show that $\phi(G) = \{h \in H : h = \phi(g) \text{ for some } g \in G\}$ is also a group under $\diamond$. Since $\phi(G) \subseteq H$, $\phi(G)$ inherits associativity under $\diamond$. Also, since ϕ is a homomorphism, it maps the identity in G, e_G, to the identity in H, e_H; that is, $\phi(e_G) = e_H \Rightarrow e_H \in H$. Thus, it suffices to show that $\phi(G)$ is closed under $\diamond$ and under inverses.

Let $h_1, h_2 \in \phi(G)$. Then there exists $g_1, g_2 \in G$ such that $h_1 = \phi(g_1)$, $h_2 = \phi(g_2)$. Therefore, $h_1 \diamond h_2 = \phi(g_1) \diamond \phi(g_2) = \phi(g_1 \star g_2) \in \phi(G)$, hence $\phi(G)$ is closed under $\diamond$. Furthermore, if $h \in \phi(G)$, then there exists $g \in G$ such that $h = \phi(G)$, which implies that $h^{-1} = [\phi(g)]^{-1} \overset{1.6.1}{=} \phi(g^{-1}) \in \phi(G)$; consequently, $\phi(G)$ is closed under inverses. We thus conclude that $\phi(G)$ is a group.

Now, suppose ϕ is injective, or one-to-one. Then, $\phi|_G$ is a bijection between the two groups G and $\phi(G)$. Moreover, $\phi|_G$ is a homomorphism (since ϕ is a homomorphism), hence $G \cong \phi(G)$.

1.6.14

Let $(G, \star)$ and $(H, \diamond)$ be groups with identities e_G and e_H respectively. We first want to show that if $\phi : G \to H$ is a homomorphism, then $\ker(\phi) := \{g \in G : \phi(g) = e_H\}$ is a subgroup of H. Since $\ker(\phi) \subseteq G$, $\ker(\phi)$ inherits associativity. Also, since ϕ is a homomorphism, $\phi(e_G) = e_H \Rightarrow e_G \in \ker(\phi)$. Therefore, it suffices to show that $\ker(\phi)$ is clused under $\diamond$ and under inverses.

Let $g_1, g_2 \in \ker(\phi)$. Then

$$\phi(g_1 \star g_2) = \phi(g_1) \diamond \phi(g_2) = e_H \diamond e_H = e_H$$

$\Rightarrow g_1 \star g_2 \in \ker(\phi)$. Now, if $g \in \ker(\phi)$, then

$$\phi(g^{-1}) = [\phi(g)]^{-1} = e_H^{-1} = e_H$$

$\Rightarrow g^{-1} \in \ker(\phi)$. Hence, $\ker(\phi)$ is a subgroup of G.

Next we want to show that ϕ injective $\iff \ker(\phi) = \{e_G\}$.
($\Rightarrow$) Suppose ϕ is injective. Then for any $g_1, g_2 \in G$, $\phi(g_1) = \phi(g_2) \Rightarrow g_1 = g_2$; since ϕ is a homomorphism, this implies that $\phi(e_G) = e_H$. Therefore, $\ker(\phi) = \{e_G\}$.
($\Leftarrow$) Suppose that $\ker(\phi) = \{e_G\}$. If $g_1, g_2 \in G$ and $\phi(g_1) = \phi(g_2)$, then this implies that

$$\phi(g_1) \diamond [\phi(g_2)]^{-1} = e_H \iff \phi(g_1) \diamond \phi(g_2^{-1}) = e_H \iff \phi(g_1 \star g_2^{-1}) = e_H$$

$\Rightarrow g_1 \star g_2^{-1} = e_G \Rightarrow g_1 = g_2$, hence ϕ is injective.

1.6.15

Assuming $\mathbb{R}^2$ and $\mathbb{R}$ are additive groups we want to show that the function $\pi : \mathbb{R}^2 \to \mathbb{R}$ defined as $\pi(x, y) = x$ is a homomorphism. Observe that

$$\pi\big(x_1, y_2) + (x_2, y_2)\big) = \pi\big((x_1 + x_2, y_1 + y_2)\big) = x_1 + x_2 = \phi\big((x_1, y_2)\big) + \pi\big((x_2, y_2)\big)$$

$\Rightarrow \pi$ is a homomorphism.

Now, we want to describe $\ker(\pi)$. Observe that

$$\begin{aligned}\ker(\pi) &= \{(x, y) \in \mathbb{R}^2 : \pi(x, y) = 0\}\\ &= \{(x, y) \in \mathbb{R}^2 : x = 0\}\\ &= \{(0, y) : y \in \mathbb{R}\} \cong \mathbb{R}\end{aligned}$$

1.6.16

Given groups $(A, \star)$ and $(B, \diamond)$, we want to show that the functions $\pi_1 : A \times B \to A$ and $\pi_2 : A \times B \to B$ defined as $\pi_1\big((a, b)\big) = a$ and $\pi_2\big((a, b)\big) = b$ are homomorphisms. Observe that

$$\pi_1\big((a_1, b_1) \star (a_2, b_2)\big) = \pi_1\big((a_1 \star a_2, b_1 \diamond b_2)\big) = a_1 \star a_2 = \pi_1\big(a_1, b_2)\big) \star \pi_1\big((a_2, b_2)\big)$$

and similarly,

$$\pi_2\big((a_1, b_1) \star (a_2, b_2)\big) = \pi_2\big((a_1 \star a_2, b_1 \diamond b_2)\big) = b_1 \diamond b_2 = \pi_2\big((a_1, b_2)\big) \diamond \pi_2\big((a_2, b_2)\big)$$

Hence, π_1 and π_2 are homomorphisms. Furthermore,

$$\ker(\pi_1) = \{(a, b) \in A \times B : \pi_1\big((a, b)\big) = e_A\} = \{(e_A, b) : b \in B\} \cong B$$

and similarly

$$\ker(\pi_2) = \{(a, b) \in A \times B : \pi_2\big((a, b)\big) = e_B\} = \{(a, e_B) : a \in A\} \cong A$$

1.6.17

We want to show that the function $\phi : G \to G$ defined as $\phi(g) = g^{-1}$ is a homomorphism if and only if G is abelian.
$(\Rightarrow)$ Suppose ϕ is a homomorphism Then for any $g_1, g_2 \in G$, we have:

$$g_2^{-1} g_1^{-1} = (g_1 g_2)^{-1} = \phi(g_1 g_2) = \phi(g_1)\phi(g_2) = g_1^{-1} g_2^{-1}$$

$\Rightarrow g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1} \iff e_G = g_1 g_2 g_1^{-1} g_2^{-1} \iff g_2 g_1 = g_1 g_2 \Rightarrow G$ is abelian.
$(\Leftarrow)$ Suppose G is abelian. Then for every $g_1, g_2 \in G$, $g_1 g_2 = g_2 g_1$. Therefore,

$$\phi(g_1 g_2) = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1} = \phi(g_1)\phi(g_2)$$

$\Rightarrow \phi$ is a homomorphism.

1.6.18

$$\begin{aligned}\phi : G \to G \text{ defined by } \phi(g) = g^2 \text{ is a homomorphism} &\iff \forall\, g, h \in G, \phi(gh) = \phi(g)\phi(h)\\ &\iff (gh)^2 = g^2 h^2\\ &\iff ghgh = gghh\\ &\iff hg = gh\\ &\iff G \text{ is abelian.}\end{aligned}$$

1.6.19

We want to show that given the group $G = \{z \in \mathbb{C} : z^n = 1 \text{ for some } n \in \mathbb{N}\}$, the function $\phi : G \to G$ defined as $\phi(z) = z^k$ is a surjective homomorphism, but not isomorphism, for any integer $k > 1$.

Let $w, z \in G$. Then observe that $\phi(wz) = (wz)^k = w^k z^k = \phi(w)\phi(z) \Rightarrow \phi$ is a homomorphism. Moreover, if $z \in G$, then there exists $m \in \mathbb{N}$ such that $z^m = 1$. Therefore, $(z^{\frac{1}{k}})^{km} = z^{\frac{km}{k}} = z^m = 1 \Rightarrow z^{\frac{1}{k}} \in G$, and $\phi(z^{\frac{1}{k}}) = (z^{\frac{1}{k}})^k = z^{\frac{k}{k}} = z$; hence, ϕ is surjective. Note, however, ϕ is not an isomorphism because

$$\begin{aligned}
\ker(\phi) &= \{z \in G : \phi(z) = 1\} \\
&= \{z \in G : z^k = 1\} \\
&= \{e^{i\frac{2m\pi}{k}} : m = 0, 1, ..., k-1\} \\
&= \left\{\cos\left(\frac{2m\pi}{k}\right) + i \sin\left(\frac{2m\pi}{k}\right) : m = 0, 1, ..., k-1\right\} \\
&\neq \{1\}
\end{aligned}$$

$\Rightarrow \phi$ is not injective.

1.6.20

Let $\text{Aut}(G) := \{\phi : G \to G | \phi \text{ is an isomorphism}\}$; we want to show that $\text{Aut}(G)$ is a group under function composition.

If $f, g, h \in \text{Aut}(G)$, then observe that

$$\big(f \circ (g \circ h)\big)(x) = f\big((g \circ h)(x)\big) = f\big(g(h(x)\big) = \big(f \circ g\big)\big(h(x)\big) = \big((f \circ g) \circ h\big)(x)$$

$\Rightarrow \text{Aut}(G)$ is associative under $\circ$. Now, if $f, g \in \text{Aut}(G)$, then $f \circ g$ is a bijection and $\forall\, x, y \in G$,

$$(f \circ g)(xy) = f(g(xy)) = f\big(g(x)g(y)\big) = f\big(g(x)\big)f\big(g(y)\big) = (f \circ g)(x)(f \circ g)(y)$$

$\Rightarrow (f \circ g) \in \text{Aut}(G)$; i.e., $\text{Aut}(G)$ is closed under $\circ$. Lastly, if $f \in \text{Aut}(G)$, since f is a bijection, there exists a unique inverse functions $f^{-1} : G \to G$; moreover, $x', y' \in G \Rightarrow$ there exists unique $x, y \in G$ such that $x' = f(x), y' = f(y)$. Therefore,

$$f^{-1}(x'y') = f^{-1}\big(f(x)f(y)\big) = f^{-1}\big(f(xy)\big) = xy = f^{-1}(x')f^{-1}(y')$$

$\Rightarrow f^{-1} \in \text{Aut}(G)$; i.e., $\text{Aut}(G)$ is closed under inverses. Hence, $(\text{Aut}(G), \circ)$ is a group.

1.6.21

We want to show that for each fixed integer $k \neq 0$ that the function $\phi : \mathbb{Q} \to \mathbb{Q}$ is an automorphism, where $\mathbb{Q}$ is understood to be an additive group.

Let $k \neq 0$. Then observe that if $p, q \in \mathbb{Q}$, then

$$\begin{aligned}
& \phi(p) = \phi(q) \\
\iff & kp = kq \\
\iff & p = q
\end{aligned}$$

$\Rightarrow \phi$ is injective. Now, if $q \in \mathbb{Q}$, then since $k \neq 0$, $\frac{q}{k} \in \mathbb{Q}$; moreover, $\phi\left(\frac{q}{k}\right) = k \cdot \frac{q}{k} = q \Rightarrow \phi$ is surjective. Lastly, if $p, q \in \mathbb{Q}$, then $\phi(p+q) = k(p+q) = kp + kq = \phi(p) + \phi(q) \Rightarrow \phi$ is an isomorphism. Therefore, we conclude that ϕ is an automorphism on $\mathbb{Q}$.

1.6.22

Let e be the identity of the abelian group A. Then given a fixed integer k, we first want to show that the function $\phi : A \to A$ defined as $\phi(a) = a^k$ is a homomorphism. Let $a, b \in A$. Then observe that

$$\phi(ab) = (ab)^k \xlongequal{A \text{ abelian}} a^k b^k = \phi(a)\phi(b)$$

$\Rightarrow \phi$ is a homomorphism.

Now, we want to show that when $k = -1$, ϕ is an automorphism. It suffices to prove that when $k = -1$, ϕ is a bijection. Observe that

$$\begin{aligned} \ker(\phi) &= \{a \in A : \phi(a) = e\} \\ &= \{a \in A : a^{-1} = e\} \\ &= \{e\} \end{aligned}$$

$\Rightarrow \phi$ is injective. Now, if $a \in A$, then $a^{-1} \in A$ (since A is a group), and $\phi(a^{-1}) = (a^{-1})^{-1} = a \Rightarrow \phi$ is surjective. Therefore, when $k = -1$, ϕ is an automorphism.

1.6.23

We are told that $\sigma : G \to G$ is an automorphism such that $\sigma(g) = g$ if and only if $g = 1$, where 1 is the identity of G. We want to show that if $\sigma^2 : G \to G$ is the identity map, then G is abelian.

Set $H := \{x^{-1}\sigma(x) : x \in G\} \subseteq G$, and define the function $\phi : G \to H$ as $\phi(x) = x^{-1}\sigma(x)$. First note that $\phi(1) = 1^{-1}\sigma(1) = 1 \cdot 1 = 1$. Now, let $x \in G \setminus \{1\}$. Then since $x \neq 1 \Rightarrow \sigma(x) \neq x \Rightarrow x^{-1}\sigma(x) \neq 1$; furthermore, if $x, y \in G \setminus \{1\}$ and $\phi(x) = \phi(y)$, then we have:

$$x^{-1}\sigma(x) = y^{-1}\sigma(y) \iff yx^{-1} = \sigma(y)[\sigma(x)]^{-1} \iff yx^{-1} = \sigma(y)\sigma(x^{-1}) \iff yx^{-1} = \sigma(yx^{-1})$$

$\Rightarrow yx^{-1} = 1 \Rightarrow x = y$; i.e., $\phi : G \to H$ is one-to-one. Hence, $|G| \leq |H|$. Since $H \subseteq G$, this implies that $|G| \geq |H| \Rightarrow |G| = |H| \Rightarrow G = H$. Therefore, we conclude that every element in G can be expressed as $x^{-1}\sigma(x)$, where x is some other elment in G.

Thus, if $g \in G$, then there exists $x \in G$ such that $g = x^{-1}\sigma(x)$. Therefore,

$$\begin{aligned} \sigma(g) &= \sigma(x^{-1}\sigma(x)) \\ &= \sigma(x^{-1})\sigma^2(x) \\ &= [\sigma(x)]^{-1}x \\ &= [x^{-1}\sigma(x)]^{-1} \\ &= g^{-1} \end{aligned}$$

Hence, if $g, h \in G$, then $\sigma(gh) = (gh)^{-1} = h^{-1}g^{-1}$, yet on the other hand, $\sigma(gh) = \sigma(g)\sigma(h) = g^{-1}h^{-1}$; thus, $h^{-1}g^{-1} = g^{-1}h^{-1} \Rightarrow g^{-1}h = hg^{-1} \Rightarrow hg = gh$. That is, G is abelian.

1.6.24

We are told that the elements x and y, both of order 2, generate the finite group G; i.e., $\langle x, y \rangle = G$. Let $t := xy \in G$; note that we are told that $|t| = |xy| = n$. Then $|x| = 2$ implies that $x = x^{-1}$; hence,

$$\begin{aligned} & t = xy \\ \iff & t = xy^{-1} \\ \Rightarrow & tx = xy^{-1}x^{-1} \\ \iff & tx = x(xy)^{-1} \\ \iff & tx = xt^{-1} \end{aligned}$$

Also, $xt = x(xy) = x^{-1}xy = y \Rightarrow t$ and x generate G. Therefore, we have the group presentation of G:

$$\langle x, t | x^2 = t^n = 1, tx = xt^{-1} \rangle$$

Which is the same, up to notation, presentation as D_{2n}; thus, $G \cong D_{2n}$.

1.6.25

Do later....

1.6.26

We want to show that the function $\phi : Q_8 \to GL_2(\mathbb{C})$ defined by $\phi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$ and $\phi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ extends to a homomorphism. Recall that the presentation of Q_8 is:

$$\langle i, j | i^4 = 1, i^2 = j^2, ij = ji^{-1} \rangle$$

Therefore, if $\phi(i)$ and $\phi(j)$ satisfy the same relations in the presentation above, then we conclude that ϕ is a homomorphism between Q_8 to the group generated by $\phi(i)$ and $\phi(j)$, which we denote as $H \subset GL_2(\mathbb{C})$.

Observe that

$$[\phi(i)]^2 = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_{2\times 2}$$

$\Rightarrow [\phi(i)]^4 = (-I_{2\times 2})^2 = I_{2\times 2}$, and

$$[\phi(j)]^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_{2\times 2}$$

$\Rightarrow [\phi(i)]^2 = [\phi(j)]^2$; also,

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

and, on the other hand,

$$\phi(j)[\phi(i)]^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -\sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} = \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix}$$

$\Rightarrow \phi(i)\phi(j) = \phi(j)[\phi(i)]^{-1}$. Therefore, ϕ is a homomorphism between Q_8 and $H := \langle \phi(i), \phi(j) \rangle$. Furthermore, we have shown that $i, j, i^2 = j^2 = -1$, and $ij = k$ are not in $\ker(\phi) = \left\{ x \in Q_8 : \phi(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$, hence $i^{-1} = -i, j^{-1} = -j$, and $k^{-1} = -k$ are not in $\ker(\phi)$. Therefore, the only element of Q_8 in $\ker(\phi)$ is 1; thus, ϕ is injective $\Rightarrow Q_8 \cong H$.

1.7

1.7.1

Let $g_1, g_2 \in F^\times$ and $a \in F$. Then observe that

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &= g_1 \cdot (g_2 a) \\ &= g_1(g_2 a) \\ &= (g_1 g_2)a, \text{ by associativity in } F^\times \\ &= (g_1 g_2) \cdot a \end{aligned}$$

Moreover, if 1 is the multiplicative identity (or unit) in F, then $1 \cdot a = 1a = a$. Hence, $F^\times$ acts on F.

1.7.2

Let $z_1, z_2, a \in \mathbb{Z}$. Then

$$\begin{aligned} z_1 \cdot (z_2 \cdot a) &= z_1 \cdot (z_2 + a) \\ &= z_1 + (z_2 + a) \\ &= (z_1 + z_2) + a, \text{ by associativity of } (\mathbb{Z}, +) \\ &= (z_1 + z_2) \cdot a \end{aligned}$$

Also, 0 is the identity element in $(\mathbb{Z}, +)$, and $0 \cdot a = 0 + a = a$. Hence, $\mathbb{Z}$ acts on itself via left translation.

1.7.3

Let $r, s \in \mathbb{R}$ and $(x, y) \in \mathbb{R} \times \mathbb{R}$. Then observe that:

$$\begin{aligned} r \cdot (s \cdot (x, y)) &= r \cdot ((x + sy, y)) \\ &= ((x + sy) + ry, y) \\ &= (x + (r + s)y, y) \\ &= (r + s) \cdot (x, y) \end{aligned}$$

Also, 0 is the identity in $(\mathbb{R}, +)$, and $0 \cdot (x, y) = (x + 0y, y) = (x, y)$. Thus, $\mathbb{R}$ acts on $\mathbb{R} \times \mathbb{R}$ with the given map.

1.7.4

(a) Recall that the kernal of the action of G on A is the set $\{g \in G : g \cdot a = a, \forall a \in A\}$, which I will denote as $\ker$. To show that $\ker$ is a subgroup of G, we need to show that $\ker$ is nonempty, and that $h, k \in \ker$ implies that $h^{-1} \in \ker$ and $hk \in \ker$. First note that if e is the identity element in G, then $e \in \ker$ since by the definition of a group action $e \cdot a = a \ \forall a \in A$. Thus, $\ker$ is nonempty. Now, suppose $h, k \in \ker$. Then, since by the definition of group action, for any $a \in A$, we have:

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

Now, since $h \cdot a = a \ \forall a \in A$, this implies that $h^{-1} \cdot a = a \ \forall a \in A$; hence, $h^{-1} \in \ker$. Furthermore, for all $a \in A$, we have:

$$(hk) \cdot a = h \cdot (k \cdot a) = h \cdot a = a$$

$\Rightarrow hk \in \ker$. Hence, $\ker$ is a subgroup of G.

(b) For fixed $a \in G$, denote the stabilizer of G as $G_a := \{g \in G : ga = a\}$. Again, to show that G_a is a subgroup of G, we need to show that it is nonempty and closed under both its group operations and inverses. First, note that if e is the identity element of G, then $ea = a \Rightarrow e \in G_a$, hence $G_a \neq \emptyset$. Now, suppose $h, k \in G_a$. Then observe that

$$h^{-1}a = h^{-1}(ha) = (h^{-1}h)a = ea = a$$

$\Rightarrow h^{-1} \in G_a$. Also, observe that

$$(hk)a = h(ka) = ha = a$$

$\Rightarrow hk \in G_a$. Hence, G_a is a subgroup of G, for each $a \in G$.

1.7.5

We want to show that the kernal of an action of the group G on the set A is the same as the kernal of the corresponding permutation representation $G \to S_A$ defined as $g \mapsto \sigma_g$. That is, we want to show that the set $\{g \in G : g \cdot a = a, \forall a \in A\}$ is the same as the set $\{g \in G : \sigma_g = id_A\}$. If $g \in G$ is such that $g \cdot a = a \ \forall a \in A$, then for every $a \in A$, $\sigma_g(a) = g \cdot a = a \Rightarrow \sigma_g = id_A$. Hence, $\{g \in G : g \cdot a = a, \forall a \in A\} \subseteq \{g \in G : \sigma_g = id_A\}$. Alternatively, if $g \in G$ is such that $\sigma_g = id_A$, then for every $a \in A$, $g \cdot a = \sigma_g(a) = a \Rightarrow g \cdot a = a \ \forall a \in A$. Hence, $\{g \in G : \sigma_g = id_A\} \subseteq \{g \in G : g \cdot a = g\}$. Therefore, the two sets are equal.

1.7.6

By definition of a group action, the group identity element, e, satisfies the property $e \cdot a = a \; \forall a \in A$, which is the necessary condition for an element to be in the kernal of the group action.

Suppose G acts faithfully on A. This means that for every $g_1, g_2 \in G$ such that $g_1 \neq g_2$, we have

$$g_1 \cdot a \neq g_2 \cdot a$$

for some $a \in A$. Therefore, if g is in the kernal of the group action, then $g \cdot a = a \; \forall a \in A \Rightarrow g = e$. That is, the kernal only consists of e.

Conversely, suppose that the kernal consists only of e, and assume for the sake of contradiction that G does not act faithfully on A. Then, there exists $g_1, g_2 \in G$ such that $g_1 \cdot a = g_2 \cdot a$ for every $a \in A$. Consequently, for each $a \in A$, we have:

$$\begin{aligned}
(g_1^{-1} g_2) \cdot a &= g_1^{-1} \cdot (g_2 \cdot a) \\
&= g_1^{-1} \cdot (g_1 \cdot a) \\
&= (g_1^{-1} g_1) \cdot a \\
&= e \cdot a \\
&= a
\end{aligned}$$

$\Rightarrow g_1^{-1} g_2$ is in the kernal of the group action $\Rightarrow g_1^{-1} g_2 = e \Rightarrow g_2 = g_1 \Rightarrow\Leftarrow$. Hence, when the kernal consists of only the identity element, G acts faithfully on A.

1.7.7

The group action $F^\times \times V \to V$ is defined as the normal (componentwise) scalar multiplication equipped to vector spaces. That is, $\lambda \cdot \mathbf{v} \mapsto \lambda(v_1, ..., v_n) = (\lambda v_1, ..., \lambda v_n)$. We want to show that F^X acts faithfully on V; that is, we want to show that for every $\lambda_1, \lambda_2 \in F^\times$ such that $\lambda_1 \neq \lambda_2$, there exists $\mathbf{v} \in V$ such that $\lambda_1 \cdot \mathbf{v} \neq \lambda_2 \cdot \mathbf{v}$.

Assume for the sake of contradiction that the $F^\times$ does not act faithfully on V. Then, there exists $\lambda_1, \lambda_2 \in F^\times$ such that $\lambda_1 \neq \lambda_2$ and for every $\mathbf{v} \in V$,

$$\begin{aligned}
&\lambda_1 \cdot \mathbf{v} = \lambda_2 \cdot \mathbf{v} \\
\iff\; &\lambda_1(v_1, ..., v_n) = \lambda_2(v_1, ..., v_n) \\
\iff\; &(\lambda_1 v_1, ..., \lambda_1 v_n) = (\lambda_2 v_1, ..., \lambda_2 v_n) \\
\iff\; &\lambda_1 v_i = \lambda_2 v_i, \text{ for } i = 1, ..., n \\
\iff\; &(\lambda_1 - \lambda_2) v_i = 0, \text{ for } i = 1, ..., n \qquad (\star)
\end{aligned}$$

Since $(\star)$ must hold for every $\mathbf{v} \in V$, letting $\mathbf{v} := (1, 0, ..., 0$ gives us a contradiction. Hence, $F^\times$ acts faithfully on V.

1.7.8

We are told that A is a nonempty set and that for fixed $k \in \mathbb{N}$ with $k \leq |A|$, B is a collection of subsets of A with cardinality k. We are also told that $S_A \times B \to B$ is defined as $\sigma \cdot \{a_1, ..., a_k\} = \{\sigma(a_1), ..., \sigma(a_k)\}$.

(a) First we want to show that $S_A \times B \to B$ as defined above is a group action. Observe that if $\sigma_1, \sigma_2 \in S_A$ and $\{a_1, ..., a_k\} \in B$, then

$$\begin{aligned}
\sigma_1 \cdot (\sigma_2 \cdot \{a_1, ..., a_k\}) &= \sigma_1 \cdot \{\sigma_2(a_1), ..., \sigma_2(a_k)\} \\
&= \{\sigma_1(\sigma_2(a_1)), ..., \sigma_1(\sigma_2(a_k))\} \\
&= \{(\sigma_1 \circ \sigma_2)(a_1), ..., (\sigma_1 \circ \sigma_2)(a_k)\} \\
&= (\sigma_1 \circ \sigma_2) \cdot \{a_1, ..., a_k\}
\end{aligned}$$

Also, $id_A \cdot \{a_1, ..., a_k\} = \{id_A(a_1), ..., id_A(a_k)\} = \{a_1, ..., a_k\}$. Hence, $S_A \times B \to B$ as defined above is a group action.

(b) The six $2-$element subsets of $\{1,2,3,4\}$ are $\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}$. Observe that

$$\begin{aligned} (1,2)\cdot\{1,2\} &= \{1,2\} & (1,2)\cdot\{2,3\} &= \{1,3\} \\ (1,2)\cdot\{1,3\} &= \{2,3\} & (1,2)\cdot\{2,4\} &= \{1,4\} \\ (1,2)\cdot\{1,4\} &= \{2,4\} & (1,2)\cdot\{3,4\} &= \{3,4\} \end{aligned}$$

and

$$\begin{aligned} (1,2,3)\cdot\{1,2\} &= \{2,3\} & (1,2,3)\cdot\{2,3\} &= \{1,3\} \\ (1,2,3)\cdot\{1,3\} &= \{1,2\} & (1,2,3)\cdot\{2,4\} &= \{3,4\} \\ (1,2,3)\cdot\{1,4\} &= \{2,4\} & (1,2,3)\cdot\{3,4\} &= \{1,4\} \end{aligned}$$

1.7.9

Omitted.

1.7.10

Omitted.

1.7.11

Denote the set of vertices of the square on page 24 of D&F as V. We denote the permutation obtained by an element x acting on the vertices as $x \cdot V$. Then, we have:

$$\begin{aligned} 1\cdot V &= (1) & s\cdot V &= (24) \\ r\cdot V &= (1234) & sr\cdot V &= (14)(23) \\ r^2\cdot V &= (13)(24) & sr^2\cdot V &= (13) \\ r^3\cdot V &= (1432) & sr^3\cdot V &= (12)(34) \end{aligned}$$

1.7.12

Omitted.

1.7.13

Let e be the identity element of G, and recall that the left regular action $G \times G \to G$ on G is given by $g \cdot a = ga$; i.e., it is just left multiplication of elements in G.

Then $\ker = \{g \in G : g \cdot a = a \ \forall a \in G\} = \{g \in G : ga = a \ \forall a \in G\}$; in particular, $g \in \ker \Rightarrow g \cdot g = g \iff g^2 = g \Rightarrow g = e$. Hence, $\ker = \{e\}$.

1.7.14

Since G is not abelian, there exists $g_1, g_2 \in G$ such that $g_1g_2 \neq g_2g_1$. Then observe that for any $a \in A$, we have:

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (ag_2) = ag_2g_1$$

but

$$(g_1g_2) \cdot a = ag_1g_2$$

Since $A = G$, we may let $a = e$. Then since $g_1g_2 \neq g_2g_1$, this implies that $g_1 \cdot (g_2 \cdot a) \neq (g_1g_2) \cdot a$ for atleast one $a \in G$, hence the group action conditions are not satisfied.

1.7.15

Let $g_1, g_2 \in G$ and $a \in A = G$. Then observe that:

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &= g_1 \cdot a g_2^{-1} \\ &= a g_2^{-1} g_1^{-1} \\ &= a(g_1 g_2)^{-1} \\ &= (g_1 g_2) \cdot a \end{aligned}$$

Moreover, if e denotes the identity element in G, then we have:

$$e \cdot a = a e^{-1} = a$$

Therefore, $g \cdot a = a g^{-1}$ satisfies the group action axioms.

1.7.16

Let $g_1, g_2 \in G$ and $a \in A = G$. Then observe that:

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &= g_1 \cdot g_2 a g_2^{-1} \\ &= g_1 (g_2 a g_2^{-1}) g_1^{-1} \\ &= (g_1 g_2) a (g_1 g_2)^{-1} \\ &= (g_1 g_2) \cdot a \end{aligned}$$

Moreover, if e denotes the identity element in G, then we have:

$$e \cdot a = e a e^{-1} = a$$

Therefore, conjugation is a group action.

1.7.17

For fixed $g \in G$, let $\chi_g : G \to G$ be given by $\chi_g(x) = g x g^{-1}$. Then observe that for any $x, y \in G$, we have:

$$\begin{aligned} \chi_g(x)\chi_g(y) &= (g x g^{-1})(g y g^{-1}) \\ &= g x (g^{-1} g) y g^{-1} \\ &= g x y g^{-1} \\ &= \chi_g(xy) \end{aligned}$$

$\Rightarrow \chi_g$ is a homomorphism. Now, consider $\chi_{g^{-1}}$. Observe that for any $x \in G$, we have:

$$\begin{aligned} \big(\chi_g \circ \chi_{g^{-1}}\big)(x) &= \chi_g\big(\chi_{g^{-1}}(x)\big) \\ &= \chi_g\big(g^{-1} x (g^{-1})^{-1}\big) \\ &= \chi_g(g^{-1} x g) \\ &= g(g^{-1} x g) g^{-1} \\ &= x \end{aligned}$$

and similarly

$$\begin{aligned} (\chi_{g^{-1}} \circ \chi_g)(x) &= \chi_{g^{-1}}\big(\chi_g(x)\big) \\ &= \chi_{g^{-1}}(g x g^{-1}) \\ &= g^{-1}(g x g^{-1})(g^{-1})^{-1} \\ &= g^{-1}(g x g^{-1}) g \\ &= x \end{aligned}$$

Hence, $\chi_{g^{-1}}$ is the inverse of χ_g, which shows that χ_g is a bijection; thus, χ_g is an isomorphism.

Now, suppose $|x| = n$. Then for any $g \in G$, it is easy to see that $\prod_{i=1}^{n} gxg^{-1} = gx^n g^{-1}$; hence $|x| = n$ implies that $|gxg^{-1}| = n$. Furthermore, since we showed above that $\chi_g : G \to G$ is an isomorphism, if $A \subset G$, this implies that $|A| \cong |\chi_g(A)| = |gAg^{-1}|$.

1.7.18

Let $a, b, c \in A$. Then observe that:

- $a \sim a \iff a = ha$ for some $h \in H$; let $h := e$, and reflexivity is satisfied.
- $a \sim b \iff a = hb \Rightarrow h^{-1}a = h^{-1}hb = b \Rightarrow b \sim a$, thus symmetry is satisfied.
- $a \sim b, b \sim c \iff a = h_1 b, b = h_2 c \Rightarrow a = h_1(h_2 c) = (h_1 h_2)c \Rightarrow a \sim c$, thus transitivity is satisfied.

Therefore, $\sim$ is an equivalence relation.

1.7.19

Let $\theta : H \to \mathcal{O}_x$ be given by $\theta(h) = hx$. If $h_1, h_2 \in H$, then observe that:

$$\begin{aligned} &\theta(h_1) = \theta(h_2) \\ \iff\ & h_1 x = h_2 x \\ \iff\ & h_1 = h_2, \quad \text{since } x \in G \end{aligned}$$

$\Rightarrow$ θ is injective. Now, if $y \in \mathcal{O}_x$, then $y = hx$ for some $h \in H$, which implies that $y = \theta(h)$, showing that θ is surjective. Therefore, θ is a bijection; since $x \in G$ is arbitrary, we conclude that all orbits under the action of H have the same cardinality as H.

Now, we are assuming G is a finite group, say of cardinality n; denote the elements of G as $x_1, x_2, ..., x_n$. In the previous exercise we showed that orbits under the action of H partition H, and in this exercise we have shown that the orbits under the action of H each have the same cardinality; the same cardinality as H in particular. Therefore,

$$|G| = \sum_{i=1}^{n} |\mathcal{O}_x| = \sum_{i=1}^{n} |H| = n|H|$$

$\Rightarrow |H|$ divides $|G|$.

1.7.20

Let S denote the group of symmetries of a tetrahedron, and let A denote the vertices of the tetrahedron; note that $|A| = 4$. Then by definition of rigid motions, for each $s \in S$, s sends each vertex in A to a vertex in A, and it does so bijectively; that is, s induces a permutation on A, which we denote σ_s. Therefore, S acts on A, and the action is given by $s \cdot a = \sigma_s(a)$.

Now, consider the map $\varphi : S \to S_4$ given by $\varphi(s) = \sigma_s$. Let $s, t \in S$. Then observe that for each $a \in A$, we have:

$$\begin{aligned} \varphi(st)(a) &= \sigma_{st}(a) \\ &= (st) \cdot a \\ &= s \cdot (t \cdot a) \\ &= s \cdot \sigma_t(a) \\ &= \sigma_s\big(\sigma_t(a)\big) \\ &= (\sigma_s \circ \sigma_t)(a) \\ &= \varphi(s)\varphi(t)(a) \end{aligned}$$

which shows that φ is a homomorphism. Note that it is also injective, since

$$\begin{aligned} &\varphi(s) = \varphi(t) \\ \iff\ &\varphi(s)(a) = \varphi(t)(a), \forall a \in A \\ \iff\ &\sigma_s(a) = \sigma_t(a), \forall a \in A \\ \iff\ &s \cdot a = t \cdot a, \forall a \in A \end{aligned}$$

$\Rightarrow s = t$. Consequently, $S \cong \varphi(S) \leq S_4$.

1.7.21

Omitted.

1.7.22

Omitted.

1.7.23

Omitted.