Chapter 1.1

These problems implicitly make use of the following lemma (stated casually in the book).

Lemma *If $(G, \star)$ is a group and $H \subseteq G$ is closed under $\star$, then $\star$ is associative in H.*

Proof. We know $\star$ is associative in G by definition of a group. Now let $a, b, c \in H$. Since H is closed, $a \star (b \star c), (a \star b) \star c \in H$. However, since $a, b, c \in H$ implies $a, b, c \in G$ we also know $a \star (b \star c) = (a \star b) \star c$. Hence, $\star$ is associative in H.

Problem 1.1.1 *Determine which of the following binary operations are associative:*

(a) *the operation $\star$ on $\mathbb{Z}$ defined $a \star b = a - b$*

(b) *the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$*

(c) *the operation $\star$ on $\mathbb{Q}$ defind by $a \star b = \frac{a+b}{5}$*

(d) *the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$*

(e) *the operation $\star$ on $\mathbb{Q} - \{0\}$ defined by $a \star b = \frac{a}{b}$.*

Solution. (a) Not associative. For example, $(2 \star 1) \star 1 = 0 \neq 2 = 2 \star (1 \star 1)$.

(b) Associative, because

$$\begin{aligned}(a \star b) \star c &= (a + b + ab) \star c = (a + b + ab) + c + (a + b + ab)c \\ &= a + (b + c + bc) + a(b + c + bc) = a + (b \star c) + a(b \star c) = a \star (b \star c).\end{aligned}$$

The intermediate steps follow because usual addition and multiplication is associative and commutative in $\mathbb{Z}$.

(c) Not associative. For example, $(0 \star 0) \star 25 = 5 \neq 1 = 0 \star (0 \star 25)$.

(d) Associative, because

$$\begin{aligned}((a, b) \star (c, d)) \star (e, f) &= (ad + bc, bd) \star (e, f) = ((ad + bc)f + (bd)e, (bd)f) \\ &= (a(df) + b(cf + de), b(df)) = (a, b) \star (cf + de, df) \\ &= (a, b) \star ((c, d) \star (e, f)).\end{aligned}$$

Notice we could not say $(\mathbb{Z} \times \mathbb{Z}, \star)$ is isomorphic to $(\mathbb{Q}, +)$ even though intuitively $\frac{a}{b} + \frac{c}{d} = \frac{ab+bc}{bd}$, because this would exclude b or d equal to 0 (which is encompassed by the former).

(e) Not associative. For example, $(1 \star 1) \star 2 = \frac{1}{2} \neq 2 = 1 \star (1 \star 2)$.

Problem 1.1.2 *Decide which of the binary operations in the preceding exercise are commutative.*

Solution. (a) Not commutative. For example, $1 \star 0 = 1 \neq -1 = 0 \star 1$.

(b) Commutative, because

$$a \star b = a + b + ab = b + a + ba = b \star a,$$

due to addition and multiplication being commutative in $\mathbb{Z}$.

(c) Commutative, because

$$a \star b = \frac{a+b}{5} = \frac{b+a}{5} = b \star a,$$

due to addition being commutative in $\mathbb{Z}$.

(d) Commutative, because

$$(a,b)\star(c,d) = (ad+bc, bd) = (cb+da, db) = (c,d)\star(a,b),$$

due to addition and multiplicaiton being commutative in $\mathbb{Z}$.

(e) Not commutative. For example, $2\star 1 = 2 \neq \frac{1}{2} = 1\star 2$.

Problem 1.1.3 *Prove that the addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).*

Proof. Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$. Then $\overline{a} + \left(\overline{b} + \overline{c}\right) = \overline{a} + \overline{b+c}$ (by definition--see page 9 in the book), which equals $\overline{a + (b+c)} = \overline{a+b+c}$ (again by definition). However,

$$\overline{a+b+c} = \overline{(a+b)+c} = \overline{a+b} + \overline{c} = \left(\overline{a} + \overline{b}\right) + \overline{c}. \square$$

Problem 1.1.4 *Prove that the multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).*

Proof. Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$. Then $\overline{a}\left(\overline{b} \cdot \overline{c}\right) = \overline{a} \cdot \overline{bc}$ (by definition--see page 9 in the book), which equals $\overline{a(bc)} = \overline{abc}$ (again by definition). However,

$$\overline{abc} = \overline{(ab)c} = \overline{ab} \cdot \overline{c} = \left(\overline{a} \cdot \overline{b}\right)\overline{c}. \square$$

Problem 1.1.5 *Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.*

Proof. In the book, we've seen $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group. Hence, $\overline{0}$ must be the guilty element of breaking this structure. Indeed, $\overline{0}$ has no inverse, since $\overline{0} \cdot \overline{a} = \overline{0 \cdot a} = \overline{0} = \overline{a \cdot 0} = \overline{a} \cdot \overline{0}$ for any $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, and we know $\overline{1}$ is the identity since $\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a} = \overline{a \cdot 1} = \overline{a} \cdot \overline{1}$ for any $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Since there is no element $\overline{a}$ such that $\overline{0} \cdot \overline{a} = \overline{1}$, $\overline{0}$ has no inverse and by definition $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes. $\square$

Problem 1.1.6 *Determine which of the following sets are groups under addition:*

(a) *the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd*

(b) *the set of rational numbers (inculding $0 = 0/1$) in lowest terms whose denominators are even*

(c) *the set of rational numbers of absolute value < 1*

(d) *the set of rational numbers of absolute value ≥ 1 together with 0*

(e) *the set of rational numbers with denominators equal to 1 or 2*

(f) *the set of rational numbers with denominators equal to 1, 2, or 3.*

Solution. For each respective problem, call the group G.

(a) This is a group. First, if $\frac{a}{b}, \frac{c}{d} \in G$ with $2 \nmid b$ and $2 \nmid d$ (i.e., both are odd) and $(a,b) = (c,d) = 1$, then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in G$$

since $2 \nmid bd$; hence we have closure. We know it is associative since $\mathbb{Q}$ is on addition and $G \subset \mathbb{Q}$. The identity is $0/1$ since $\frac{0}{1} + \frac{a}{b} = \frac{a}{b} = \frac{a}{b} + \frac{0}{1}$ for all $\frac{a}{b} \in G$. Finally, each element has an inverse since $\frac{a}{b} + \frac{-a}{b} = \frac{0}{1}$ for any $\frac{a}{b} \in G$.

(b) This is not a group because it does not have closure. For example, $\frac{1}{2} \in G$ but $\frac{1}{2} - \frac{1}{2} = \frac{1}{1} \notin G$ since $\frac{1}{1}$ is in lowest terms and the denominator is odd (not even).

(c) This is not a group because it does not have closure. For example, $\frac{1}{2} \in G$ since $\left|\frac{1}{2}\right| \leq 1$ but $\frac{1}{2} + \frac{1}{2} = 1 \notin G$ since $|1| \not< 1$.

(d) This is not a group since it fails closure. For example, $\frac{3}{2}, -1 \in G$ since $\left|\frac{3}{2}\right| > |-1| \geq 1$, but $\frac{3}{2} + (-1) = \frac{1}{2} \notin G$ since $\left|\frac{1}{2}\right| \not\geq 1$ and $\frac{1}{2} \neq 0$.

(e) Assume each rational number is in lowest form. This is a group. First, take $\frac{a}{b}, \frac{c}{d} \in G$ with the greatest common divisor of a and b, and c and d equal to 1. Consider $b = d = 2$. Then $\frac{a}{2} + \frac{c}{2} = \frac{a+c}{2} \in G$. Otherwise, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in G$ since $bd = 1$ or 2 since $\gcd(bd, ad + bc) = 1$ or 2 (if $bd = 2$ and $ad + bc$ is even, the gcd becomes 1). Hence, G is closed. We know it is associative since $\mathbb{Q}$ is on addition and $G \subset \mathbb{Q}$. The identity is $0/1$ since $\frac{0}{1} + \frac{a}{b} = \frac{a}{b} = \frac{a}{b} + \frac{0}{1}$ for all $\frac{a}{b} \in G$. Finally, each element has an inverse since $\frac{a}{b} + \frac{-a}{b} = \frac{0}{1}$ for any $\frac{a}{b} \in G$. By definition, G is a group.

(f) This is not a group because it is not closed. For example, $\frac{1}{2}, \frac{-1}{3} \in G$ but $\frac{1}{2} + \frac{-1}{3} = \frac{1}{6} \notin G$. □

Problem 1.1.7 *Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$ (i.e., $x \star y = x + y - [x + y]$ where $[a]$ is the greatest integer less than or equal to a). Prove that $\star$ is a well-defined binary operation on G and that G is an abelian group under $\star$ (called the real numbers mod* 1).

Proof. To show the operation is well-defined, notice either $0 \leq x + y < 1$ or $1 \leq x + y < 2$. In the former case, $[x + y] = 0$ so that $x \star y = x + y - [x + y] = x + y$. Otherwise, $[x + y] = 1$ so that $x \star y = x + y - 1$. Hence, $\star$ is a well-defined binary operation on G. To show closure, again consider the two cases mentioned earlier. In the former, $x \star y = x + y$ and since $0 \leq x + y = x \star y < 1$ by assumption, $x \star y \in G$. In the latter case, $x \star y = x + y - 1$ and since $1 \leq x + y < 2$ we have $1 - 1 = 0 \leq x + y - 1 = x \star y < 2 - 1 = 1$ so again $x \star y \in G$. Therefore, G is closed. To show it is associative, notice for $x, y, z \in G$,

$$(x \star y) \star z = (x + y + [x + y]) \star z = (x + y - [x + y]) + z - [x + y - [x + y] + z] =$$
$$= x + y + z - [y + z] - [x + y + z - [y + z]] = x + (y \star z) - [x + (y \star z)] = x \star (y \star z).$$

The middle equality holds because $[x + y] + [x + y - [x + y] + z] = [y + z] + [x + y + z - [y + z]]$ which needs to be explicitly justified case-by-case. Assume $0 \leq x + y \leq 1$ and $0 \leq y + z \leq 1$, or $1 \leq x + y < 2$ and $1 \leq y + z < 2$. Then $[x + y] = [y + z] = 1$ so the equation holds. Otherwise, assume without loss of generality $0 \leq x + y \leq 1$ and $1 \leq y + z < 2$. Then $[x + y] = 0$ and $[y + z] = 1$, so that

$$[x + y] + [x + y - [x + y] + z] = [x + y + z] = 1 + [x + y + z - 1] = [y + z] + [x + y + z - [y + z]].$$

Hence, the operation is associative. Furthermore, 0 is the identity since
$0 + x + [0 + x] = x + 0 + [x + 0] = x + [x]$ for any $x \in G$. Finally, each element has an inverse, since
$x + (-x) + [x + (-x)] = (-x) + x + [(-x) + x] = 0 + [0] = 0$ for each $x \in G$. Therefore, G is a group. Finally, G is abelian since for any $x, y \in G$, we have that $x + y + [x + y] = y + x + [y + x]$ since addition is commutative in $\mathbb{R}$. Hence, G is an abelian group. □

Problem 1.1.8 *Let $G = \{z \in \mathbb{C} \mid z^n = 1$ for some $n \in \mathbb{Z}^+\}$.*

(a) *Prove that G is a group under multiplication (called the group of* roots of unity *of $\mathbb{C}$).*

(b) *Prove that G is not a group under addition.*

Proof. (a) To prove closure, let $w, z \in G$. Then $\exists n, m \in \mathbb{Z}^+$ such that $w^n = z^m = 1$. Then $(wz)^{nm} = (w^n)^m (z^m)^n = 1^m 1^n = 1$ and since $nm \in \mathbb{Z}^+$ (the positive integers are closed under multiplication), by definition $wz \in G$. Hence, G is closed. Associativity is guaranteed since $\mathbb{C}\backslash\{0\}$ is a group under multiplication, and $G \subset \mathbb{C}\backslash\{0\}$ (notice $0 \notin G$ since there is no $n \in \mathbb{Z}^+$ such that $0^n = 1$). The identity

is 1 since for $n = 1 \in \mathbb{Z}^+$ we have $1^1 = 1$ so that $1 \in G$, and furthermore for all $z \in G$, $1 \cdot z = z \cdot 1 = z$. Finally, each element has an inverse since for each $z \in G$ there is an $n \in \mathbb{Z}^+$ such that $z^n = 1$, so that $z^{n-1}z = z \cdot z^{n-1} = z^n = 1$. Therefore, $(G, \cdot)$ is a group. □

(b) Since $1 \in G$, it can not be a group under multiplication since $1 + 1 = 2 \notin G$ as there is no $n \in \mathbb{Z}^+$ such that $2^n = 1$ (and hence G is not closed). □

Problem 1.1.9 *Let* $G = \left\{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\right\}$.

(a) *Prove that G is a group under addition.*

(b) *Prove that the nonzero elements of G are a group under multiplication.*

Proof. (a) Let $a + b\sqrt{2}, c + d\sqrt{2} \in G$. Then $\left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right) = (a + c) + (b + d)\sqrt{2}$ is in the group, because $a + c, b + d \in \mathbb{Q}$ (since $(\mathbb{Q}, +)$ is a group). Associativity is guaranteed since $G \subset \mathbb{R}$ and $(\mathbb{R}, +)$ is a group. The identity is $0 + 0\sqrt{2}$ since $\left(0 + 0\sqrt{2}\right) + \left(a + b\sqrt{2}\right) = \left(a + b\sqrt{2}\right) + \left(0 + 0\sqrt{2}\right) = a + b\sqrt{2}$ for any $a + b\sqrt{2} \in G$. Finally, each element has an inverse since for $a + b\sqrt{2} \in G$, $\left(a + b\sqrt{2}\right) + \left(-a + (-b)\sqrt{2}\right) = \left(-a + (-b)\sqrt{2}\right) + \left(a + b\sqrt{2}\right) = 0 + 0\sqrt{2}$. Therefore, G is a group under addition. □

(b) Let $a + b\sqrt{2}, c + d\sqrt{2} \in G$. Then $\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = (ac + 2bd) + (ad + bc)\sqrt{2}$ is in the group, because $ac + 2bd, ad + bc \in \mathbb{Q}$ (since $(\mathbb{Q}, \cdot)$ is a group). Associativity is guaranteed since $G \subset \mathbb{R}$ and $(\mathbb{R}, \cdot)$ is a group. The identity is $1 + 0\sqrt{2}$ since $\left(1 + 0\sqrt{2}\right)\left(a + b\sqrt{2}\right) = \left(a + b\sqrt{2}\right) \cdot \left(1 + 0\sqrt{2}\right) = a + b\sqrt{2}$ for any $a + b\sqrt{2} \in G$. Finally, each element has an inverse since for $a + b\sqrt{2} \in G$, $\left(a + b\sqrt{2}\right)\left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right) = \left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right)\left(a + b\sqrt{2}\right) = 1 + 0\sqrt{2}$ (this was obtained by solving for c and d in $ac + 2bd = 1, ad + bc = 0$). We know $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in G$ since $\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in G$ (notice the denominator can never be 0 or that would contradict $a, b \in \mathbb{Q}$, and neither can both the terms be 0 since $0 \notin G\backslash\{0\}$). Therefore, $G\backslash\{0\}$ is a group under multiplication. □

Problem 1.1.10 *Prove that a finite group is abelian if and only if its group table is a symmetric matrix.*

Proof. Assume $G = \{g_1, ..., g_n\}$ is a finite abelian group. Then the i, j entry in its group table is the group element $g_ig_j = g_jg_i$. The j, i entry in its group table is the group element $g_jg_i = g_ig_j$. Hence, by definition, the group table is a symmetric matrix. Now assume $G = \{g_1, ..., g_n\}$ is a finite group with a symmetric matrix. Then the i, j entry is the same as the j, i entry, that is, $g_ig_j = g_jg_i$. However, this holds for any two elements $g_i, g_j \in G$ so that $g_ig_j = g_jg_i$ for all elements of G. This is precisely the definition of an abelian group. □

Problem 1.1.11 *Find the orders of each element of the additive group* $\mathbb{Z}/12\mathbb{Z}$.

Solution. The group is $\mathbb{Z}/12\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{11}\right\}$. Then the orders, respectively, are 1, 12, 6, 4, 3, 12, 2, 12, 3, 4, 6, and 12. Notice these are $|G|/\gcd(x, |G|)$. Indeed, this will be proven later. □

Problem 1.1.12 *Find the orders of the following elements of the multiplicative group* $(\mathbb{Z}/12\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{7}$, $\overline{-7}, \overline{13}$.

Solution. The identity is 1, so the order for $\overline{x}$ is the smallest $n \in \mathbb{Z}^+ \cup \{\infty\}$ such that $x^n = 1$ (with $x^\infty = 1$). Respectively, these are $1, 2, 2, 2, 4$, and 1 (since $\overline{13} = \overline{1}$). $\square$

Problem 1.1.13 *Find the orders of the following elements of the additive group* $\mathbb{Z}/36\mathbb{Z}$: $\overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.

Solution. The identity is 0, so the order for $\overline{x}$ is the smallest $n \in \mathbb{Z}^+ \cup \{\infty\}$ such that $nx = 0$ (with $\infty x = 0$). Respectively, these are $36, 18, 6, 4, 18, 3, 36, 18, 2$. $\square$

Problem 1.1.14 *Find the orders of the following elements of the multiplicative group* $(\mathbb{Z}/36\mathbb{Z})^\times$: $\overline{1}, \overline{-1}, \overline{5}, \overline{13}, \overline{-13}, \overline{17}$.

Solution. The identity is 1, so the order for $\overline{x}$ is the smallest $n \in \mathbb{Z}^+ \cup \{\infty\}$ such that $x^n = 1$ (with $x^\infty = 1$). Respectively, these are $1, 2, 6, 3, 6, 2$. $\square$

Problem 1.1.15 *Prove that* $(a_1 a_2 ... a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} ... a_1^{-1}$

Proof. Assume $(a_1 a_2 ... a_n)x = 1$ so that $x = (a_1 a_2 ... a_n)^{-1}$. Then $a_1^{-1}(a_1 a_2 ... a_n)x = a_1^{-1} \cdot 1$ so that $(a_1^{-1} a_1)(a_2 a_3 ... a_n)x = (a_2 a_3 ... a_n)x = a_1^{-1}$. Similarly, $(a_3 a_4 ... a_n)x = a_2^{-1} a_1^{-1}$. Applying this n times results in $x = a_n^{-1} a_{n-1}^{-1} ... a_1^{-1}$, as desired. $\square$

Problem 1.1.16 *Let* x *be an element of* G. *Prove that* $x^2 = 1$ *if and only if* $|x|$ *is either* 1 *or* 2.

Proof. Assume $x^2 = 1$. If $x = 1$, then $|x| = 1$. Otherwise, $|x| \neq 1$ (only the identity has order 1) so that $|x| = 2$ by definition since 2 would be the smallest power x need be raised to in order to obtain the identity. On the other hand, assume $|x|$ is either 1 or 2. If $|x| = 1$, then $x = 1$ as only the identity has order 1. Otherwise $|x| = 2$ so by definition of order, $x^2 = 1$. $\square$

Problem 1.1.17 *Let* x *be an element of* G. *Prove that if* $|x| = n$ *for some positive integer* n *then* $x^{-1} = x^{n-1}$.

Proof. Let $|x| = n$. By definition, $x^n = 1$. Hence, $x \cdot x^{n-1} = x^{n-1} \cdot x = 1$. This is precisely the definition of $x^{-1} = x^{n-1}$. $\square$

Problem 1.1.18 *Let* x *and* y *be elements of* G. *Prove that* $xy = yx$ *if and only if* $y^{-1}xy = x$ *if and only if* $x^{-1}y^{-1}xy = 1$.

Proof. Assume $x, y \in G$ and $xy = yx$. Multiplying by y^{-1} on the left, $y^{-1}xy = y^{-1}yx = x$. Now assume $y^{-1}xy = x$. Multiplying by x^{-1} on the left, $x^{-1}y^{-1}xy = x^{-1}x = 1$. Finally, assume $x^{-1}y^{-1}xy = 1$. Multipling by yx on the left, $(yx)x^{-1}y^{-1}xy = y(x \cdot x^{-1})y^{-1}xy$ [generalized associativity] $= (y \cdot y^{-1})xy = xy = 1 \cdot (yx) = yx$. $\square$

Problem 1.1.19 *Let* $x \in G$ *and let* $a, b \in \mathbb{Z}^+$.

(a) *Prove that* $x^{a+b} = x^a x^b$ *and* $(x^a)^b = x^{ab}$.

(b) *Prove that* $(x^a)^{-1} = x^{-a}$.

(c) *Establish part* (a) *for arbitrary integers* a *and* b (*positive, negative, or zero*).

Proof. Notice it is obvious $x^a = x^{a-1}x$ for all $a \in \mathbb{Z}^+$. This is because we can recursively define x^a. If $a = 0$, then $x^a = 1$. Otherwise, $x^a = x^{a-1} \cdot x$.[†] Similarly, $x^{-a} = x^{-a+1} \cdot x^{-1}$.

(a) We will induct on a and b using strong induction. First, notice $x^{1+1} = x^2 = x \cdot x$ [definition] $= x^1x^1$. Now assume $x^{n+m} = x^n x^m$ for all $m \leq n$ and $n \leq k$ for some $k \in \mathbb{Z}^+$. Then inductively we show $x^{(k+1)+m} = x^{k+1}x^m$ for all $m \leq k+1$. First, $x^{k+1} = x^k x^1$ so that $x^{k+1}x = \left(x^k x\right)x = x^k(xx) = x^k x^2$ [definition] $= x^{k+2}$. The last step follows because if $k = 1$, $x^1x^2 = xxx = x^3 = x^{1+2}$. Otherwise, we use our inductive assumption. Since $x^{k+2} = x^{(k+1)+1}$, we have shown $x^{(k+1)+1} = x^{k+1}x$. Now assume $x^{(k+1)+q} = x^{k+1}x^q$ for some $q \leq k$. Then $x^{k+1}x^{q+1} = x^{k+1}x^q x = x^{(k+1)+q}x$ [inductive assumption] $= x^{(k+1)+q+1}x = x^{(k+1)+(q+1)}$. □

Similarly, we can show $\left(x^a\right)^b = x^{ab}$. First, notice $\left(x^1\right)^1 = x^{1\cdot 1}$. Now assume $\left(x^n\right)^m = x^{nm}$ for all $m \leq n$ and $n \leq k$ for some $k \in \mathbb{Z}^+$. Then inductively we show $\left(x^{n+1}\right)^m = x^{(n+1)m}$ for all $m \leq n+1$. First, $\left(x^{n+1}\right)^1 = x^{(n+1)1}$. Now assume $\left(x^{n+1}\right)^k = x^{(n+1)k}$ for some $k \leq n$. Then $\left(x^{n+1}\right)^{k+1} = \left(x^{n+1}\right)^k\left(x^{n+1}\right)$ [part (a)] $= x^{(n+1)k}x^{(n+1)} = x^{(n+1)k+(n+1)}$ [part (a)] $= x^{(n+1)(k+1)}$. □

(b) As in part (a), we can show this inductively. First, $\left(x^1\right)^{-1} = x^{-1}$. Assume $\left(x^k\right)^{-1} = x^{-k}$. Then $x^{-(k+1)} = x^{-(k+1)+1} \cdot x^{-1} = x^{-k} \cdot x^{-1} = \left(x^k\right)^{-1}x^{-1} = \left(x \cdot x^k\right)^{-1}$ [Proposition 1.1.1(4)] $= \left(x^{k+1}\right)^{-1}$. Hence, $\left(x^a\right)^{-1} = x^{-a}$ in general. □

(c) Let a be any integer. Then $x^{a+0} = x^{0+a} = x^a = x^0x^a = x^ax^0$, and $x^{0\cdot a} = x^{a\cdot 0} = 1^a = \left(x^0\right)^a = 1^0 = \left(x^a\right)^0$. Hence, part (a) is valid when a or b is zero. Otherwise, consider when a and b are negative. Then we know $x^{-(a+b)} = x^{-a}x^{-b} = x^{-b}x^{-a}$ by part (a). Then $\left(x^{-(a+b)}\right)^{-1} = \left(x^{-b}x^{-a}\right)^{-1}$ and using part (b) and Proposition 1.1.1(4), this yields $x^{-(-(a+b))} = \left(x^{-a}\right)^{-1}\left(x^{-b}\right)^{-1} = x^{-(-a)}x^{-(-b)}$ so that $x^{a+b} = x^ax^b$. Now without loss of generality assume a is positive and b is negative. Consider $|a| \geq |b|$. Then $a = (a+b) - b$ with both parts positive. Hence, $x^ax^b = x^{(a+b)-b}x^b = x^{a+b}x^{-b}x^b = x^{a+b}$. Now assume $|a| < |b|$. Then $a = (a+b) - b$ with $-b$, $a+b$ negative, and $|-b| \geq |a+b|$, so by what we have just proved, $x^a = x^{a+b}x^{-b}$. Therefore, $x^ax^b = x^{a+b}x^{-b}x^b = x^{a+b}$. □

Problem 1.1.20 *For x an element in G show that x and x^{-1} have the same order.*

Proof. Assume $|x| = n \in \mathbb{Z}^+$. By part (b) of the previous exercise, $\left(x^{-1}\right)^n = x^{-n} = \left(x^n\right)^{-1} = 1^{-1} = 1$. All that remains to be shown is that this is the least n. Assume there is a $m \in \mathbb{Z}^+$ such that $m < n$ and $\left(x^{-1}\right)^m = 1$. Then $\left(x^m\right)^{-1} = 1$ so that $\left(\left(x^m\right)^{-1}\right)^{-1} = x^m = 1^{-1} = 1$. However, this would contradict the assumption $|x| = m$. Hence, $|x^{-1}| = n$. Now assume $|x| = \infty$. Suppose x^{-1} has finite order, n. Then $\left(x^{-1}\right)^n = \left(x^n\right)^{-1} = 1$ so again $\left(\left(x^n\right)^{-1}\right)^{-1} = x^n = \left(1^{-1}\right) = 1$. However, this would mean x has finite order, a contradiction. Therefore, $|x^{-1}| = \infty$. □

Problem 1.1.21 *Let G be a finite group and let x be an element of order n. Prove that if n is odd, then $x = \left(x^2\right)^k$ for some k.*

Proof. If $n = 1$, x is the identity so the problem is trivial. Otherwise, let $m \in \mathbb{Z}^+$ be such that $n = 2m + 1$. Then by the previous exercise, $\left(x^{-1}\right)^m = 1$ so that $\left(x^{-1}\right)^m = \left(x^{-1}\right)^{2m+1} = \left(x^{-1}\right)^{2m}x^{-1} = 1$. Multiplying by x on the right hand side, $\left(x^{-1}\right)^{2m}x^{-1}x = \left(x^{-1}\right)^{2m} = \left(x^{2m}\right)^{-1} = x$. Then $\left(\left(x^{2m}\right)^{-1}\right)^{-1} =$

[†]This is justified because $x^a = \prod_{i=1}^{a} x = \left(\prod_{i=1}^{a-1} x\right)x = x^{a-1}x$.

$x^{2m} = x^{-1}$. But by the previous exercise, $x^{2m} = (x^2)^m$. Hence, $x^{-1} = (x^2)^m$ so that $(x^{-1})^{-1} = x = \left((x^2)^{-m}\right)^{-1} = (x^2)^{-m} = (x^2)^k$ for $k = -m$. If we wish to have a positive k, let r be the least positive integer such that $rn > m$. Then $x = (x^2)^k \cdot 1^{2r} = (x^2)^k \cdot (x^n)^{2r} = (x^2)^k (x^2)^{rn} = (x^2)^{k+rn}$. □

Problem 1.1.22 *If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.*

Proof 1. First, we will show that for all $n \in \mathbb{Z}^+$, $(g^{-1}xg)^n = g^{-1}x^n g$. Inductively, when $n = 1$ we have $(g^{-1}xg)^1 = g^{-1}x^1 g$. Otherwise, assume $(g^{-1}xg)^k = g^{-1}x^k g$. Then

$$(g^{-1}xg)^{k+1} = (g^{-1}xg)^k (g^{-1}xg) = (g^{-1}x^k g)(g^{-1}xg) = g^{-1}x^k (gg^{-1})xg = g^{-1}x^k xg = g^{-1}x^{k+1}g.$$

Hence, $(g^{-1}xg)^n = g^{-1}x^n g$ for $n \in \mathbb{Z}^+$. Then if $|x| = n \in \mathbb{Z}^+$ we see $(g^{-1}xg)^n = g^{-1}x^n g = g^{-1}g = 1$. Now assume there is a $m \in \mathbb{Z}^+$ such that $m < n$ and $(g^{-1}xg)^m = 1$. Then $g^{-1}x^m g = 1$ so left and right multiplication by g and g^{-1}, respectively, yields $gg^{-1}x^m gg^{-1} = gg^{-1}$ so that $x^m = 1$. However, this contradicts the assumption $|x| = n$. Now assume that $|x| = \infty$. If $|g^{-1}xg| = n < \infty = |x|$, then

$$(g^{-1}xg)^n = g^{-1}x^n g = 1$$

so again left and right multiplication by g and g^{-1}, respectively, yields $x^n = 1$, contradicting $|x| = \infty$. Hence, $|g^{-1}xg| = |x|$ for all elements $x, g \in G$. To see the last part, let $x = ab$ and $g = b^{-1}a$. Then

$$|ab| = |(ba^{-1})(ab)(b^{-1}a)| = |ba|. \square$$

Proof 2.[†] As in Proof 1, we know $(g^{-1}xg)^n = g^{-1}x^n g$. First, we show $|g^{-1}xg| \leq |x|$. This is obvious when $|x| = \infty$. If $|x| = n$, then

$$(g^{-1}xg)^n = g^{-1}x^n g = g^{-1}g = 1,$$

so that $|g^{-1}xg| \leq |x|$ for all $x, g \in G$. To see the opposite direction, substitute $g^{-1}xg$ for x and g^{-1} for g in the previous statement:

$$\left|(g^{-1})^{-1}(g^{-1}xg)g^{-1}\right| = |x| \leq |g^{-1}xg|.$$

Thus, $|x| = |g^{-1}xg|$ for all $x, g \in G$. To see the last part of the problem, just notice $ba = a^{-1}(ab)a$ (e.g., take $x = ab$ and $g = a$). □

Problem 1.1.23 *Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s and t, prove that $|x^s| = t$.*

Proof. First, it is clear $(x^s)^t = x^{st} = x^n = 1$. Assume there is a $m \in \mathbb{Z}^+$ such that $m < t$ and $(x^s)^m = 1$. Then $x^{sm} = 1$, but $sm < st = n$, so this contradicts the fact $|x| = n$. □

Problem 1.1.24 *If a and b are commuting elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.*

Proof. Inductively, $(ab)^1 = a^1 b^1$. Assume $(ab)^k = a^k b^k$. Then $(ab)^{k+1} = (ab)^k (ab) = a^k b^k ab = \left(a^k a\right) b^k b = a^{k+1} b^{k+1}$. Notice the penultimate step is justified by commutativity of a and b. Hence, $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}^+$. When $n = 0$, $(ab)^0 = 1 = a^0 b^0$. Finally, when $n \in \mathbb{Z}^-$, we know $(ab)^{-n} = a^{-n} b^{-n}$ by

[†] This somewhat more elegant proof is due to Anssi Lahtinen from Stanford: math.stanford.edu/~lahtinen/math-120-f08/hw-solutions/math-120-sol-01.pdf

what we have just shown, but a and b commute so $(ab)^{-n} = (ba)^{-n} = b^{-n}a^{-n}$. Then $((ab)^{-n})^{-1} = (ab)^n = (b^{-n}a^{-n})^{-1} = (a^{-n})^{-1}(b^{-n})^{-1} = a^n b^n$. □

Problem 1.1.25 *Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.*

Proof 1. Let $x, y \in G$. Then $(xy)^2 = 1$ since $xy \in G$. Hence, $xyxy = 1$ so $xy = y^{-1}x^{-1}$. However, notice that $(yx)^2 = 1$ since $yx \in G$, so $yxyx = 1$ and consequently $yx = x^{-1}y^1$. Then $(xy)(yx) = y^{-1}x^{-1}x^{-1}y^{-1} = 1$. This implies $xy = x^{-1}y^{-1} = yx$. Hence, $xy = yx$ for all $x, y \in G$ and by definition G is abelian. □

Proof 2. Let $x, y \in G$. Then $(xy)^2 = xyxy = 1$. Multiplying by x on the left and y on the right and noting that $x^2 = 1$ and $y^2 = 1$, we obtain $yx = xy$. □

Problem 1.1.26 *Assume H is a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all h and $k \in H$, hk and $h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H (such a subset is called a subgroup of G).*

Proof. Closure is given. Associativity follows from the lemma at the beginning of this section's solutions. For each $h \in H$, $1_G \star h = h \star 1_G = h$. Hence, $1_H = 1_G$. Finally, for each $h \in H$, there is an $h^{-1} \in H$ (by our assumption of closure of inverses) such that $hh^{-1} = h^{-1}h = 1_G = 1_H$. Hence, H is a group under the operation. □

Problem 1.1.27 *Prove that if x is an element of the group G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup of G (called the cyclic subgroup of G generated by x).*

Proof. Call the set $H = \{x^n \mid n \in \mathbb{Z}\}$. Let $h, k \in H$. Then there are $p, q \in \mathbb{Z}$ such that $h = x^q$ and $k = x^p$. Then $hk = x^q x^p = x^{q+p}$ (exercise 19). Since $q + p \in \mathbb{Z}$, $hk \in H$ by definition. Therefore, H is closed under the operation of G. Finally, if $h^{-1} = x^{-q}$, then $hh^{-1} = x^q x^{-q} = 1$ and $h^{-1}h = x^{-q}x^q = 1$. Since $-q \in \mathbb{Z}$, $h^{-1} \in H$ by definition, so H is closed under inverses. By the previous exercise, H is a subgroup of G. □

Problem 1.1.28 *Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product. Verify all the group axioms for $A \times B$:*[+].

(a) *prove that the associative law holds: for all $(a_i, b_i) \in A \times B$, $i = 1, 2, 3$,*
$(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = [(a_1, b_1)(a_2, b_2)](a_3, b_3)$,

(b) *prove that $(1, 1)$ is the identity of $A \times B$, and*

(c) *prove that the inverse of (a, b) is (a^{-1}, b^{-1}).*

Proof. (a) Let $(a_i, b_i) \in A \times B$ with $i = 1, 2, 3$. Then

$$(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = (a_1, b_1)(a_2 \star a_3, b_2 \diamond b_3) = (a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3))$$

$$= ((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3) = (a_1 \star a_2, b_1 \diamond b_2)(a_3, b_3)$$

$$= [(a_1, b_1)(a_2, b_2)](a_3, b_3).$$

The intermediate step follows because $a_1 \star (a_2 \star a_3) = (a_1 \star a_2) \star a_3$ and $b_1 \diamond (b_2 \diamond b_3) = (b_1 \diamond b_2) \diamond b_3$ by the fact associativity holds for these elements because A and B is a group. □

(b) Let $(a, b) \in A \times B$. Then $(1, 1)(a, b) = (1 \star a, 1 \diamond b) = (a, b) = (a \star 1, b \diamond 1) = (a, b)(1, 1)$. □

(c) Let $(a,b) \in A \times B$. Then $(a,b)(a^{-1},b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (1,1) = (a^{-1} \star a, b^{-1} \diamond b) = (a^{-1},b^{-1})(a,b)$. $\square$

Problem 1.1.29 *Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.*

Proof. Assume $A \times B$ is abelian. Then for all $a_1, a_2 \in A$ and $b_1, b_2 \in B$, it is true $(a_1,b_1)(a_2,b_2) = (a_2,b_2)(a_1,b_1)$. However, $(a_1,b_1)(a_2,b_2) = (a_1a_2, b_1b_2)$ and $(a_2,b_2)(a_1,b_1) = (a_2a_1, b_2b_1)$. But then $(a_1a_2, b_1b_2) = (a_2a_1, b_2b_1)$, and the components must be equal by definition, so that $a_1a_2 = a_2a_1$ and $b_1b_2 = b_2b_1$. Hence, A and B are abelian. Now assume this. Let $(a_1,b_1),(a_2,b_2) \in A \times B$ with $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then $(a_1,b_1)(a_2,b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) = (a_2,b_2)(a_1,b_1)$. The intermediate step is justified since we assumed A and B are abelian. By definition, we now know $A \times B$ is abelian. $\square$

Problem 1.1.30 *Prove that the elements $(a,1)$ and $(1,b)$ of $A \times B$ commute and deduce the order of (a,b) is the least common multiple of $|a|$ and $|b|$.*

Proof. We see $(a,1)(1,b) = (a \cdot 1, 1 \cdot b) = (1 \cdot a, b \cdot 1) = (1,b)(a,1)$. The intermediate step is justified because $a \in A$, $b \in B$, and A and B are groups so multiplying a or b by the identity is commutative. Let $|a| = n$ and $|b| = m$. Then $(a,1)^n = (a^n, 1^n)$ (by a trivial inductive argument) and so $(a,1)^n = (1,1)$. If there were a $k \in \mathbb{Z}^+$ with $k < n$ such that $(a,1)^k = (1,1)$. then $\left(a^k, 1^k\right) = \left(a^k, 1\right) = (1,1)$ so that $a^k = 1$, contradicting the fact $|a| = n$. Hence, $|(a,1)| = n = |a|$. Similarly, $|(1,b)| = m = |b|$. Now let $\gamma = \text{lcm}(m,n)$ with $\gamma = \alpha m$ and $\gamma = \beta n$ for $\alpha, \beta \in \mathbb{Z}^+$. Then $(a,b)^\gamma = (a^\gamma, b^\gamma) = \left(a^{\alpha m}, b^{\beta n}\right) = \left((a^m)^\alpha, (b^n)^\beta\right) = \left(1^\alpha, 1^\beta\right) = (1,1)$. Now assume there is a $\delta \in \mathbb{Z}^+$ such that $\delta < \gamma$ and $(a,b)^\delta = 1$. Then $\left(a^\delta, b^\delta\right) = 1$ so that $a^\delta = b^\delta = 1$. Assume $n \nmid \delta$ so that $\delta = pn + r$ for some $p, r \in \mathbb{Z}^+ \cup \{0\}$ with $0 < r < n$. Then $a^\delta = a^{pn+r} = a^{pn}a^r = (a^n)^p a^r = 1^p a^r = a^r = 1$. However, this again contradicts the fact $|a| = n$ since $r < n$, so that $n \mid \delta$. Similarly, $m \mid \delta$. But then by definition $\delta \geq \text{lcm}(m,n) = \gamma$, a contradiction. Hence, $|a,b| = \text{lcm}(m,n)$. $\square$

Problem 1.1.31 *Prove that any finite group G of even order contains an element of order 2.*

Proof. Let $|G| = 2n$. If there was an element of order 2, say x, we would have $x^2 = 1$ so that $x = x^{-1}$. Let $H = \{g \in G \mid g \neq g^{-1}\}$. Clearly, $1 \notin H$. Furthermore, consider the following procedure. Let $H_0 = H$ and define H_{i+1} by removing some pair $\{g_i, g_i^{-1}\}$ from H_i with $g_i \in H_i$; that is $H_{i+1} = H_i \backslash \{g, g^{-1}\}$. In each iteration, we know $g \neq g^{-1}$ so that two elements are removed. Since H is finite (as G is finite), eventually $H_k = \emptyset$ for some k. But then $|H_{k-1}| = |H_k| + 2 = 2$, $|H_{k-2}| = |H_{k-1}| + 2 = 4$, etc., so that $|H_0| = |H| = 2m$ for some $m \in \mathbb{Z}^+$. Therefore, H has an even number of elements. Since $1 \notin H$, $|H| < |G|$. It is impossible that $|H| = |G| - 1$ since $|G| - 1$ is odd. Hence, $|H| < |G| - 1$. In other words, $G \backslash (H \cup \{1\}) \neq \emptyset$. But this means there is some $x \in G$ such that $x \neq 1$ with $x = x^{-1}$ ($x \notin H$ by definition). That is, $|x| = 2$. $\square$

Problem 1.1.32 *If x is an element of finite order n in G, prove that the elements $1, x, x^2, ..., x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.*

Proof. Assume $x^i = x^j$ for some $i \neq j$ ($0 \leq i, j < n$). Without loss of generality, let $i > j$. Then $x^{i-j} = 0$, but $i - j < n$, so this contradicts the fact $|x| = n$. Hence, $1, x, x^2, ..., x^{n-1}$ are all distinct. There are n of these elements, so $|G| \geq n = |x|$. $\square$

Problem 1.1.33 *Let x be an element of finite order n in G.*

(a) *Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, ..., n-1$.*

(b) *Prove that if $n = 2k$ and $1 \leq i \leq n$ then $x^i = x^{-i}$ if and only if $i = k$.*

Proof. (a) If $n = 1$ there is nothing to prove so assume $n > 1$. Assume $x^i = x^{-i}$ for some $1 \leq i \leq n-1$. Then $x^i x^i = 1$ so that $x^{2i} = 1$. Clearly, $2i \neq n$ since $2i$ is even and n is odd. If $2i \leq n$ there would thus be a contradiction (since $|x| = n > 2i$). Since $i < n$, we then know $n < 2i < 2n$ so that $0 < 2i - n < n$. However, $x^{2i} = x^{(2i-n)+n} = x^{2i-n}x^n = x^{2i-n} = 1$. In other words, we found a positive integer less than n such that x to the power of that integer is 1. But this contradicts the fact $|x| = n$. Hence, $x^i \neq x^{-i}$ for all $1 \leq i \leq n-1$. □

(b) Let $x^i = x^{-i}$ for $1 \leq i \leq n$ and assume $i \neq k$. Then $x^i x^i = 1$ so that $x^{2i} = 1$. By assumption, $2i \neq n$. If $2i \leq n$ there would thus be a contradiction (since $|x| = n > 2i$). Since $i < n$, we then know $n < 2i < 2n$ so that $0 < 2i - n < n$. However, $x^{2i} = x^{(2i-n)+n} = x^{2i-n}x^n = x^{2i-n} = 1$. In other words, we found a positive integer less than n such that x to the power of that integer is 1. But this contradicts the fact $|x| = n$. Hence, $i = k$. Now assume $i = k$. Since $1 = x^n = x^{2k} = x^k x^k$, we have $x^k = x^{-k}$, or $x^i = x^{-i}$. □

Problem 1.1.34 *If x is an element of infinite order in G, prove that the elements x^n, $n \in \mathbb{Z}$ are all distinct.*

Proof. Assume $x^i = x^j$ for some $i, j \in \mathbb{Z}$ with $i \neq j$. Then $x^{i-j} = 1$. If $i - j > 0$, this contradicts the assumption x has infinite order. If $i - j < 0$, $(x^{i-j})^{-1} = 1^{-1} = 1$ so that $x^{-(i-j)} = x^{j-i} = 1$. Then $j - i > 0$, but again this contradicts the assumption x has infinite order. Hence, $x^i \neq x^j$ for all $i, j \in \mathbb{Z}$ with $i \neq j$; that is, the elements x^n, $n \in \mathbb{Z}$ are all distinct.□.

Problem 1.1.35 *If x is an element of finite order n in G, use the Division Algorithm to show that any integral power of x equals one of the elements in the set $\{1, x, x^2, ..., x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup of G generated by x).*

Proof. Let $k \in \mathbb{Z}$. Then $k = qn + r$ for some $q \in \mathbb{Z}$, $r \in \mathbb{Z}$ with $0 \leq r < n$ by the Division Algorithm. Hence,

$$x^k = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = 1^q x^r = x^r$$

with $0 \leq r < n$ as required. □

Problem 1.1.36 *Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4. Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.*

Proof. Assume there are two group tables M_1 and M_2 with the same rows and colums both "representing" $1, a, b,$ and c, in that order (so that $g_2 = a$, $g_3 = b$, and $g_4 = c$). Now assume there is some i, j such that $M_1(x_{ij}) \neq M_2(x_{ij})$ where $M_k(x_{ij})$ is the ijth entry of group table (matrix) M_k.

Chapter 1.2

Problem 1.2.1 *Compute the order of each of the elements in the following groups:*

(a) D_6 (b) D_8 (c) D_{10}.

Solution. This problem is trivial. The solution for each group is

(a) The orders are $|1| = 1$, $|r| = 3 = |r^2| = 3$, $|s| = |sr| = |sr^2| = 2$.

(b) The orders are $|1| = 1$, $|r| = |r^3| = 4$, $|r^2| = |s| = |sr| = |sr^2| = |sr^3| = 2$.

(c) The orders are $|1| = 1$, $|r| = |r^2| = |r^3| = |r^4| = 5$, $|s| = |sr| = |sr^2| = |sr^3| = |sr^4| = 2$.

Problem 1.2.2 *Use the generators and relations $\langle r, s \,|\, r^n = s^2 = 1,\ rs = sr^{-1}\rangle$ to show that if x is any element of D_{2n}, which is not a power of r, then $rx = xr^{-1}$.*

Proof. If x is not a power of r, $x = sr^i$ for some $0 \leq i < n$. Then $rs = sr^{-1}$ so that $(rs)r^i = sr^{-1}r^i$, or in other words, $r(sr^i) = (sr^i)r^{-1}$. □

Problem 1.2.3 *Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.*

Proof. If x is not a power of r, $x = sr^i$ for some $0 \leq i < n$. But then $r^i s = r^{i-1}(rs) = r^{i-1}(sr^{-1})$ by one of the relations of D_{2n}, and applying this $i-1$ times, $r^i s = s(r^{-1})^i = sr^{-i}$, so that $r^i s = (r^i s)^{-1}$ and hence $|r^i s| = 2$. Since $s(sr) = r$, $\langle s, sr\rangle = \langle s, sr, r\rangle = \langle r, s\rangle = D_{2n}$, D_{2n} is generated by s and sr. □

Problem 1.2.5 *If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}.*

Proof. Let n be odd and greater than 1. No r^i commutes with all elements for some $1 \leq i < n$. If it did, it would particularly for s giving $r^i s = sr^i$, but our knowledge that $r^i s = sr^{-i}$ would then mean $sr^{-i} = sr^i$, or $r^i = r^{-i}$ or $r^{2i} = 1$. Since $1 \leq i < n$, we know $2 \leq 2i < 2n$ so that the former statement can only be true when $2i = n$. The fact n is odd gives a contradiction. Finally, assume sr^i commutes with all elements for some $1 \leq i < n$. But then

$$(sr^i)r = r(sr^i) \Leftrightarrow sr^{i+1} = rsr^i \Leftrightarrow s(sr^{i+1}) = s(rsr^i) \Leftrightarrow r^{i+1} = (sr)(sr^i) = (r^{-1}s)(sr^i) = r^{i-1}$$

which implies $r^{(i+1)-(i-1)} = r^2 = 1$ again giving a contradiction. □

Problem 1.2.6 *Let x and y be elements of order 2 is any group G. Prove that if $t = xy$ then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, t satisfy the same relations in G as s, r do in D_{2n}).*

Proof. The elements x and y are of order 2 so that $x^{-1} = x$ and $y^{-1} = y$. Then $t^{-1} = (xy)^{-1} = y^{-1}x^{-1} = yx$ so that $tx = (xy)x = x(yx) = xt^{-1}$. □

Problem 1.2.7 *Show that $\langle a, b \,|\, a^2 = b^2 = (ab)^n = 1\rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in Exercise 3 above.*

Proof. Notice in the usual presentation of D_{2n}, $ab = s(sr) = r$. Hence, we need to show that

$$\langle\, a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle = \langle\, ab, a \mid (ab)^n = a^2 = 1,\, (ab)a = a(ab)^{-1} \rangle$$

because the latter is the presentation of D_{2n} with $ab = r$ and $a = s$ (considered as literal strings, where the meaning of ab as "a times b" can be dropped). Notice $b = a^2b = a(ab)$. Hence, any element generated by a and b is also generated by a and ab, and conversely any element generated by ab and a is also generated by a and b.

To show the relations of the latter are implied by the former, notice we already have $(ab)^n = a^2 = 1$. To show the final relation, we need to prove $(ab)a = a(ab)^{-1}$ but by the cancellation law this amounts to $ba = (ab)^{-1}$. This is trivial since $(ab)(ba) = ab^2a = a^2 = 1$ so indeed $ba = (ab)^{-1}$. □

Problem 1.2.8 *Find the order of the cyclic subgroup of D_{2n} generated by r.*

Solution. We know $r^0(=1), r^1, r^2, ..., r^{n-1}$ are all distinct elements of D_{2n} with $r^n = 1$. Furthermore, we know if $k \in \mathbb{Z}$ then by the division algorithm $k = qn + p$ for some $q, p \in \mathbb{Z}$ with $0 \leq p < n$. Hence, $r^k = r^{qn+p} = (r^n)^q r^p = 1^q r^p = r^p$. Hence, we know any r^k is equivalent to one of the aforementioned elements. Thus, $\left\{r^k \mid k \in \mathbb{Z}\right\}$ (the cyclic subgroup of D_{2n} generated by r) has n distinct elements given by $r^0, r^1, ..., r^{n-1}$ so that by definition its order is n. □

In each of Exercises 9 to 13 you can find the order of the group of rigid motions in $\mathbb{R}^3$ of the given Platonic solid by following the proof for order of D_{2n}: find the number of positions to which an adjacent pair of vertices can be sent. Alternatively, you can find the number of places to which a given face may be sent and, once a face is fixed, the number of positions to which a vertex on that face may be sent.

Problem 1.2.9 *Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.*

Proof. A rigid motion of the tetrahedron is taking a copy of the tetrahedron, moving this copy in any fashion in 3-space, and then placing the copy back on the original n-gon so it exactly covers it. Notice this rigid motion is a symmetry (and notice we could get more symmetries by moving through 4-space, which can also be made into a group). We can describe these symmetries by choosing some labelling of the 4 vertices numerically from 1 to 4. Then each symmetry s can be described uniquely by the corresponding permutation $\sigma : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$ where if the symmetry s places vertex i in the position where vertex j was originally, then σ is the corresponding permutation sending i to j. These symmetries can be made into a group G as follows. Define st for $s, t \in G$ to be the symmetry obtained by applying t and then s to the tetrahedron. If s, t effect the permutations σ, τ respectively on the vertices, then st will effect $\sigma \circ \tau$. The binary operation of G is associative since composition of functions is associative. The identity of G is the identity symmetry (effecting the identity permutation), and the inverse of $s \in G$ is the symmetry that reverses all rigid motions of s (so that if s effects σ, s^{-1} effects σ^{-1}). This shows we can indeed make a group out of the rigid motions of a tetrahedron, just like with D_{2n}.

To show $|G| = 12$, notice for any vertex i and some adjacent vertex j, there is are 3 symmetries which send vertex 1 into position i. A particular symmetry is obtained by sending the vertex j to any of the 3 adjacent vertices to i. Hence, there are $4 \times 3 = 12$ possible such symmetries (since a tetrahedron has four vertices). These symmetries are the only symmetries of the tetrahedron, since a rigid motion in $\mathbb{R}^3$ is completely determined by where it positions three given points (apply this to the vertices i, j, and the unique vertex adjacent to these two). □

Problem 1.2.10 *Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.*

Proof. As in Problem 1.2.9, it can be verified that G is indeed a group. To show $|G| = 24$, notice for any vertex i and some adjacent vertex j, there is are 3 symmetries which send vertex 1 into position i. A

particular symmetry is obtained by sending the vertex j to any of the 3 adjacent vertices to i. Hence, there are $8 \times 3 = 24$ possible such symmetries (since a cube has eight vertices). These symmetries are the only symmetries of the cube, since a rigid motion in $\mathbb{R}^3$ is completely determined by where it positions three given points (apply this to the vertices i, j, and the unique vertex adjacent to these two). □

Problem 1.2.11 *Let G be the group of rigid motions in $\mathbb{R}^3$ of a octahedron. Show that $|G| = 24$.*

Proof. As in Problem 1.2.9, it can be verified that G is indeed a group. To show $|G| = 24$, notice for any vertex i and some adjacent vertex j, there is are 4 symmetries which send vertex 1 into position i. A particular symmetry is obtained by sending the vertex j to any of the 4 adjacent vertices to i. Hence, there are $6 \times 4 = 24$ possible such symmetries (since an octahedron has six vertices). These symmetries are the only symmetries of the octahedron, since a rigid motion in $\mathbb{R}^3$ is completely determined by where it positions three given points (apply this to the vertices i, j, and the unique vertex adjacent to these two). □

Problem 1.2.12 *Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.*

Proof. As in Problem 1.2.9, it can be verified that G is indeed a group. To show $|G| = 60$, notice for any vertex i and some adjacent vertex j, there is are 3 symmetries which send vertex 1 into position i. A particular symmetry is obtained by sending the vertex j to any of the 3 adjacent vertices to i. Hence, there are $20 \times 3 = 60$ possible such symmetries (since an octahedron has twenty vertices). These symmetries are the only symmetries of the dodecahedron, since a rigid motion in $\mathbb{R}^3$ is completely determined by where it positions three given points (apply this to the vertices i, j, and the unique vertex adjacent to these two). □

Problem 1.2.13 *Let G be the group of rigid motions in $\mathbb{R}^3$ of an icosahedron. Show that $|G| = 60$.*

Proof. As in Problem 1.2.9, it can be verified that G is indeed a group. To show $|G| = 24$, notice for any vertex i and some adjacent vertex j, there is are 5 symmetries which send vertex 1 into position i. A particular symmetry is obtained by sending the vertex j to any of the 5 adjacent vertices to i. Hence, there are $12 \times 5 = 60$ possible such symmetries (since an icosahedronhas twelve vertices). These symmetries are the only symmetries of the icosahedron, since a rigid motion in $\mathbb{R}^3$ is completely determined by where it positions three given points (apply this to the vertices i, j, and the unique vertex adjacent to these two). □

Problem 1.2.14 *Find a set of generators for $\mathbb{Z}$.*

Solution. Let the group operation be $+$ and an inverse of an element $k \in \mathbb{Z}$ be written $-k$. It suffices to consider $\{1\}$. First, notice $0 = 1 + (-1)$. Furthermore, for $-k \in \mathbb{Z}^-$,

$$-k = \underbrace{(-1) + (-1) + ... + (-1)}_{k \text{ times}},$$

and for $k \in \mathbb{Z}^+$,

$$k = \underbrace{1 + 1 + ... + 1}_{k \text{ times}}.$$

Hence, each element in $\mathbb{Z}$ can be represented as a sum of 1's and -1's (the group operation applied to 1's and its inverse). By definition, $\{1\}$ is a set of generators for $\mathbb{Z}$, that is $\mathbb{Z} = \langle 1 \rangle$. □

Problem 1.2.15 *Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.*

Solution. Let $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Then $\overline{0} = \overline{1} + \left(-\overline{1}\right)$ and we for any other element

$$\overline{a} = \underbrace{\overline{1} + ... + \overline{1}}_{a' \text{ times}}$$

where $a' \in \mathbb{Z}$ with $0 \leq a < n$ so that $\overline{a'} = \overline{a}$. Hence, $\left\{\overline{1}\right\}$ generates $\mathbb{Z}/n\mathbb{Z}$. If for $n \in \mathbb{Z}$ we define $n\overline{a}$ to be $\overline{0}$ if $n = 0$, the sum $\overline{a} + \overline{a} + ... + \overline{a}$ taken n times if n is positive, and the sum $\overline{a}^{-1} + ... + \overline{a}^{-1}$ taken $-n$ times if n is negative, then the only relation we need for $\mathbb{Z}/n\mathbb{Z}$ is $n\overline{1} = \overline{0}$. Notice $0 \cdot \overline{1}, 1 \cdot \overline{1}, ..., (n-1) \cdot \overline{1}$ must all be distinct elements so we know the order of a group with this generator and relation must be at least n. Furthermore, these elements must be the only elements of such a group. For any element $\overline{a}$, the group being generated by 1 means there is a $k \in \mathbb{Z}$ such that $\overline{a} = k\overline{1}$. By the division algorithm, there are $p, q \in \mathbb{Z}$ with $0 \leq q < n$ such that $k = pn + q$, so that $\overline{a} = (pn+q)\overline{1} = (pn)\overline{1} + q\overline{1} = p\left(n\overline{1}\right) + q\overline{1} = p \cdot \overline{0} + q\overline{1} = q\overline{1}$ where $n\overline{1} = \overline{0}$ was given by our sole relation. In other words, any element $\overline{a}$ must be one of $0 \cdot \overline{1}, 1 \cdot \overline{1}, ...,$ $(n-1) \cdot \overline{1}$. Hence, there are exactly n elements in such a group. In conclusion, the only such group is $\mathbb{Z}/n\mathbb{Z}$ so that

$$\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \,|\, n\overline{1} = \overline{0} \rangle. \square$$

Problem 1.2.16 *Show that the group $\langle\, x_1,\, y_1 \,|\, x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \,\rangle$ is the dihedral group D_4 (where x_1 may be replaced by the letter r and y_1 by s).*

Proof. Recall the usual presentation of D_{2n},

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

Then a presentation of $D_4 = D_{2\cdot 2}$ is $\langle\, r, s \,|\, r^2 = s^2 = 1,\, rs = sr^{-1} \rangle$. If we replace x_1 by r and y_1 by s, we want to show this presentation is equivalent to $\langle\, r,\, s \,|\, r^2 = s^2 = 1, (rs)^2 = 1 \rangle$. The first relation in this presentation is the same as the first in the usual presentation of D_4, so we merely need to show $(rs)^2 = 1$ implies the relation $rs = sr^{-1}$. This is clear, since $(rs)^2 = 1$ means $rsrs = 1$ so that $rsrss^{-1}r^{-1} = s^{-1}r^{-1}$ and on the left-hand side ss^{-1} cancel and then rr^{-1} cancel so we obtain $rs = s^{-1}r^{-1} = sr^{-1}$ (since $s^2 = 1$ gives $s = s^{-1}$). $\square$

Problem 1.2.17 *Let X_{2n} be the group whose presentation is displayed in (1.2).*

(a) *Show that if $n = 3k$, then X_{2n} has order 6, and it has the same generators and relations as D_6 when x is replaced by r and y by s.*

(b) *Show that if $(3, n) = 1$, then x satisfies the additional relation: $x = 1$. In this case deduce that X_{2n} has order 2.*

Proof. The presentation in question is given by

$$X_{2n} = \langle\, x, y \mid x^n = y^2 = 1,\, xy = yx^2 \rangle.$$

(a) Assume $n = 3k$. As has been shown in the discussion in the book, X_{2n} is of order at most 6 and a "hidden" relation is $x^3 = 1$. Notice because $n = 3k$ the first relation $x^n = 1$ can be replaced by $x^3 = 1$ since the former gives us no new information. Hence, $x^2 = x^{-1}$ so that $xy = yx^{-1}$. In other words, given this knowledge about n we can rewrite the presentation,

$$X_{2n} = \langle\, x, y \mid x^3 = y^2 = 1,\, xy = yx^{-1} \rangle.$$

However, notice if x and y are replaced by r and s respectively, this is exactly the canonical presentation of D_6. Therefore, a group satisfying the presentation for X_{2n} with at least 6 elements exists, and so X_{2n} must be of order exactly 6. $\square$

(b) Assume $(3, n) = 1$ so that $n = 3k + 1$ for some $k \geq 0$. Then as in part (a) we know $x^3 = 1$, so that $x^n = 1$ gives $1 = x^n = x^{3k+1} = (x^3)^k x^1 = 1^k x = x$. Hence, $x = 1$, and since any element must be of the form $y^k x^i$ with $0 \leq i \leq n - 1$ and $k = 0$ or 1. This reduces to just y^k, so X_{2n} has at most two possible elements, y and the identity. Additionally, the representation reduces to $\langle\, y \,|\, y^2 = 1 \rangle$. Notice from Problem 1.2.15, this is exactly the representation for $\mathbb{Z}/2\mathbb{Z}$ (with $y^2 = 1$ written $2 \cdot \overline{y} = 0$), so there is such a group X_{2n} with exactly 2 elements. Hence, this presentation must give a group with order 2. □

Problem 1.2.18 *Let Y be the group whose presentation is displayed in (1.3).*

(a) *Show that $v^2 = v^{-1}$.*

(b) *Show that v commutes with u^3.*

(c) *Show that v commutes with u.*

(d) *Show that $uv = 1$.*

(e) *Show that $u = 1$, deduce that $v = 1$, and conclude that $Y = 1$.*

Proof. Let Y be the group whose presentation is given by

$$Y = \langle\, u, v \mid u^4 = v^3 = 1,\ uv = v^2u^2 \,\rangle.$$

Then since $v^3 = 1$, we know $v^2v = 1$ so that $v^2 = v^{-1}$. We now show $vu^3 = u^3v$. This is equivalent to showing $v^{-1}u^3v = u^3$, or $u^3 = v^2u^3v$. This we can show because

$$v^2u^3v = (v^2u^2)(uv) = (uv)(v^2u^2) = \ uv^3u^2 = u^3.$$

Hence v commutes with u^3. Next, notice $u^9 = u^8u = (u^4)^2u = 1^2u = u$. Then

$$vu = vu^9 = \ (vu^3)u^6 = (u^3v)u^6 = u^3(vu^3)u^3 = u^3(u^3v)u^3 = u^6(vu^3) = u^6(u^3v) = u^9v = uv.$$

Hence, v also commutes with u. Then the relation $uv = v^2u^2$ implies $vuv = u^2$ so that $uv^2 = u^2$ and so $u^3v^2 = 1$, or $u^{-1}v^{-1} = 1$ (since $u^4 = 1$ implues $u^3 = u^{-1}$). Hence, $vu = uv = 1$. Then $1 = (uv)^3 = u^3v^3 = u^{-1}$ so that $u = 1$. Finally, the last relation is reduced to $v = v^2$ so that the cancellation law gives $v = 1$. Hence, the only element in this group is the identity, so it must be the trivial group; that is, $Y = 1$. □

Chapter 1.3

Problem 1.3.1 *Let σ be the permutation*

$$1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 5 \quad 4 \mapsto 2 \quad 5 \mapsto 1$$

and let τ be the permutation

$$1 \mapsto 5 \quad 2 \mapsto 3 \quad 3 \mapsto 2 \quad 4 \mapsto 4 \quad 5 \mapsto 1.$$

Find the cycle decompositions of each of the following permutations: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma,$ and $\tau^2\sigma$.

Solution. First, notice $\sigma = (1\,3\,5)(2\,4)$ and $\tau = (1\,5)(2\,3)$. Hence,

$\sigma^2 = \sigma \circ \sigma = (1\,3\,5)(2\,4) \circ (1\,3\,5)(2\,4) = (1\,5\,3)$

$\sigma\tau = \sigma \circ \tau = (1\,3\,5)(2\,4) \circ (1\,5)(2\,3) = (5\,3\,4\,2).$

$\tau\sigma = \tau \circ \sigma = (1\,5)(2\,3) \circ (1\,3\,5)(2\,4) = (1\,2\,4\,3).$

$\tau^2\sigma = \tau \circ \tau \circ \sigma = (1\,5)(2\,3) \circ (1\,5)(2\,3) \circ (1\,3\,5)(2\,4) = (1\,3\,5)(2\,4).$

Problem 1.3.2 *Let σ be the permutation*

$1 \mapsto 13 \quad 2 \mapsto 2 \quad 3 \mapsto 15 \quad 4 \mapsto 14 \quad 5 \mapsto 10 \quad 6 \mapsto 6 \quad 7 \mapsto 12 \quad 8 \mapsto 3 \quad 9 \mapsto 4 \quad 10 \mapsto 1$
$11 \mapsto 7 \quad 12 \mapsto 9 \quad 13 \mapsto 5 \quad 14 \mapsto 11 \quad 15 \mapsto 8$

and let τ be the permutation

$1 \mapsto 14 \quad 2 \mapsto 9 \quad 3 \mapsto 10 \quad 4 \mapsto 2 \quad 5 \mapsto 12 \quad 6 \mapsto 6 \quad 7 \mapsto 5 \quad 8 \mapsto 11 \quad 9 \mapsto 15 \quad 10 \mapsto 3$
$11 \mapsto 8 \quad 12 \mapsto 7 \quad 13 \mapsto 4 \quad 14 \mapsto 1 \quad 15 \mapsto 13.$

Find the cycle decomposition of the following permutations: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma,$ and $\tau^2\sigma$.

Solution. First, notice

$$\sigma = (1\,13\,5\,10)(3\,15\,8)(4\,14\,11\,7\,12\,9) \text{ and } \tau = (1\,14)(2\,9\,15\,13\,4)(3\,10)(5\,12\,7)(8\,11).$$

Hence,

$\sigma^2 = (1\,5)(3\,8\,15)(4\,11\,12)(7\,9\,14)(10\,13)$ $\qquad$ $\sigma\tau = (1\,11\,3)(2\,4)(5\,9\,8\,7\,10\,15)(13\,14)$

$\tau\sigma = (1\,4)(2\,9)(3\,13\,12\,15\,11\,5)(8\,10\,14)$ $\qquad$ $\tau^2\sigma = (1\,2\,15\,8\,3\,4\,14\,11\,12\,13\,7\,5\,10)$

Notice $\tau^2\sigma$ is one big cycle that fixes 6 and 9. □

Problem 1.3.3 *For each of the permutations whose cycle decompositions were computed in the precesing two exercises, compute its order.*

Solution. The orders can either be computer directly (a very laborious process), or a quick mental inspection which will later be proved in Problem 1.3.15 yields

$$|\sigma| = |12|, |\tau| = |30|, \ |\sigma^2| = |\sigma\tau| = |\sigma\tau| = |6|, \text{ and } |\tau^2\sigma| = 13$$

for the previous exercise and

$$|\sigma| = |\tau^2\sigma| = 6, |\tau| = 2, |\sigma^2| = |\sigma\tau| = |\tau\sigma| = 4.$$

for the first exercise. □

Problem 1.3.4 *Compute the order of each of the elements in the following groups* (a) S_3 (b) S_4 .

Solution. As in the previous problem, in S_3

$$|1| = 1, |(2\,3)| = |(1\,3)| = |(1\,3)| = 2, |(1\,2\,3)| = |(1\,3\,2)| = 3$$

and in S_4 the above permutations (the ones that fix 4) all have the same orders, and

$|(1\,4)| = |(2\,4)| = |(3\,4)| = 2,$

$|(1\,2\,4)| = |(2\,1\,4)| = |(1\,3\,4)| = |(3\,1\,4)| = |(2\,3\,4)| = |(3\,2\,4)| = 3,$

$|(1\,2\,3\,4)| = |(2\,1\,3\,4)| = |(1\,3\,2\,4)| = |(2\,3\,1\,4)| = |(3\,1\,2\,4)| = |(3\,2\,1\,4)| = 4,$ and

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

The author of the book probably intended these elements to be written the permutations to be written explicitly (e.g., define σ_i for each of the $n!$ permutations in S_n), but finding the cycle decomposition is a fairly trivial process for these elements, so they were written as such, and hence they are indeed all unique elements. Note doing this makes Problems 1.3.6 and 1.3.7 trivial.□

Problem 1.3.5 *Find the order of* $(1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6\,9)$.

Proof. As in Problem 1.3.3, $|(1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6\,9)| = 30$. □

Problem 1.3.6 *Write out the cycle decomposition of each element of order* 4 *in* S_4.

Proof. See Problem 1.3.4. □

Problem 1.3.7 *Write out the cycle decomposition of each element of order* 2 *in* S_4.

Proof. See Problem 1.3.4. □

Problem 1.3.8 *Prove that if* $\Omega = \{1, 2, 3, ...\}$ *then* S_Ω *is an infinite group* (*do not say* $\infty! = \infty$).

Proof. Consider permutations of the form $\sigma_i = (1\,i)$, that is, those for which 1 and i are exchanged and all other elements are fixed. There are an (countably) infinite such σ_i and since $\{\sigma_i\} \subseteq S_\Omega$, $|\{\sigma_i\}| \leq |S_\Omega|$ so that S_Ω is an infinite group. □

Problem 1.3.9

(a) *Let* σ *be the* 12*-cycle* $(1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12)$. *For which positive integers* i *is* σ^i *also a* 12*-cycle?*

(b) *Let* τ *be the* 8*-cycle* $(1\,2\,3\,4\,5\,6\,7\,8)$. *For which positive integers* i *is* τ^i *also an* 8*-cycle?*

(c) *Let* ω *be the* 14*-cycle* $(1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14)$. *For which positive integers* i *is* ω^i *also a* 14*-cycle?*

Proof. It is an obvious result (proved in Problem 1.3.11) that for an n-cycle σ, σ^i is an n-cycle if and only if $(n, i) = 1$. Hence, (a) for a 12-cycle, σ^i is also a 12-cycle if and only if $i \in \{1,\ 5,\ 7,\ 11\}$, (b) for an 8-cycle, σ^i is also an 8-cycle if and only if $i \in \{1,\ 3,\ 5,\ 7\}$, and (c) for a 14-cycle, σ^i is also a 14-cycle if and only if $i \in \{1,\ 3,\ 5,\ 9,\ 11,\ 13\}$. □

Problem 1.3.10 *Prove that if* σ *is the* m*-cycle* $(a_1\,a_2\,...\,a_m)$, *then for all* $i \in \{1, 2, ..., m\}$, $\sigma^i(a_k) = a_{k+i}$, *where* $k + i$ *is replaced by its least residue mod* m *when* $k + i > m$. *Deduce that* $|\sigma| = m$.

Proof. We proceed inductively. First, notice $\sigma(a_k) = a_{k+1}$ where $k+1$ is considered mod m. This is because if $k < m$, then σ assigns a_k to the element in the cycle adjacent on the right to a_k, i.e., a_{k+1}. If $k = m$, then σ assigns a_k to the first element in the cycle, i.e., $a_1 = a_{m+1} = a_{k+1}$. Now assume that $\sigma^i(a_k) = a_{k+i}$ for some $i < m$. Then $\sigma^{i+1}(a_k) = \sigma \circ \sigma^i(a_k) = \sigma(\sigma^i(a_k)) = \sigma(a_{k+i})$. Again, if $k + i < m$, then σ assigns a_{k+i} to the element in the cycle adjacent on the right to a_{k+i}, i.e., a_{k+i+1}. If $k + i = m$, then σ assigns a_{k+i} to the first element in the cycle, i.e., $a_1 = a_{m+1} = a_{k+i+1}$. Hence, $\sigma^{i+1}(a_k) = \sigma(a_{k+i}) = a_{k+(i+1)}$. Therefore, for any $i \in \{1, 2, ..., m\}$, $\sigma^i(a_k) = a_{k+i}$. Since

$$\sigma^0(a_k) = a_{k+0},\ \sigma^1(a_k) = a_{k+1},\ ...,\ \sigma^{m-1}(a_k) = a_{k+(m-1)}$$

are all distinct elements, $|\sigma| \geq m$. However, $\sigma^m(a_k) = a_{k+m} = a_k$ then implies $|\sigma| = m$. □

Problem 1.3.11 *Let σ be the m-cycle $(1\,2\,...\,m)$. Show that σ^i is also an m-cycle if and only if i is relatively prime to m.*

Proof. Assume $i \leq m$. By the previous exercise, $\sigma^i(a_k) = a_{k+i}$ and the inductive argument is easily extended to $i > m$ by recognizing a_k for $k \in \mathbb{Z}^+$ define equivalence classes on $\{a_1, ..., a_m\}$ with $a_k \equiv a_i$ for $1 \leq i \leq m$ if and only if $k \equiv i \pmod m$. Hence, $\sigma^{ni}(a_k) = a_{k+ni}$. Notice $\sigma^{ni}(a_k) = a_k$ for all a_k (i.e., σ^i is by definition an n-cycle) if and only if $k \equiv k + ni \pmod m$ for all $k \in \{1, 2, ..., m\}$ which holds if and only if $ni \equiv 0 \pmod m$. This is obvious for $i = m$ so assume $i < m$. If $(i, m) = 1$, the lowest such integer n is m since any other integer $n < m$ must satisfy $m \mid ni$ and hence also $m \mid i$ (by the fact n is relatively prime to m and so they can have no common factors), which is impossible since $i < m$. Hence σ^i is an m-cycle. The other direction follows when we show that if the lowest integer n such that $ni \equiv 0 \pmod m$ is $n = m$, then $(i, m) = 1$. Assume this hypothesis. Then if $(i, m) \neq 1$, i.e., if $\exists d > 1$ such that $d \mid i$ and $d \mid m$, this would mean that $m/d, i/d \in \mathbb{Z}$ so that $(m/d)i = m(i/d) \equiv 0 \pmod m$ would contradict that m is the lowest such integer for n (since $m/d < m$). Hence $(i, m) = 1$.

To finish the argument for $i > m$, notice by the division algorithm $i = qm + p$ for $q, p \in \mathbb{Z}$, $0 \leq p < m$. Since $\sigma^m(a_k) = a_{k+m} = a_k$, we have $\sigma^m \equiv 1$. Then

$$\sigma^i(a_k) = \sigma^{qm+p}(a_k) = \sigma^{qm}\sigma^p(a_k) = (\sigma^m)^q\sigma^p(a_k) = (1)^q\sigma^p(a_k) = \sigma^p(a_k)$$

for which we have already proven the statement. □

Problem 1.3.12

(a) *If $\tau = (1\,2)(3\,4)(5\,6)(7\,8)(9\,10)$ determine whether there is an n-cycle σ $(n \geq 10)$ with $\tau = \sigma^k$ for some integer k.*

(a) *If $\tau = (1\,2)(3\,4\,5)$ determine whether there is an n-cycle σ $(n \geq 5)$ with $\tau = \sigma^k$ for some integer k.*

Proof. (a) Yes, namely $\sigma = (1\,3\,5\,7\,9\,2\,4\,6\,8\,10)$ for $k = 5$. This can be deduced by realizing each of the elements in each 2-cycle must be $10/2 = 5$ elements apart in a 10-cycle so that they can all "reach each other" while passing over the elements in the other 2-cycles.

(b) No. We can attempt to construct such a σ. If there was such a $\sigma = (a_1\,a_2\,...\,a_n)$, then assume without loss of generality (we can cyclically permute the elements in the cycle until we get) $a_1 = 1$. If $n > 5$, then in order to fix $\{a_i \mid a_i > 5\}$ through σ^k (as τ does), we would need $n \mid k$. If this were false, take a_i to be such that $a_i = 6$, and then (decomposing k as usual with the division algorithm for $0 < r < n$)

$$\sigma^k(a_i) = \sigma^{qn+r}(a_i) = (\sigma^n)^q\sigma^r(a_i) = (1)^q\sigma^r(a_i) = \sigma^r(a_i) = a_{i+r} \neq a_i$$

so that 6 would not be fixed. However, then $n \mid k$ would imply for any $i \in \{1, ..., n\}$,

$$\sigma^k(a_i) = \sigma^{qn}(a_i) = (\sigma^n)^q(a_i) = 1^q(a_i) = a_i,$$

that is, *any* element in the n-cycle would be fixed. Hence, $n = 5$, meaning $\sigma = (1\, a_2\, a_3\, a_4\, a_5)$. However, this does not work either, since we need $\sigma^k(a_1) = \sigma^k(1) = 2 = a_i$ (for some $2 \leq i \leq 5$) and $\sigma^k(a_i) = a^k(2) = 1 = a_1$, so that $\sigma^k \circ \sigma^k(a_1) = a_1$, and hence $\sigma^{2k}(a_1) = a_{1+2k} = a_1$ meaning $1 + 2k \equiv 1 \pmod 5$, or $2k \equiv 0 \pmod 5$. However, $(2, 5) = 1$ so we would need $5 \mid k$. However, then $\sigma^k(a_1) = a_{1+k} = a_1$, contradicting our assumption $\sigma^k(a_1) = a_i$. Hence, there is no such n-cycle σ for $n \geq 5$ (and indeed, none for any n). □

Problem 1.3.13 *Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.*

Proof. Assume an element σ has order 2. If its cycle decomposition had an r-cycle $(a_1 \ldots a_r)$ for $r > 2$ we would attain a contradiction as follows. Since $\sigma^2(a_1) = a_{1+2} = a_3 \neq a_1$ (because this r-cycle has at least 3 elements), σ^2 would not fix a_1 so that by definition the order of $\sigma \neq 2$. Hence its cycle decomposition is a product of commuting 2-cycles.

Conversely, assume $\sigma = (a_1\, b_1)\ldots(a_r\, b_r)$. Then for $1 \leq i \leq r$, $\sigma^2(a_i) = \sigma(\sigma(a_i)) = \sigma(b_i) = \sigma(a_i)$ and similarly $\sigma^2(b_i) = \sigma(\sigma(b_i)) = \sigma(a_i) = b_i$ and hence $\sigma^2 \equiv 1$ so that $|\sigma| = 2$. □

Problem 1.3.14 *Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.*

Proof. Assume $\sigma \in S_n$ is a product of commuting p-cycles σ_i, $\sigma = \prod \sigma_i$. By Problem 1.3.10, notice $|\sigma_i| = p$ for each i so that $\sigma_i^p = 1$. By commutativity of the cycles,

$$\sigma^p = (\prod \sigma_i)^p = \prod \sigma_i^p = \prod 1 = 1.$$

Notice the order of $\sigma(|\sigma| = s)$ could not be less than p, because by the disjointness of the p-cycles this would imply that $\sigma_i^s = 1$ for some i with $s < p$ (in fact, for all i), which is a contradiction. Hence $|\sigma| = p$.

Conversely, let $|\sigma| = p$. Assume σ has a cycle decomposition with an r-cycle $\tau = (a_1 \ldots a_r)$ for $r \neq p$ (with $r > 1$). Then we need $\sigma^p(a_1) = \tau^p(a_1) = a_{1+p} = a_1$. This would mean $1 + p \equiv 1 \pmod r$, so that $p \equiv 0 \pmod r$. This is clearly false when $r > p$, so consider $r < p$. The condition holds when $r \mid p$, but this would imply either $r = p$ or $r = 1$, a contradiction since $1 < r < p$. Hence σ has a cycle decomposition with only p-cycles. Take the unique cycle decomposition and its p-cycles will be disjoint, so that they commute.

This need not be true when p is not prime. The element $(1\,3\,2\,4) \in S_4$ has order 2 but is a product of commuting 4-cycles. □

Problem 1.3.15 *Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.*

Proof. Assume the order of an element $\sigma \in S_n$ is smaller, with $\sigma = \prod_i \sigma_i$ for σ_i disjoint n_i-cycles. Then there is such an i so that $n_i = |\sigma_i| \nmid n := |\sigma|$ (the former equality is by Problem 1.3.10), meaning $n = qn_i + r$ for $q, r \in \mathbb{Z}$ with $0 < r < n_i$. First, notice it is necessary $\sigma_i^n = \sigma^n = \sigma_i^{n_i} = 1$ (since all elements fixed by σ^n must be fixed by σ_i^n, and also the order of σ_i is n_i). If $\sigma_i = (a_1 \ldots a_{n_i})$, then

$$\sigma_i^n(a_1) = \sigma_i^{qn_i+r}(a_1) = (\sigma_i^{n_i})^q \sigma^r(a_1) = \sigma^r(a_1) = a_{1+r} \neq a_1$$

since $0 < r < s_i$. This contradicts that $|\sigma| = s$ (since one of its cycles does not fix a_1 when applied to it s times). If $n = \text{lcm}\{n_i = |\sigma_i| : \sigma_i \text{ a } n_i\text{-cycle in the cycle decomposition of } \sigma\}$, then $n_i \mid n$ (say $n = q_i n_i$) so

$$\sigma^n = (\prod_i \sigma_i)^n = \prod_i \sigma_i^n = \prod_i \sigma_i{}^{q_i n_i} = \prod_i (\sigma_i^{n_i})^{q_i} = \prod_i (1)^{q_i} = 1.$$

Hence $|\sigma| = n$. $\square$

Problem 1.3.16 *Show that if $n \geq m$ then the number of m-cycles in S_n is given by*

$$\frac{n(n-1)(n-2)...(n-m+1)}{m}.$$

Proof. Let $\sigma = (a_1 \, ... \, a_m)$. There are n ways of choosing a_1, $n-1$ ways of choosing a_2 (since a_1 can not appear again), etc., so there are in total $n(n-1)(n-2)...(n-m+1)$ possible m-cycles. However, not all of these are unique, since cyclically permuting the elements of an m-cycle is an equivalence relation. For each m-cycle, there are m such permutations, corresponding to $a_i \mapsto a_i$, ..., $a_i \mapsto a_{i+m}$ (that is, $a_i \mapsto a_{i+k}$ means the cycle's elements are shifted to the right by k spots, leaving the same cycle but a different representation). Hence, there are in total

$$\frac{n(n-1)(n-2)...(n-m+1)}{m}$$

m-cycles in S_n. $\square$

Problem 1.3.17 *Show that if $n \geq 4$ then the number of permutations in S_n which are the product of two disjoint 2-cycles is $n(n-1)(n-2)(n-3)/8$.*

Proof. The elements in question are of the form $(a\,b)(c\,d)$. By the previous problem, there are $n(n-1)/2$ ways to form the first 2-cycle. However, now we need $c, d \in \{1, ..., n\} - \{a, b\}$ to satisfy that we have disjoint cycles. Since $|\{1, ..., n\} - \{a, b\}| = |\{1, ..., n\}| - |\{a, b\}| = n - 2$, there are $n-2$ ways of picking c, and then $n-3$ ways of picking d so that $c \neq d$. Hence, there are $(n-2)(n-3)$ ways in total. However, if $(c\,d)$ is a 2-cycle, $(d\,c)$ is equivalent to it so we divide by 2. In summary, there are:

$$\frac{n(n-1)}{2}\frac{(n-2)(n-3)}{2} = \frac{n(n-1)(n-2)(n-3)}{4}$$

different elements which are products of disjoint 2-cycles. However, when $(a\,b)(c\,d)$ is a 2-cycle, by commutativity of disjoint cycles $(a\,b)(c\,d) = (c\,d)(a\,b)$. Hence, we have to divide by 2 again to obtain the final number of *unique* products of two disjoint 2-cycles:

$$\frac{n(n-1)(n-2)(n-3)}{4}/2 = \frac{n(n-1)(n-2)(n-3)}{8}. \square$$

Problem 1.3.18 *Find all numbers n such that S_5 contains an element of order n.*

Proof. The possible cycles in S_5 are $2, 3, 4,$ and 5 cycles. Hence, unique permutations in S_5 can be written as one of these, or a product of 2- and 2- or 2- and 3-cycles (no 2- and 4-, 2- and 5-, or 4- and 5-cycles, since these would not be disjoint and hence not a valid cycle decomposition). Problem 1.3.15 gives

$$n \in \{1, 2, 3, 4, 5, \text{lcm}(2, 2), \text{lcm}(2, 3)\} = \{1, 2, 3, 4, 5, 6\}. \square$$

Problem 1.3.19 *Find all numbers n such that S_7 contains an element of order n.*

Proof. The possible cycles in S_7 are $2, 3, 4,$ 5, 6, and 7 cycles. Hence, unique permutations in S_7 can be written as one of these, or a product of 2- and 2-, 2- and 3-, 2- and 4-, 2- and 5-, 3- and 3-, 3- and 4-, cycles (none of the other products of cycles, since these could not be disjoint and hence not a valid cycle decomposition). Thus, by Problem 1.3.15,

$$n \in \{1, 2, 3, 4, 5, 6, 7, \text{lcm}(2, 2), \text{lcm}(2, 3), \text{lcm}(2, 4), \text{lcm}(2, 5), \text{lcm}(3, 3), \text{lcm}(3, 4)\} = \{1, 2, 3, 4, 5, 6, 7, 10, 12\}. \square$$

Problem 1.3.20 *Find a set of generators and relations for S_3.*

Proof. Notice a single generator would have to be of order 6. However, by Problem 1.3.15 the only way to achieve this would be to have an element have a cycle decomposition of a 2- and a 3-cycle. However, this is impossible since that would require 5 distinct elements in $\{1, 2, 3\}$, and there only are 3. Hence, S_3 is not generated by one element. Additionally, we cannot have commutative (disjoint) generators. Let $\sigma = (1\,2)$, $\tau = (1\,3)$. Then $\sigma^2 = 1$, $\tau\sigma = (1\,2\,3)$, $\sigma\tau = (1\,3\,2)$, and $\sigma\tau\sigma = (2\,3)$, so indeed the elements generate S_3. Then the relations $\sigma^2 = \tau^2 = (\sigma\tau)^3 = 1$ suffice. It's easy to see the last relation implies $(\sigma\tau)^2 = \tau\sigma$, which means $\sigma\tau \neq \tau\sigma$ and neither $\sigma\tau$ nor $\tau\sigma$ reduce to $1, \sigma,$ or τ (by examining orders). This gives us five elements, $1, \sigma, \tau, \sigma\tau, \tau\sigma$. Furthermore, notice no element can have a σ^2 or τ^2 since these would just cancel out. Hence each element has to be a "chain" of single σ's and τ's. Furthermore, $(\sigma\tau)^2 = \tau\sigma$ gives $\sigma\tau\sigma = \tau\sigma\tau$ so that any chain of σ and τ's of length greater than 3 can be reduced to a chain of length 3 or less. Hence the only chain of length 3 is $\sigma\tau\sigma$, and these are all possible elements since any others can be reduced. To verify this last one is unique, notice $(\sigma\tau\sigma)^2 = 1$, but it cannot be either of the other two elements of order 2 (σ or τ), because $(\sigma\tau\sigma)\sigma = \sigma\tau \neq 1$ and $(\sigma\tau\sigma)\tau = (\tau\sigma\tau)\tau = \tau\sigma \neq 1$. Hence, the elements $1, \sigma, \tau, \sigma\tau, \tau\sigma, \sigma\tau\sigma$ are all unique and are the only possible elements, so the group is indeed of order 6. Of course we constructed this presentation explicitly from S_3, S_3 satisfies these generators and relations:

$$S_3 = \langle\, a, b \mid a^2 = b^2 = (ab)^3 = 1 \rangle.$$

Notice omitting the last relation would give us the infinite dihedral group Dih_∞ (the group of symmetries generated by a reflection and rotation, where the rotation is not a rational multiple of a full rotation; i.e., the group of symmetries of a circle), where ab is a product of two elements of finite order (with torsion) but itself is of infinite order (torsion-free). □

Chapter 1.4

Problem 1.4.1 *Prove that* $|GL_2(\mathbb{F}_2)| = 6$.

Proof. Elements must be of the form $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with each a, b, c, d equal to 0 or 1. This matrix is invertible (in $GL_2(\mathbb{F}_2)$) if and only if $\det A = ad - bc \neq 0$. That is, we need $ad \neq bc$. Notice if $xy = 1$ if and only if $x = y = 1$ for $x, y \in \mathbb{F}_2$. Hence, if $a = 1$ and $d = 1$, then either $(c, b) = (0, 0)$, $(0, 1)$, or $(1, 0)$. On the other hand, if $(a, d) = (0, 0)$, $(0, 1)$, or $(1, 0)$ we would need $(c, d) = (1, 1)$. Hence we have six such possible (a, b, c, d), so that $|GL_2(\mathbb{F}_2)| = 6$. □

Problem 1.4.2 *Write out all the elements of* $GL_2(\mathbb{F}_2)$ *and compute the order of each element.*

Solution.

$$\left|\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right| = 1, \left|\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right| = \left|\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right| = \left|\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right| = 2, \text{ and } \left|\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right| = \left|\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right| = 3. \square$$

Problem 1.4.3 *Show that* $GL_2(\mathbb{F}_2)$ *is non-abelian.*

Proof.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \square$$

Problem 1.4.4 *Show that if* n *is not prime then* $\mathbb{Z}/n\mathbb{Z}$ *is not a field.*

Proof. Assume $n = ab$ for some $a, b \in \mathbb{Z}^+ - \{1\}$. Then $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ is not a group because the operation is not well-defined: $a \cdot b = 0 \notin (\mathbb{Z}/n\mathbb{Z})^*$. Hence it is not a field. □

Problem 1.4.5 *Show that* $GL_n(F)$ *is a finite group if and only if* F *has a finite number of elements.*

Proof. Assume $GL_n(F)$ is finite and F is not. This is a contradiction because for each $a \in F$,

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

has non-zero determinant ($= 1$), and each of these elements is distinct, so that $GL_n(F)$ would have infinite elements.

Take F to have finitely many elements, say r. Then $A \in GL_n(F)$ must be of the form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with } a, b, c, d \in F,$$

and there are hence at most r^4 distinct elements in $GL_n(F)$ (r choices for $a \times r$ choices for $b \times$ ...) . □

Problem 1.4.6 *If* $|F| = q$ *is finite prove that* $|GL_n(F)| < q^{n^2}$.

Proof. An element in $GL_n(F)$ is a matrix with n rows and n columns, with each spot in the matrix taking one of q possible values (since $|F| = q$ and the element must be in F). Hence, an upper bound for the unique number of distinct elements in $GL_n(F)$ is (taking $a_{ij} \in F$ to be the ith row and jth column):

$$\prod_{i=1}^{n}\prod_{j=1}^{n}(q \text{ choices for } a_{ij}) = q^{n^2}.$$

To show $|GL_n(F)| < q^{n^2}$ it then suffices to find one element of this form not in $GL_n(F)$, e.g.,

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \square$$

Problem 1.4.7 *Let p be a prime. Prove that the order of $GL_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$.*

Proof. As in Problem 1.4.5, $GL_2(\mathbb{F}_p)$ has at most p^4 elements (all possible matrices, invertible and non-invertible). From linear algebra, we know a matrix is invertible if and only if its rows are linearly independent. Hence, matrices of the following form are NOT invertible:

$$\begin{pmatrix} a & b \\ ca & cb \end{pmatrix} \text{ and } \begin{pmatrix} ca & cb \\ a & b \end{pmatrix} \tag{1}$$

Notice the second form of matrix can almost always be constructed by the first. For example, if we want to start with d, e in the bottom row and look at multiples of it for the first row, we could let $a = cd$ and $b = ce$ so that

$$\begin{pmatrix} cd & ce \\ d & e \end{pmatrix} = \begin{pmatrix} a & b \\ c^{-1}a & c^{-1}e \end{pmatrix}.$$

However, notice c has a multiplicative inverse if and only if $c \in \mathbb{F}_p^*$ if and only if $c \neq 0$. Hence, the second form of matrix in (1) can be expressible in the first if and only if $c \neq 0$. This gives us a classification of all non-invertible matrices in $GL_2(\mathbb{F}_p)$: elements are of the form

$$\begin{pmatrix} a & b \\ ca & cb \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 0 \\ d & e \end{pmatrix} \text{ with } a, b, c, d, e \in F \text{ and } a \text{ and } b \text{ not both } 0.$$

Now it remains to count how many possible options there are. There are $p^2 - 1$ choices for a and b (since a and b can be anything from F, except for both 0). Once a and b are fixed, there are p choices for c. Hence, the number of matrices of the first form is $(p^2 - 1)p = p^3 - p$. For the second form, there are no restrictions on d or e, so the number of choices is p^2. Hence, in total, the number of non-invertible matrices in $GL_2(\mathbb{F}_p)$ is $p^3 - p + p^2 = p^3 + p^2 - p$. Finally, a matrix is either invertible or not, so if $M_2(F)$ is the set of 2×2 matrices with entries in F,

$$|GL_2(\mathbb{F}_p)| = |M_2(\mathbb{F}_p)| - |\{A \in M_2(\mathbb{F}_p) : A \text{ not invertible}\}| = p^4 - (p^3 + p^2 - p) = p^4 - p^3 - p^2 + p. \square$$

Problem 1.4.8 *Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any F.*

Proof. A simple but not rigorous way of showing this is to consider just the outer edges of a matrix. Assume $A = (a_{ij}), B = (b_{ij}) \in GL_n(F)$. Then the top-left value for AB would be $\sum_{k=1}^{n} a_{1k}b_{k1}$ and the top-left value for BA would be $\sum_{k=1}^{n} a_{k1}b_{1k}$. These do not have to be equal, although this is not immediately obvious, since the condition that A and B have an inverse could place an important restriction on a_{ij} and b_{ij} so that these two sums are indeed equal.

To see a more specific example of this, let $0 = 1_{(F,+)}$ and $1 = 1_{(F,\cdot)}$. That is, let 0 and 1 denote the additive and multiplicative identity in F, respectively. Finally, let -1 denote the additive inverse of 1. Consider the matrix given by $A = (a_{ij})$ such that $a_{ij} = \delta_{i(n-j+1)}$, where δ is the Kronecker delta (i.e., let A

be the matrix with 1 in the bottom-left to top-right diagonal); and consider the matrix $B = (b_{ij})$ with $b_{ij} = 1 - \delta_{ij}$ except for $b_{nn} = 1$ (i.e., B is the matrix with 1's everywhere except the main diagonal, with the additional exception that the bottom-right element is 1). Then notice that $\det A = \pm 1$ (depending on n) and similarly $\det B = (-1)^{n+1}$ (the zero's in the diagonal mean the determinant is just the appropriate sign times the bottom-right element, 1). Hence $A, B \in GL_n(F)$. Finally, it's then simple to show that AB is B mirrored vertically and BA is B mirrored horizontally. These are different matrices (the former has a 1 in the lower left corner whereas the latter does not), so $GL_n(F)$ is not abelian. □

Problem 1.4.9 *Prove that the binary operation of matrix multiplication of* 2×2 *matrices with real number entries is associative.*

Proof. We can prove this in general for $n > 1$ and elements in any field F. Let $A = (a_{ij}), B = (b_{ij}), C = (c_{ij}) \in GL_n(\mathbb{R})$ with $a_{ij}, b_{ij}, c_{ij} \in F$ for $i, j \in \{1, ..., n\}$. Then component-wise:

$$(AB)C = ((a_{ij})(b_{ij}))(c_{ij}) = \left(\sum_{k=1}^{n} a_{ik}b_{kj}\right)(c_{ij}) = \left(\sum_{h=1}^{n}\left(\sum_{k=1}^{n} a_{ik}b_{kh}\right)c_{hj}\right), \text{ and}$$

$$A(BC) = (a_{ij})((b_{ij})(c_{ij})) = (a_{ij})\left(\sum_{h=1}^{n} b_{ih}c_{hj}\right) = \left(\sum_{k=1}^{n} a_{ik}\left(\sum_{h=1}^{n} b_{kh}c_{hj}\right)\right).$$

Notice these last two are equivalent, since we can rearrange terms due to the abelian nature of addition and multiplication in F (this is what gives associativity). □

Problem 1.4.10 *Let* $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R},\ a \neq 0,\ c \neq 0 \right\}$.

(a) *Compute the product of* $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ *and* $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ *to show that* G *is closed under matrix multiplication.*

(b) *Find the matrix inverse of* $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ *and deduce that* G *is closed under inverses,*

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

Solution.

(a)
$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix} \in G.$$

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

Notice the inverse is in G (since $a \neq 0, c \neq 0$ means all the entries are real) so G is closed under inverses.

(c) From Problem 1.4.9, G is associative since it is a subset of 2×2 matrices with real number entries. Additionally, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is an identity for G, so that all the group axioms are satisfied. Then G is a group, and it is a subset of $GL_2(\mathbb{R})$, so it must be a subgroup. □

The next exercise introuces the Heisenberg group over the field F and develops some of its basic properties. When $F = \mathbb{R}$ this group plays an important role in quantum mechanics and signal theory by giving a group theoretic interepretation (due to H. Weyl) of Heisenberg's Uncertainty Principle. Note also that the Heisenberg group may be defined more generally -- for example, with entries in $\mathbb{Z}$.

Problem 1.4.11 *Let* $H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$-- *called the* Heisenberg group *over* F. *Let* $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ *and* $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ *be elements of* $H(F)$.

(a) *Compute the matrix product* XY *and deduce that* $H(F)$ *is closed under matrix multiplication. Exhibit explicit matrices such that* $XY \neq YX$ (*so that* $H(F)$ *is always non-abelian*).

(b) *Find an explicit formula for the matrix inverse* X^{-1} *and deduce that* $H(F)$ *is closed under inverses.*

(c) *Prove the associative law for* $H(F)$ *and deduce that* $H(F)$ *is a group of order* $|F|^3$.

(d) *Find the order of each element of the finite group* $H(\mathbb{Z}/2\mathbb{Z})$.

(e) *Prove that every nonidentity element of the group* $H(\mathbb{R})$ *has infinite order.*

Solution. (a)

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}.$$

Since F is closed under $+$ and $\cdot$, $a+d, e+af+b, c+f \in F$ so that $XY \in H$.

(b)

$$\left(\begin{array}{ccc|ccc} 1 & a & b & 1 & 0 & 0 \\ 0 & 1 & c & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc|ccc} 1 & 0 & b-ac & 1 & -a & 0 \\ 0 & 1 & c & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -a & ac-b \\ 0 & 1 & 0 & 0 & 1 & -c \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right).$$

Hence,

$$X^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \in G$$

since $-a, ac-b, -c \in F$. Hence, $H(F)$ is closed under inverses.

(c) This follows Problem 1.4.9. However, it is possible to do it explicitly:

$$\left(\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\right)\begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & (a+d)+g & h+(a+d)i+(e+af+b) \\ 0 & 1 & (c+f)+i \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+(d+g) & (h+di+e)+a(f+i)+b \\ 0 & 1 & c+(f+i) \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d+g & h+di+e \\ 0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\left(\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}\right).$$

(d) First, notice

$$A^2 = \begin{pmatrix} 1 & 2a & ac+2b \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ and}$$

$$A^4 = \begin{pmatrix} 1 & 4a & 6ac+4b \\ 0 & 1 & 4c \\ 0 & 0 & 1 \end{pmatrix} = 1.$$

Hence each non-identity element has order between 2 and 4. If $ac = 0$ (6 possible matrices), the matrix has order 2. Otherwise, it's easily checked the cases $a, c = 1$, $b = 0$ or 1 yield a matrix of order 4.

(e) We will show inductively that

$$A^n = \begin{pmatrix} 1 & na & \frac{n(n-1)}{2}ac + nb \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}.$$

This is trivial for $n = 1$. Assume A^k has this form for some $k \geq 1$. Then

$$A^{k+1} = A^k A = \begin{pmatrix} 1 & ka & \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & ka+a & b + kac + \frac{k(k-1)}{2}ac + kb \\ 0 & 1 & kc + c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (k+1)a & \frac{k(k+1)}{2}ac + (k+1)b \\ 0 & 1 & (k+1)c \\ 0 & 0 & 1 \end{pmatrix}. \square$$

Chapter 1.5

Problem 1.5.1 *Compute the order of each of the elements in Q_8.*

Solution. The orders of 1 and -1 are 1 and 2, respectively, and everything else has order 4. □

Problem 1.5.2 *Write out the group tables for S_3, D_8 and Q_8.*

Solution.

Group table for S_3:

$(S_3, \circ)$	1	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
1	1	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,2)$	$(1\,2)$	1	$(1\,2\,3)$	$(1\,3\,2)$	$(1\,3)$	$(2\,3)$
$(1\,3)$	$(1\,3)$	$(1\,3\,2)$	1	$(1\,2\,3)$	$(2\,3)$	$(1\,2)$
$(2\,3)$	$(2\,3)$	$(1\,3\,2)$	$(1\,3\,2)$	1	$(1\,2)$	$(1\,3)$
$(1\,2\,3)$	$(1\,2\,3)$	$(2\,3)$	$(1\,2)$	$(1\,3)$	$(1\,3\,2)$	1
$(1\,3\,2)$	$(1\,3\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2)$	1	$(1\,2\,3)$

Group table for D_8:

$(D_8, \circ)$	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	1	sr^3	s	rs	rs^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	rs
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	1	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

Group table for Q_8:

$(Q_8, \cdot)$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-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

Problem 1.5.3 *Find a set of generators and relations for Q_8*

Proof. Notice we need two generators. Take x, y. We will show necessary relations are

$$x^2 = y^2 \text{ and } yxy^{-1} = x^{-1}.$$

If $x = i, y = j$, and $xy = k$, it's easy to see Q_8 is generated by and satisfies these relations. Namely, $1 = i^4$, $-1 = i^2$, $-i = i^3$, $-j = j^3$, $k = (ji)^3$ and $-k = (ij)^3$. A group of order 8 satisfying this presentation exists, so it must be of order 8 at least. [Stop reading here. Need to finish this.]

Notice $1, i, i^2, i^3$ must all be different elements. Additionally, from the third relation $(ij)^3 = j^3 i^3$ so that $(ji)^4 = 1$, and also $(ij)^2 ij = j^3 i^3$ so that $(ij)^2 = (ij) j^2 i^2 (ij)$. But this gives $j^2 i^2 = 1$, and from the first two relations $i^2 j^2 = 1$ and $i^2 = j^2$. Additionally, $j^2 i^2 = 1$ gives us how to commute i and j, namel

Hence, all powers of j greater than 1 can be expressed in i, so only j itself can be unique. To verify it is, we see $j = i^r$ for some $0 \leq r < 4$ gives a contradiction: if r were odd the fact $i^2 j^2 = 1$ would give $i^k = 1$ for a $1 < k < 4$, a contradiction; if r were even, $i^2 = j^2 = 1$ would then give a contradiction as well. Again, $ji = i^r$, $ji^2 = i^r$ or $ji^3 = i^r$ would give a similar contradiction, so that j, ji, ji^2, and ji^3 are all distinct elements. Adding any further i or j's to $1, i, i^2, i^3, j, ji, ji^2,$ or ji^3 will give use a reduction using our relations, so these are the only possible elements. Hence,

$$Q_8 = \langle i,\, j \mid i^4 = j^4 = (ij)^4 = 1 \rangle.$$

Chapter 1.6

Problem 1.6.1 *Let $\varphi : G \to H$ be a homomorphism.*

(a) *Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.*

(b) *Do part* (a) *for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.*

Proof. (a) This is a simple inductive argument. Assume $\varphi\big(x^k\big) = \varphi(x)^k$ for some $k \in \mathbb{Z}^+$. Then

$$\varphi\big(x^{k+1}\big) = \varphi\big(x^k x\big) = \varphi\big(x^k\big)\varphi(x) = \varphi(x)^k\varphi(x) = \varphi(x)^{k+1}.$$

(b) First, notice $\varphi(x^0) = \varphi(1) = \varphi(x)^0 = 1$. This is because $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$. Furthermore, $1 = \varphi(1) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$, so that $\varphi(x^{-1}) = \varphi(x)^{-1}$. Hence, for $n \in \mathbb{Z}^+$,

$$\varphi(x^{-n}) = \varphi\big((x^{-1})^n\big) = \varphi(x^{-1})^n = \big(\varphi(x)^{-1}\big)^n = \varphi(x)^{-n},$$

so that the statement holds for all $n \in \mathbb{Z}$. □

Problem 1.6.2 *If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?*

Proof. Let $|\varphi(x)| = n \in \mathbb{Z}^+$ so that $\varphi(x)^n = 1$. Of course $\varphi(1) = 1$ since

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$$

so by cancellation $\varphi(1) = 1$. Then $\varphi(x)^n = \varphi(1)$. However, $\varphi(x)^n = \varphi(x^n)$ from the previous exercise. Hence, $\varphi(x^n) = \varphi(1)$ and since isomorphisms are injective, $x^n = 1$. Assume $|x|$ was smaller, say $m < n$. But then $\varphi(x^m) = 1$ so that $\varphi(x)^m = 1$, giving $|\varphi(x)| \leq m < n$, a contradiction. Hence $|\varphi(x)| = |x|$. Let G_n and H_n be the subsets of G and H with order n. Since φ is an isomorphism, $\varphi(x) \in H_n$ is unique for each $x \in G_n$. Hence, $|G_n| = |H_n|$, that is, two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. This result is not true if φ is a homomorphism. For example, if p is prime then

$$\varphi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z},\ \big(\overline{a}, \overline{b}\big) \mapsto \overline{a}$$

is a homomorphism such that $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ has $p^2 - 1$ elements of order p whereas $\mathbb{Z}/p\mathbb{Z}$ only has $p - 1$.□

Problem 1.6.3 *If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?*

Proof. Assume G is abelian. If $a, b \in H$, there are unique $x, y \in G$ such that $a = \varphi(x)$ and $y = \varphi(b)$. Then $ab = \varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x) = ba$. Assume H is abelian. If $x, y \in G$, then $\varphi(xy) = \varphi(x)\varphi(y) = \varphi(y)\varphi(x) = \varphi(yx)$ so that $xy = yx$ by the fact φ is injective. Hence G is abelian if and only if H is. If φ is a homomorphism and G is abelian, then for $x, y \in G$, $\varphi(x)\varphi(y) = \varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x)$. Hence, for two elements $a, b \in H$, if there are $x, y \in G$ such that $a = \varphi(x)$ and $b = \varphi(y)$, then we can say the two elements commute. In other words, φ has to be surjective (but not necessarily injective). □

Problem 1.6.4 *Prove that multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.*

Proof. The group $\mathbb{R} - \{0\}$ has no elements of order 4, but $\mathbb{C} - \{0\}$ has two ($\pm i$), so by Problem 1.6.2 the groups are not isomorphic. To verify the former rigorously, notice if $x \in \mathbb{R} - \{0\}$ with finite order k, then $x^k = 1$ and $|x|^k = \left|x^k\right| = 1$ (where $|\cdot|$ denotes absolute value, not order). But then $|x| = 1$ (since the only non-negative real k-th root of unity is 1), so that either $x = 1$ which has order 1, or $x = -1$ which has order 2. □

Problem 1.6.5 *Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.*

Proof. There is no injection from $\mathbb{R}$ to $\mathbb{Q}$ since the former is uncountable and the latter is countable. This can be seen more explicitly in the following argument. Let $\varphi : \mathbb{R} \to \mathbb{Q}$ be an isomorphism. First, notice if $x \in \mathbb{R}^+$, then $0 = \varphi(0) = \varphi(-x + x) = \varphi(-x) + \varphi(x)$ so that $\varphi(x)$ and $\varphi(-x)$ are inverses in $(\mathbb{Q}, +)$. Assume $\varphi(1) = \frac{a}{b} \in \mathbb{Q}$. From the previous result, we can consider $a, b > 0$ without loss of generality. Then $\varphi(b) = b\varphi(1) = a$. Thus, $\varphi(b) = \varphi\left(a \cdot \frac{b}{a}\right) = a \cdot \varphi\left(\frac{b}{a}\right) = a \cdot 1$. Then $\varphi\left(\frac{b}{a}\right) = 1$ (otherwise we would get $a \cdot c = a$ for some $c \neq 1$ in $(\mathbb{Q}, +)$). Let $\frac{c}{d} \in \mathbb{Q}^+$ be a lowest form representation. Then $\varphi\left(\frac{cb}{a}\right) = c\varphi\left(\frac{b}{a}\right) = c$, so that $c = \varphi\left(\frac{cb}{a}\right) = \varphi\left(\frac{dbc}{ad}\right) = d\varphi\left(\frac{bc}{ad}\right)$. This implies $\varphi\left(\frac{bc}{ad}\right) = \frac{c}{d}$ (otherwise, $dx = c$ for some $x \neq \frac{c}{d}$ in $(\mathbb{Q}, +)$). From earlier, this implies $\varphi\left(-\frac{bc}{ad}\right) = -\frac{c}{d}$. This applies for any rational in $\mathbb{Q}^+$, so that φ must map all rationals to rationals ($\varphi|_{\mathbb{Q}} = \mathbb{Q}$). However, this contradicts the fact φ is injective, since any irrational in $\mathbb{R}$ must also map to a rational. □

Problem 1.6.6 *Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.*

Proof. Let $\varphi : \mathbb{Z} \to \mathbb{Q}$ be an isomorphism. First, notice if $x \in \mathbb{Z}^+$, then $0 = \varphi(-x + x) = \varphi(-x) + \varphi(x)$ so that $\varphi(x)$ and $\varphi(-x)$ are inverses in $(\mathbb{Q}, +)$. Assume $\varphi(1) = \frac{a}{b} \in \mathbb{Q}$. Then for $k \in \mathbb{Z}^+$, $\varphi(k) = \varphi(k \cdot 1) = k\varphi(1) = \frac{ak}{b}$. From earlier, $\varphi(-k) = -\frac{ak}{b}$. Hence, all elements in $\mathbb{Z}$ must be mapped to integer multiples of $\frac{a}{b}$. However, then no element will be mapped to, e.g., $\frac{a}{2b}$. This contradicts the fact φ is surjective. □

Problem 1.6.7 *Prove that D_8 and Q_8 are not isomorphic.*

Proof. The group D_8 only has two elements of order 4 (r and r^3), whereas Q_8 has six. By Problem 1.6.2, they cannot be isomorphic. □

Problem 1.6.8 *Prove that if $n \neq m$, S_n and S_m are not isomorphic.*

Proof. This is obvious, since then $n! \neq m!$ so that $|S_n| \neq |S_m|$, and there is no bijection between finite sets of different cardinality. □

Problem 1.6.9 *Prove that D_{24} and S_4 are not isomorphic.*

Proof. From Problem 1.3.4, we know S_4 has six elements of order 2, whereas D_{24} has 13 (sr^i for $0 \leq i < 12$, and s^6). By Problem 1.6.2, they cannot be isomorphic. Alternatively, notice by Problem 1.3.15 that the only possible orders of elements of S_4 are in $\{1, 2, 3, 4, \text{lcm}(2, 2)\} = \{1, 2, 3, 4\}$. However, D_{24} has an element of order 12 (namely r). □

Problem 1.6.10 *Fill in the details of the proof that the symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$ as follows: let $\theta : \Delta \to \Omega$ be a bijection. Define*

$$\varphi : S_\Delta \to S_\Omega \text{ by } \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \text{ for all } \sigma \in S_\Delta$$

and prove the following

(a) φ is well-defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω.

(b) φ is a bijection from S_Δ onto S_Ω. [Find a 2-sided inverse for φ.]

(c) φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

Note the similarity to the *change of basis* or *similarity* transformations for matrices.

Proof. (a) Notice $\theta : \Delta \to \Omega$, $\sigma : \Delta \to \Delta$, and $\theta^{-1} : \Omega \to \Delta$, so that

$$\theta \circ \sigma \circ \theta^{-1} : \Omega \to \Omega.$$

This is a definition of $\theta \circ \sigma \circ \theta^{-1}$ being a permutation of Ω, so φ is indeed well-defined.

(b) A two-sided inverse is $\varphi^{-1} = \theta \circ \sigma^{-1} \circ \theta^{-1}$:

$$\varphi \circ \varphi^{-1} = \theta \circ \sigma \circ \theta^{-1} \circ \theta \circ \sigma^{-1} \circ \theta^{-1} = \theta \circ \sigma \circ \sigma^{-1} \circ \theta^{-1} = \theta \circ \theta^{-1} = 1, \text{ and}$$

$$\varphi^{-1} \circ \varphi = \theta \circ \sigma^{-1} \circ \theta^{-1} \circ \theta \circ \sigma \circ \theta^{-1} = \theta \circ \sigma^{-1} \circ \sigma \circ \theta^{-1} = \theta \circ \theta^{-1} = 1.$$

(c) $$\varphi(\sigma \circ \tau) = \theta \circ \sigma \circ \tau \circ \theta^{-1} = \theta \circ \sigma \circ \theta^{-1} \circ \theta \circ \tau \circ \theta^{-1} = \varphi(\sigma)\varphi(\tau). \square$$

Problem 1.6.11 *Let A and B be groups. Prove that $A \times B \cong B \times A$.*

Proof. Let $(a, b) \overset{\varphi}{\mapsto} (b, a)$. If $\varphi(a, b) = \varphi(c, d)$ (with $a, c \in A$ and $b, d \in B$) then $\varphi(a, b) = (b, a)$ and $\varphi(c, d) = (d, c)$ so that $(b, a) = (d, c)$. But then $b = d$ and $a = c$, so that $(a, b) = (c, d)$. Assume $(b, a) \in B \times A$. Then $\varphi(a, b) = (b, a)$ so that φ^{-1} exists for all elements in $B \times A$. Hence, φ is a bijection. Finally, if $(a, b), (c, d) \in A \times B$, then (leaving group operations implicit)

$$\varphi((a, b)(c, d)) = \varphi(ac, bd) = (bd, ac) = (b, a)(d, c) = \varphi(a, b)\varphi(c, d). \square$$

Problem 1.6.12 *Let A, B, and C be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C$ is isomorphic to $A \times H$.*

Proof. In other words, prove $(A \times B) \times C \cong A \times (B \times C)$. Let $\varphi : (A \times B) \times C \to A \times (B \times C)$ be defined by $\varphi((a, b), c) = (a, (b, c))$. If $\varphi((a, b), c) = \varphi((d, e), f)$, then $(a, (b, c)) = (d, (e, f))$ so that $a = d$ and $(b, c) = (e, f)$ and hence $b = e$ and $c = f$. But then $((a, b), c) = ((d, e), f)$. Now take $(a, (b, c)) \in A \times H$. Then $\varphi((a, b), c) = (a, (b, c))$ so that φ^{-1} exists for all elements in $A \times H$. Finally, for $a, d \in A$, $b, e \in B$, and $c, f \in C$ (leaving group operations implicit)

$$\begin{aligned}\varphi(((a, b), c)((d, e), f)) &= \varphi((a, b)(d, e), cf) = \varphi((ad, be), cf) = (ad, (be, cf)) \\ &= (ad, (b, c)(e, f)) = (a, (b, c))(d, (e, f)) = \varphi((a, b), c)\varphi((d, e), f). \square\end{aligned}$$

Problem 1.6.13 *Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the image of φ, $\varphi(G)$, is a subgroup of H. Prove that if φ is injective then $G \cong \varphi(G)$.*

Proof. Let $x, y \in \varphi(G) \subseteq H$ with $a, b \in G$ such that $\varphi(a) = x$ and $\varphi(b) = y$. Then $\varphi(a)\varphi(b) = \varphi(ab)$, and since $ab \in G$, $\varphi(ab) \in \varphi(G)$. Similarly, $\varphi(b)\varphi(a) \in \varphi(G)$. Hence, the operation is closed in $\varphi(G)$. Furthermore, for $x \in \varphi(G)$, let $y \in G$ be such that $\varphi(y) = x$. Then $\varphi(y^{-1}) = \varphi(y)^{-1} = x^{-1} \in \varphi(G)$, so that $\varphi(G)$ is closed under inverses. Since H is a group and $\varphi(G) \subseteq H$, associativity holds. Hence $\varphi(G)$ is a subgroup of H. If φ is injective, then since $\varphi(G) = \{h \in H \mid \exists g \in G \text{ s.t. } \varphi(g) = h\}$, by definition if $h \in \varphi(G)$, then there is $g \in G$ such that $\varphi(g) = h$. Hence, φ is injective. This gives a bijective homomorphism from G to $\varphi(G)$, so that $G \cong \varphi(G)$. $\square$

Problem 1.6.14 *Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Define the* kernel *of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$. Prove that the kernel of φ is a subgroup of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.*

Proof. If $x, y \in \ker \varphi$, then $\varphi(xy) = \varphi(x)\varphi(y) = 1_H 1_H = 1_H$ so that $xy \in \ker \varphi$. Hence it is closed under the operation. Next, notice $1_H = \varphi(1_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = 1_H\varphi(x^{-1}) = \varphi(x^{-1})$ so that $x^{-1} \in \ker \varphi$. Hence it is also closed under inverses. Since $1_G \in \ker \varphi$ and associativity follows from the fact G is a group, $\ker \varphi$ is itself a group and hence a subgroup of G. If φ is injective, then there can only be one element mapped to 1_H. This must necessarily be 1_G, so that $\ker \varphi = 1 \leq G$. Conversely, if $\ker \varphi = 1$, then if $\varphi(g) = \varphi(h)$, $g \neq h$ would give a contradiction, as then $1_H = \varphi(g)\varphi(h)^{-1} = \varphi(gh^{-1})$ so that $gh^{-1} \neq 1_G$ is in $\ker \varphi$. □

Problem 1.6.15 *Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π.*

Proof. We easily see that

$$\pi((x, y) + (x', y')) = \pi((x + x', y + y')) = x + x' = \pi((x, y)) + \pi((x', y')).$$

As for the kernel,

$$\pi((x, y)) = 0 \Leftrightarrow x = 0 \Leftrightarrow \ker \pi = \{(0, y) \mid y \in \mathbb{R}\}. \square$$

Problem 1.6.16 *Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels.*

Proof. We easily see that

$$\pi_1((a, b)(a', b')) = \pi_1((aa', bb')) = aa' = \pi_1((a, b))\pi_1((a', b')), \text{ and}$$
$$\pi_2((a, b)(a', b')) = \pi_2((aa', bb')) = bb' = \pi_2((a, b))\pi_2((a', b')).$$

Additionally, it's clear that

$$\pi_1((a, b)) = 0 \Leftrightarrow a = 0 \Leftrightarrow \ker \pi_1 = \{(0, b) \mid b \in B\}, \text{ and}$$
$$\pi_2((a, b)) = 0 \Leftrightarrow b = 0 \Leftrightarrow \ker \pi_2 = \{(a, 0) \mid a \in B\}.$$

In general, $\pi_k : \prod_{i \in I} A_i \to A_k$ with $(a_1, ...) \mapsto a_k$ (for A_i groups) is a homomorphism with kernel

$$\{(0, 0, ..., \underbrace{a_k}_{k\text{th term}}, ..., 0) \mid a_k \in A_k\}. \square$$

Problem 1.6.17 *Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.*

Proof. Call the map φ. Then for $a, b \in G$, $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1}$. This equals $a^{-1}b^{-1} = \varphi(a)\varphi(b)$ if and only if $b^{-1}a^{-1} = a^{-1}b^{-1}$ if and only if $ba = ab$ (multiply by ab on the right and ba on the left). □

Problem 1.6.18 *Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.*

Proof. Call the map φ. Then for $a, b \in G$, $\varphi(ab) = (ab)^2 = abab$. This equals $a^2b^2 = \varphi(a)\varphi(b)$ if and only if $abab = a^2b^2$ if and only if $ba = ab$ (cancel the a's on the left and b's on the right). □

Problem 1.6.19 *Let $G = \{z \in \mathbb{C} \mid z^n = 1$ for some $n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but not an isomorphism.*

Proof. Call the map φ. First, notice $\varphi(z_1z_2) = (z_1z_2)^k = z_1^k z_2^k = \varphi(z_1)\varphi(z_2)$. To see it is surjective, let $z \in \mathbb{C}$. By definition, $z^n = 1$ for some $n \in \mathbb{Z}^+$ so thus $1 = (z^n)^{k/k} = \left(z^{1/k}\right)^{nk}$ so that $z^{1/k} \in G$ with $\varphi\left(z^{1/k}\right) = z$. The map is not isomorphic because if $z \neq 1$ is a k-th root of unity (from complex analysis we know such a number exists for $k > 1$), then $z^k = 1$ and $1^k = 1$. □

Problem 1.6.20 *Let G be a group and let* $\mathrm{Aut}(G)$ *be the set of all isomorphisms from G onto G. Prove that* $\mathrm{Aut}(G)$ *is a group under function composition* (*called the* automorphism group *of G and the elements of* $\mathrm{Aut}(G)$ *are called* automorphisms *of G*).

Sketch. Let $\varphi, \psi \in \mathrm{Aut}(G)$. Then $\varphi \circ \psi : G \to G$, and since composition of bijective functions is bijective, $\varphi \circ \psi \in \mathrm{Aut}(G)$ so that the set is closed. Furthermore, $1 \circ \varphi = \varphi \circ 1 = \varphi$, and the inverse function φ^{-1} is an isomorphism with the property $\varphi^{-1} \circ \varphi = \varphi \circ \varphi^{-1} = 1$. Finally, associativity follows from associativity of functional composition. □

Proof. Let $\varphi, \psi \in \mathrm{Aut}(G)$. Then $\varphi \circ \psi : G \to G$. Furthermore, for $x, y \in G$,

$$(\varphi \circ \psi)(xy) = \varphi(\psi(xy)) = \varphi(\psi(x)\psi(y)) = \varphi(\psi(x)) \cdot \varphi(\psi(y)) = (\varphi \circ \psi)(x) \cdot (\varphi \circ \psi)(y),$$

so that $\varphi \circ \psi$ is a homomorphism. Assume $(\varphi \circ \psi)(x) = (\varphi \circ \psi)(y)$, that is, $\varphi(\psi(x)) = \varphi(\psi(y))$. Injectivity of φ implies $\psi(x) = \psi(y)$, and injectivity of ψ implies $x = y$. Therefore, $\varphi \circ \psi$ is injective. Furthermore, if $z \in G$, then by surjectivity of φ, there is a $y \in G$ such that $\varphi(y) = z$. By surjectivity of ψ, there is an $x \in G$ such that $\psi(x) = y$, so that $z = \varphi(y) = \varphi(\psi(x)) = (\varphi \circ \psi)(x)$. Hence, $\varphi \circ \psi$ is surjective, and so indeed an isomorphism and thus in $\mathrm{Aut}(G)$. This proves closure.

To show there is an identity, consider $1 : G \to G$ given by $g \mapsto g$. Then for $x \in G$,

$$(\varphi \circ 1)(x) = \varphi(1(x)) = \varphi(x) \text{ and } (1 \circ \varphi)(x) = 1(\varphi(x)) = \varphi(x).$$

By definition 1 is the identity in $\mathrm{Aut}(G)$. Since φ is a bijection, it has an inverse function φ^{-1} such that $(\varphi \circ \varphi^{-1})(x) = (\varphi^{-1} \circ \varphi)(x) = x$ for all $x \in G$. This is the definition of φ^{-1} being the inverse of φ in $\mathrm{Aut}(G)$. Finally, composition of functions is associative in general, and for $\varphi, \psi, \phi \in \mathrm{Aut}(G)$ with $x \in G$,

$$((\varphi \circ \psi) \circ \phi)(x) = (\varphi \circ \psi)(\phi(x)) = \varphi(\psi(\phi(x))) = \varphi((\psi \circ \phi)(x)) = (\phi \circ (\psi \circ \phi))(x).$$

This means that $\mathrm{Aut}(G)$ satisfies all the group axioms so that it is indeed a group under function composition. □

Problem 1.6.21 *Prove that for each fixed nonzero $k \in \mathbb{Q}$ the map from $\mathbb{Q}$ to itself defined by $q \mapsto kq$ is an automorphism of $\mathbb{Q}$.*

Proof. Call the map φ. For $p, q \in \mathbb{Q}$, $\varphi(p + q) = k(p + q) = kp + kq = \varphi(p) + \varphi(q)$. To show bijectivity, notice $\varphi(p) = \varphi(q)$ means $kp = kq$ so that division gives $p = q$; if $q \in \mathbb{Q}$, then $q/k \in \mathbb{Q}$ gives $\varphi(q/k) = k(q/k) = q$ so that φ is surjective. □

Problem 1.6.22 *Let A be an abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$, prove that this homomorphism is an isomorphism.*

Proof. If $a, b \in A$, then $(ab)^k = a^k b^k$ since A is abelian (Problem 1.1.24). If $k = -1$, then if $a^{-1} = b^{-1}$, then $1 = aa^{-1} = ab^{-1} = bb^{-1}$ so that cancellation on the right by b^{-1} gives $a = b$. To show surjectivity, notice if $a \in A$, then of course $(a^{-1})^{-1} = a$. □

Problem 1.6.23 *Let G be a finite group which possesses an automorphism σ such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism σ is called* fixed point free *of order* 2).

Proof. We claim there is a bijection $x \mapsto x^{-1}\sigma(x)$. To show this map is injective, let $x^{-1}\sigma(x) = y^{-1}\sigma(y)$. Then $\sigma(x) = xy^{-1}\sigma(y)$ so that $\sigma(x)\sigma(y)^{-1} = \sigma(xy^{-1}) = xy^{-1}$. Since σ is fixed point free, $xy^{-1} = 1$, so that $y = x$. Since this is a finite map from $G \to G$ and it is injective, it must be surjective. In other words, each element $g \in G$ can be written $g = x^{-1}\sigma(x)$ for some $x \in G$.

To show that G is abelian, notice if $g = x^{-1}\sigma(x)$ for any $g \in G$, then

$$\sigma(g) = \sigma(x^{-1}\sigma(x)) = \sigma(x)^{-1}x = (x^{-1}\sigma(x))^{-1} = g^{-1},$$

and apply Problem 16.17 (which states that a group possessing the homomorphism $g \mapsto g^{-1}$ is abelian). □

Problem 1.6.24 *Let G be a finite group and let x and y be distinct elements of order 2 in G that generate G. Prove that $G \cong D_{2n}$, where $n = |xy|$.*

Proof. Let $t = xy$. Then from Problem 1.2.6, these elements give a presentation

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

Notice this is the standard presentation of D_{2n}. This is enough to guarantee isomorphism, but we can show this explicitly. Let $\varphi : D_{2n} \to G$ given by $\varphi(s^i r^j) = x^i t^j$. Then x and t in G satisfy all the relations that s and r do in D_{2n}. Hence, if $\varphi(s^i r^j) = \varphi(s^n r^m)$ with $i, n \in \{0, 1\}$, $j, m \in \{0, ..., n-1\}$, then $x^i t^j = x^n t^m$. Assume $i \neq n$. Without loss of generality, let $i = 0$ and $n = 1$. Then $t^j = xt^m$, so that $x = t^{j-m}$, which is a contradiction, since x and t satisfy the same relations in G and s and r do in D_{2n}, specifically $s \neq r^i$ for any i (respectively, $x \neq t^i$ for any i, e.g., $i = j - m$). Hence, $i = n$. But then either way (by multipling x on the left if there is no x), this means $xt^j = xt^m$. However, again, we know D_{2n} has the relation $sr^i \neq sr^j$ for $i \not\equiv j \pmod n$, which induces $xt^j \neq xt^m$ for $j \not\equiv m \pmod n$. Since $j, m \in \{0, ..., n-1\}$, we have $j = m$. Hence, $i = n$ and $j = m$, so that $s^i r^j = s^n r^m$. This shows injectivity. Surjectivity is trivial, since if $x^i t^j \in G$ (and we know every element can be written this way since G has the same relations as D_{2n}), then $\varphi(s^i r^j) = x^i t^j$. Finally, homomorphism follows from:

$$\varphi(s^i r^j s^n r^m) = \varphi(s^i s^n r^{-j} r^m) = \varphi(s^{i+n} r^{m-j}) = x^{i+n} t^{m-j} = x^i x^n t^{-j} t^m = x^i t^{-j} x^n t^m = \varphi(s^i r^j)\varphi(s^n r^m),$$

where the penultimate equality follows again from the fact x and t obey the same relations in G as s and r do in D_{2n}. □

Problem 1.6.25 *Let $n \in \mathbb{Z}^+$, let r and s be the usual generators of D_{2n} and let $\theta = 2\pi/n$.*

(a) *Prove that the matrix* $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ *is the matrix of the linear transformation which rotates the x, y plane about the origin in a counterclockwise direction by θ radians.*

(b) *Prove that the map $\varphi : D_{2n} \to GL_2(\mathbb{R})$ defined on generators by*

$$\varphi(r) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \textit{and} \quad \varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$.

(c) *Prove that the homomorphism φ in part* (b) *is injective.*

Proof. (a) Let $(x, y) \in \mathbb{R}^2$. Using polar coordinates, this point is $(r\cos\psi, r\sin\psi)$. Rotating by θ means the new point is (represented as a vector)

$$\begin{pmatrix} r\cos(\psi+\theta) \\ r\sin(\psi+\theta) \end{pmatrix} = \begin{pmatrix} r(\cos\psi\cos\theta - \sin\psi\sin\theta) \\ r(\cos\psi\sin\theta + \sin\psi\cos\theta) \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}.$$

(b) Notice that from the previous exercise, the matrix r is mapped to rotates the x, y plane by θ radians, so that applying it p times leads to a rotation by $p\theta$ radians, that is,

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^p = \begin{pmatrix} \cos p\theta & -\sin p\theta \\ \sin p\theta & \cos p\theta \end{pmatrix}$$

for all $p \in \mathbb{Z}$. This can be proved using a simple inductive argument, but we will take our intuition as evidence. Then if we let $s(j) = j$ if $n = 0$ and $-j$ if $n = 1$,

$$\begin{aligned}
\varphi(s^i r^j s^n r^m) = \varphi\big(s^{i+n} r^{s(j)+m}\big) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{i+n}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{s(j)+m} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{i}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{n}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{s(j)}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{m} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{i}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{s(j)}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{n}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{m} \\
&= \varphi(s^i r^j)\varphi(s^{nm}),
\end{aligned}$$

where the middle step is trivial if $n = 0$ (so that $s(j) = j$), and for $n = 1$,

$$\begin{aligned}
\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{n}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{s(j)} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{-j} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \cos\text{-}j\theta & -\sin\text{-}j\theta \\ \sin\text{-}j\theta & \cos\text{-}j\theta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \cos j\theta & \sin j\theta \\ -\sin j\theta & \cos j\theta \end{pmatrix} \\
&= \begin{pmatrix} -\sin j\theta & \cos j\theta \\ \cos j\theta & \sin j\theta \end{pmatrix} = \begin{pmatrix} \cos j\theta & \sin j\theta \\ \sin j\theta & \cos j\theta \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{s(j)}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{n}.
\end{aligned}$$

(c) Assume

$$\varphi(s^i r^j) = \varphi(s^n r^m), \text{ or } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{i}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{j} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{n}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^{m}$$

where $i, n \in \{0, 1\}$ and $j, m \in \{0, ..., n-1\}$. However, from the initial remark in the solution of part (b),

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{i}\begin{pmatrix} \cos j\theta & -\sin j\theta \\ \sin j\theta & \cos j\theta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{n}\begin{pmatrix} \cos m\theta & -\sin m\theta \\ \sin m\theta & \cos m\theta \end{pmatrix}. \tag{1}$$

Furthermormore, notice

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \cos p\theta & -\sin p\theta \\ \sin p\theta & \cos p\theta \end{pmatrix} = \begin{pmatrix} \sin p\theta & \cos p\theta \\ \cos p\theta & -\sin p\theta \end{pmatrix}.$$

Hence, if $i \neq n$ and assuming without loss of generality that $i = 1$ so that $n = 0$, we would need

$$\begin{cases} \cos m\theta = \sin j\theta \\ \cos j\theta = -\sin m\theta \\ \cos j\theta = \sin m\theta \\ \cos m\theta = -\sin j\theta \end{cases} \tag{2}$$

in order for the two matrices in (1) to be equal. However, $j, m \in \{0, ..., n-1\}$, so $0 \leq j\theta < 2\pi$ and $0 \leq m\theta < 2\pi$. Notice the first and last equation in (2) force $j\theta \in \{0, \pi\}$ so $m\theta \in \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$, and the second and third equation give $m\theta \in \{0, \pi\}$ and so $j\theta \in \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$. Clearly, these four equations have no solution, so that $i = n$. We may multiply by the inverse of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ if $i = n = 1$. Then

$$\begin{pmatrix} \cos j\theta & -\sin j\theta \\ \sin j\theta & \cos j\theta \end{pmatrix} = \begin{pmatrix} \cos m\theta & -\sin m\theta \\ \sin m\theta & \cos m\theta \end{pmatrix}$$

so that we have the equations $\cos j\theta = \cos m\theta$ and $\sin j\theta = \sin m\theta$. This means $j\theta \equiv m\theta \pmod{2\pi}$, but since $0 \leq j\theta < 2\pi$ and $0 \leq m\theta < 2\pi$, this means $j\theta = m\theta$ and so $j = m$.[†] Hence, $i = n$ and $j = m$ so that $s^i r^j = s^n r^m$ and the map φ is injective. □

Problem 1.6.26 *Let i and j be generators of Q_8 described as in Section 5. Prove that the map φ from Q_8 to $GL_2(\mathbb{C})$ defined on generators by*

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

extends to a homomorphism. Prove that φ is injective.

Proof. First, we need to know the values of the φ:

$$\varphi(-1) = \varphi(j^2) = \varphi(j)\varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1 \cdot 1_{GL_2(\mathbb{C})}, \text{ and}$$

$$\varphi(k) = \varphi(ij) = \varphi(i)\varphi(j) = \begin{pmatrix} \sqrt{\text{-1}} & 0 \\ 0 & -\sqrt{\text{-1}} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -\sqrt{\text{-1}} \\ -\sqrt{\text{-1}} & 0 \end{pmatrix},$$

where $\varphi(-i), \varphi(-j), \varphi(-k)$ can easily be seen to be $-\varphi(i)$, $-\varphi(j)$, and $-\varphi(k)$ seen as multiplying the scalar $-1 \in \mathbb{C}$ by each matrix (the action of $\varphi(-1)$). Then $\varphi(x \cdot \pm 1) = \varphi(x)\varphi(\pm 1) = \varphi(\pm 1 \cdot x)$ for each $x \in \{i, j, k\}$. We already know $\varphi(ij) = \varphi(i)\varphi(j)$. For all the others,

$$\varphi(ji) = \varphi(-k) = -\begin{pmatrix} 0 & -\sqrt{\text{-1}} \\ -\sqrt{\text{-1}} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \sqrt{\text{-1}} \\ \sqrt{\text{-1}} & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \sqrt{\text{-1}} & 0 \\ 0 & -\sqrt{\text{-1}} \end{pmatrix} = \varphi(j)\varphi(i),$$

[†]There also more fun ways of showing this. For example, if we let $j\theta, m\theta \in [-\pi, \pi)$ for a moment, then the injectivity of $\arcsin : [-1, 1) \to [-\pi, \pi)$ gives $j\theta = m\theta$. Then take $j\theta$ and $m\theta \pmod{2\pi}$, so that $j = m$. Alternatively, we could have noticed $\frac{d}{d\theta}(\sin j\theta) = \frac{d}{d\theta}(\sin m\theta)$ so that $j \cos j\theta = m \cos m\theta$, but since $\cos j\theta = \cos m\theta$, $j \cos j\theta = m \cos j\theta$ so that $j = m$.

$$\varphi(ki) = \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -\sqrt{\text{-1}} \\ -\sqrt{\text{-1}} & 0 \end{pmatrix} \begin{pmatrix} \sqrt{\text{-1}} & 0 \\ 0 & -\sqrt{\text{-1}} \end{pmatrix} = \varphi(k)\varphi(i),$$

$$\varphi(ik) = \varphi(-j) = -\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} \sqrt{\text{-1}} & 0 \\ 0 & -\sqrt{\text{-1}} \end{pmatrix} \begin{pmatrix} 0 & -\sqrt{\text{-1}} \\ -\sqrt{\text{-1}} & 0 \end{pmatrix} = \varphi(i)\varphi(k),$$

$$\varphi(jk) = \varphi(i) = \begin{pmatrix} \sqrt{\text{-1}} & 0 \\ 0 & -\sqrt{\text{-1}} \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -\sqrt{\text{-1}} \\ -\sqrt{\text{-1}} & 0 \end{pmatrix} = \varphi(j)\varphi(k), \text{ and}$$

$$\varphi(kj) = \varphi(-i) = -\varphi(i) = \begin{pmatrix} -\sqrt{\text{-1}} & 0 \\ 0 & \sqrt{\text{-1}} \end{pmatrix} = \begin{pmatrix} 0 & -\sqrt{\text{-1}} \\ -\sqrt{\text{-1}} & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \varphi(k)\varphi(j).$$

We can look at the matrices $\{\varphi(x) : x \in Q_8\} = \text{im } \varphi$ and see that there are no two same $\varphi(x) = \varphi(y)$ for $x \neq y$, so that φ is injective by inspection. $\square$

Chapter 1.7

Problem 1.7.1 *Let F be a field. Show that the multiplicative group of nonzero elements of F (denoted by $F^\times$) acts on the set F by $g \cdot a = ga$, where $g \in F^\times$, $a \in F$ and ga is the usual product in $F$of the two field elements (state clearly which axioms in the definition of a field are used).*

Proof. Let $g_1, g_2 \in F^\times$ and $a \in F$ (as a set). Then $g_2 \cdot a = g_2 a \in F$ where $g_2 a$ is the product in F as a field. Notice this is possible since multiplication in F as an abelian group is only defined for non-zero elements, and $g_2 \in F^\times$ implies $g_2 \neq 0$. Furthermore, then $g_1 \cdot (g_2 a) = g_1(g_2 a)$, where $g_2 a$ is taken as in F and g_1 is taken as in the group $F^\times$. Since multiplication in the field F is a group, and similarly $g_1 \neq 0$, we can say $g_1(g_2 a) = (g_1 g_2)a$ by group associativity. Hence, $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$. Finally, if $a \in F$, then for $1 \in F^\times$, $1 \cdot a = 1(a) = a$, since 1 is the multiplicative identity in the field F. This shows $F^\times$ satisfies the definition of being an action on F. □

Problem 1.7.2 *Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.*

Proof. Let $z_1, z_2 \in \mathbb{Z}$ as a group and $a \in \mathbb{Z}$ as a set. Then $z_2 \cdot a = z_2 + a$ where the sum is computed as the group operation in $(\mathbb{Z}, +)$. We then get

$$z_1 \cdot (z_2 + a) = z_1 + (z_2 + a) = (z_1 + z_2) + a = (z_1 + z_2) \cdot a$$

since addition in $\mathbb{Z}$ as a group is associative. Notice since the group operation is addition here, we showed it explicitly when writing $(z_1 + z_2) \cdot a$. Finally, $1_{\mathbb{Z}} \cdot a = 0 + a = a$. □

Note. These first two problems were trivial, but showed the care that must be taken when considering the operations being applied (e.g., even though $z + a$ was an element of the set $\mathbb{Z}$, the actual element was the group operation of $(\mathbb{Z}, +)$ applied to the elements $z, a \in (\mathbb{Z}, +)$). From now on, we will drop such pedantry and immediately become less formal by treating the operations implicitly (unless some extreme trickery is at hand!).

Problem 1.7.3 *Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.*

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

$$r \cdot (s \cdot (x, y)) = r \cdot (x + sy, y) = ((x + sy) + ry, y) = (x + (r + s)y, y) = (r + s) \cdot (x, y),$$

and $1_{(\mathbb{R},+)} \cdot (x, y) = (x + 0y, y) = (x, y)$. □

Problem 1.7.4 *Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G.*

(a) *the kernel of the action,*

(b) $\{g \in G \mid ga = a\}$ *– this subgroup is called the* stabilizer *of a in G.*

Proof. (a) Let g, g_1, g_2 be in the kernel of the action. Then $g \cdot a = g_1 \cdot a = g_2 \cdot a = a$ for all $a \in A$. First, notice that $g_1 g_2$ is also in the kernel of the action, since $(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = g_1 \cdot a = a$. Thus, the kernel is closed under the group operation. Additionally, $g^{-1} \cdot a = g^{-1} \cdot (g \cdot a) = (g^{-1} g) \cdot a = 1 \cdot a = a$, so that the kernel is closed under inverses. Hence, it is a subgroup of G.

(b) Replace "kernel [of the action]" by this set and remove "for all $a \in A$" from the proof of part (a) and this shows $\{g \in G \mid ga = a\}$ is a subgroup of G. □

Problem 1.7.5 *Prove that the kernel of an action of the group G on the set A is the same as the kernel of the corresponding permutation representation $G \to S_A$.*

Proof. Let g be in the kernel of the action. Then $ga = a \; \forall a \in A$ so the permutation representation of g is the trivial permutation $1 \in S_A$. That is, if we let $\varphi : G \to S_A$ be the map that takes elements in G to their permutation representations, $\varphi(g) = 1_{S_A}$. But this is the definition of g being in the kernel of the permutation representation (see Problem 1.6.14). Conversely, let $g \in G$ such that $\varphi(g) = 1_{S_A}$. Then $\varphi(g)(a) = a$. However, by definition $\varphi(g)(a) = g \cdot a$, which means g is in the kernel of the action. □

Problem 1.7.6 *Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.*

Proof. Assume G acts faithfully on A, that is, permutation representations are unique. Notice that for $1 \in G$ (the identity), by definition $1 \cdot a = a \, \forall a \in A$. Since G acts faithfully, this must be the *only* element in G such that $g \cdot a = a$. But this means the kernel of the action is $\{1\}$. Now assume the converse. By way of contradiction, assume $g_1 a = g_2 a = a'$ for all $a \in A$ for different g_1 and g_2 in G. But then

$$g_1^{-1}a' = g_1^{-1}(g_1 a) = (g_1^{-1}g_1)a = (1)a = a \;\text{ and }\; g_2^{-1}a' = g_2^{-1}(g_2 a) = (g_2^{-1}g_2)a = (1)a = a.$$

That is, $g_1^{-1}a' = g_2^{-1}a' = a$. However, since $\{g_1 a : a \in A\} = \{g_2 a : a \in A\}$ is a permutation on A, this means that $\{a' = g_1 a = g_2 a : a \in A\}$ is also a (indeed the same) permutation. Hence, $g_1^{-1}a' = g_2^{-1}a' = a$ for *all* $a' \in A$. However, if $g_1 \neq g_2$, then $g_1^{-1} \neq g_2^{-1}$ so that one of g_1^{-1} and g_2^{-1} is not the identity, say g_1^{-1}. But then $g_1^{-1}a' = a$ for all $a' \in A$ gives a contradiction, since we assumed the kernel of the action is $\{1\}$, and $g_1^{-1} \neq 1$ so that g_1^{-1} is not in the kernel. □

Problem 1.7.7 *Prove that in Example 2 in this section the action is faithful.*

Proof. For completeness, Example 2 is copied here below:

Example 2. *The axioms for a vector space V over a field F include the two axioms that the multiplicative group $F^\times$ act on the set V. Thus vector spaces are familiar examples of actions of multiplicative groups of fields where there is even more structure* (*in particular, V must be an abelian group*) *which can be exploited. In the special case when $V = \mathbb{R}^n$ and $F = \mathbb{R}$ the action is specified by*

$$\alpha(r_1, ..., r_n) = (\alpha r_1, ..., \alpha r_n)$$

for all $\alpha \in \mathbb{R}$, $(r_1, ..., r_n) \in \mathbb{R}^n$, where αr_i is just multiplication of two real numbers. ■

Assume that the action is not faithful. That is, there are $\alpha_1, \alpha_2 \in \mathbb{R}$ so that

$$\alpha_1(r_1, ..., r_n) = \alpha_2(r_1, ..., r_n), \text{ or } (\alpha_1 r_1, ..., \alpha_1 r_1) = (\alpha_2 r_1, ..., \alpha_2 r_n)$$

for all $(r_1, ..., r_n) \in \mathbb{R}^n$. Pick some $(r_1, ..., r_n) \neq 0$ with say $r_k \neq 0$ for some $1 \leq k \leq n$. Then comparing the k-th components, $\alpha_1 r_k = \alpha_2 r_k$, so that if we take $\frac{1}{r_k} \in \mathbb{R}$, then using the definition of an action,

$$\tfrac{1}{r_k}(\alpha_1 r_k) = \left(\tfrac{1}{r_k}\alpha_1\right) r_k = \tfrac{1}{r_k}(\alpha_2 r_k) = \left(\tfrac{1}{k}\alpha_2 r_k\right).$$

Since the elements here are computed as multiplication of two real numbers, $\left(\frac{1}{r_k}\alpha_i\right) r_k = \alpha_i$ for $i \in \{1, 2\}$ so that $\alpha_1 = \alpha_2$. By definition, this means the action must be faithful. □

Problem 1.7.8 *Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, ..., a_k\} = \{\sigma(a_1), ..., \sigma(a_k)\}$.*

(a) *Prove that this is a group action.*

(b) *Describe explicitly how the elements* $(1\,2)$ *and* $(1\,2\,3)$ *act on the six* 2*-element subsets of* $\{1,2,3,4\}$.

Proof. (a) Let $\sigma_1, \sigma_2 \in S_A$. Then for all $\{a_1, ..., a_k\} \in B$,

$$\sigma_1 \cdot (\sigma_2 \cdot \{a_1, ..., a_k\}) = \sigma_1 \cdot \{\sigma_2(a_1), ..., \sigma_2(a_k)\} = \{\sigma_1(\sigma_2(a_1)), ..., \sigma_1(\sigma_2(a_k))\}$$
$$= \{(\sigma_1\sigma_2)(a_1), ..., (\sigma_1\sigma_2)(a_k)\} = (\sigma_1\sigma_2) \cdot \{a_1, ..., a_k\}.$$

To show the second property of group actions, take any $\{a_1, ..., a_k\} \in B$; then

$$1_{S_A} \cdot \{a_1, ..., a_k\} = \{1_{S_A}(a_1), ..., 1_{S_A}(a_k)\} = \{a_1, ..., a_k\}.$$

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

$$(1\,2\,3) \cdot \{1,2\} = \{2,3\}, (1\,2\,3) \cdot \{1,3\} = \{2,1\}, (1\,2\,3) \cdot \{1,4\} = \{2,4\},$$
$$(1\,2\,3) \cdot \{2,3\} = \{3,1\}, (1\,2\,3) \cdot \{2,4\} = \{3,4\}, (1\,2\,3) \cdot \{3,4\} = \{1,4\}.$$

Notice that in general, the stabilizer (see Problem 1.7.4) of a subgroup $B \subseteq A$ acted upon by $\sigma \in S_A$ is given by $\{\sigma \in S_A : \sigma(b) = b\, \forall b \in B\}$, that is, the permutations that fix all $b \in B$. □

Problem 1.7.9 *Do both parts of the preceding exercise with "ordered* k*-tuples" in place of "*k*-element subsets," where the action on* k*-tupes is defined as above but with set braces replaced by parentheses (note that, for example, the* 2*-tuple* $(1,2)$ *and* $(2,1)$ *are different even though the sets* $\{1,2\}$ *and* $\{2,1\}$ *are the same, so the sets being acted upon are different*).

Proof. (a) Let $\sigma_1, \sigma_2 \in S_A$. Then for all $(a_1, ..., a_k) \in B$,

$$\sigma_1 \cdot (\sigma_2 \cdot (a_1, ..., a_k)) = \sigma_1 \cdot (\sigma_2(a_1), ..., \sigma_2(a_k)) = \Big(\sigma_1(\sigma_2(a_1)), ..., \sigma_1(\sigma_2(a_k))\Big)$$
$$= \Big((\sigma_1\sigma_2)(a_1), ..., (\sigma_1\sigma_2)(a_k)\Big) = (\sigma_1\sigma_2) \cdot (a_1, ..., a_k).$$

To show the second property of group actions, take any $(a_1, ..., a_k) \in B$; then

$$1_{S_A} \cdot (a_1, ..., a_k) = (1_{S_A}(a_1), ..., 1_{S_A}(a_k)) = (a_1, ..., a_k).\text{(b)}$$

(b)
$$(1\,2) \cdot (1,2) = (2,1), (1\,2) \cdot (2,1) = (1,2), (1\,2) \cdot (1,3) = (2,3), (1\,2) \cdot (3,1) = (3,2),$$
$$(1\,2) \cdot (1,4) = (2,4), (1\,2) \cdot (4,1) = (4,2), (1\,2) \cdot (2,3) = (1,3), (1\,2) \cdot (3,2) = (3,1),$$
$$(1\,2) \cdot (2,4) = (1,4),\ (1\,2) \cdot (4,2) = (4,1),\ (1\,2) \cdot (3,4) = (3,4),\ (1\,2) \cdot (4,\,3) = (4,\,3),$$
$$(1\,2) \cdot (1,\,1) = (2,\,2), (1\,2) \cdot (2,\,2) = (1,\,1), (1\,2) \cdot (3,\,3) = (3,3), (1\,2) \cdot (4,\,4) = (4,\,4).$$

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

Notice that in general, the stabilizer (see Problem 1.7.4) of a sub-tuple $B = (b_1, ..., b_k) \subseteq A$ acted upon by $\sigma \in S_A$ is given by $\{\sigma \in S_A : \sigma(b_i) = b_i\, \forall 1 \leq i \leq k\}$, that is, the permutations that fix all the components of the tuple, b_i. □

Problem 1.7.10 *With reference to the preceding two exercises determine:*

(a) *for which values of* k *the action of* S_n *on* k*-element subsets is faithful, and*

(b) *for which values of* k *the action of* S_n *on ordered* k*-tuples is faithful.*

Proof. Call the set we will be taking subsets of A. We will make use of the following lemma:

Lemma. Let $A \neq \emptyset$ and $\sigma : A \to A$ be a permutation. If σ also permutes finite subsets $B \subseteq A$ and $C \subseteq A$ (that is, for each $S \in \{B, C\}, x \in S$, we have $\sigma(x) \in S$), then σ permutes $B \cap C$.

Proof. Let σ be a permutation of A, B and C. Assume there is an $x \in B \cap C$ such that $\sigma(x) \notin B \cap C$, say $\sigma(x) \in B$ without loss of generality. This contradicts the fact σ permutes C (since that fact says $\sigma(x) \in C$). Hence, σ permutes $B \cap C$. ■

Corollary. If $A \neq \emptyset$, $\sigma : A \to A$ is a permutation, and $A_i \subseteq A$ are subsets of A, then, σ is also a permutation on $\bigcap A_i$. ■

Since A is finite, index it by $A = \{a_i\}_{i=1}^{n}$ where $n = |A|$.

(a) If $k = 0$, every permutation of $\emptyset$ is $\emptyset$, so the action is not faithful. From Problem 1.7.6, all we need to determine is the kernel of the action. If $k = 1$, then if $1 \cdot S = \sigma \cdot S = S$ for each one-element subset S of A, then $\sigma(\{a_i\}) = \{a_i\}$ for each $1 \leq i \leq n$, so that $\sigma(a_i) = a_i$ for $a_i \in A$; then by definition $\sigma = 1$. Thus, for $k = 1$ the action is faithful. Let $1 < k < n$. Assume there is a non-trivial permutation σ on A so that for each $S \in \{S \subseteq A : |S| = k\}$ it is true $1 \cdot S = \sigma \cdot S = S$. For each $1 \leq i \leq n$ and $1 \leq j \leq n$ with $i \neq j$, let $S_{ij} \subseteq A - \{a_i\}$ so that $a_j \in S_{ij}$ with $|S_{ij}| = k$. We know such a set exists for each i, j with $i \neq j$, since $|S_{ij}| = k \leq n - 1 = |A - \{a_i\}|$. The fact $k > 1$ guarantees S_{ij} is non-empty. Then we claim that

$$\mathcal{S}_j \coloneqq \bigcap_{\substack{1 \leq i \leq n \\ i \neq j}} S_{ij} = \{a_j\} \text{ for } 1 \leq j \leq n.$$

First, notice $a_j \in \mathcal{S}_j$ since by definition $a_j \in S_{ij}$ for each S_{ij}. Assume there is some other $a_r \in S_{ij}$. But $a_r \notin S_{rj}$ and since $\mathcal{S}_j \subseteq S_{rj}$, this is a contradiction. Thus, $\mathcal{S}_j = \{a_j\}$. Then apply the lemma to the subsets $S_{ij.}$ This means σ is a permutation on $\mathcal{S}_j = \{a_j\}$. Hence, $\sigma(\{a_j\}) = \{a_j\}$ and thus $\sigma(a_j) = a_j$. This holds for each $1 \leq j \leq n$, so that $\sigma = 1$. We have shown explicitly that 1 is the only permutation in the kernel of the action, so that for $1 < k < n$ the action is faithful. Finally, if $k = n$, the only n-element subset of A is A itself, and $1 \cdot A = \sigma \cdot A = A$ is true for any permutation σ, since $\sigma \cdot A = \text{im } \sigma = A$, so that the action is not faithful.

In conclusion, if $k = 0$ or $k = n$ then the action is not faithful, and otherwise ($1 < k < n$) it is faithful. This stems from the fact there are at least n k-element subsets when the latter condition holds, some of which we can intersect and apply the lemma to.

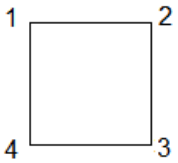
(b) If $k = 0$, every permutation of the 0-tuple is the 0-tuple, so the action is not faithful. Otherwise, again from Problem 1.7.6, we only need to determine whether the kernel of the action is just the identity. For $k > 0$, let the k-tuple T_i ($1 \leq i \leq n$) be such that each component of T_k is a_i. In other words, T_k is just the tuple $(a_i, ..., a_i)$ where a_i is written k times. Assume the action is not faithful, that is, there is a permutation σ so that $1 \cdot T = \sigma \cdot T = \sigma$ for each k-tuple T. In particular, this is true for each T_i, so that

$$\sigma \cdot (a_i, ..., a_i) = (\sigma(a_i), ..., \sigma(a_i)) = (a_i, ..., a_i),$$

and hence component-wise $\sigma(a_i) = a_i$. But we can do this for each $1 \leq i \leq n$, so $\sigma = 1$. Then the kernel of the action is just 1, so the action is faithful. Therefore, the action is faithful for all $0 < k \leq n$ and not when $k = 0$. □

Problem 1.7.11 *Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square* (*where the vertices of the square are labelled as in Section* 2).

Proof. Label the vertices as below.



Then the rotations r, r^2, r^3 correspond to the maps $(1,2,3,4) \mapsto (2,3,4,1)$, $(1,2,3,4) \mapsto (3\,,4,1,2)$, and $(1,2,3,4) \mapsto (4,1,2,3)$, respectively. Hence, the permutations corresponding to the actions by $1, r, r^2$, and r^3 are 1, $(1\,2\,3\,4)$, $(1\,3)(2\,4)$, and $(1\,4\,3\,2)$, respectively. Similarly, if we let s be the reflection with fixed points in the upper right and lower left corner (2 and 4 in the original square), we can find the permutations corresponding to the actions by $s, sr, sr^2,$ and sr^3 to be $(1\,3)$, $(1\,4)(2\,3)$, $(2\,4)$, and $(1\,2)(3\,4)$, respectively. □

Problem 1.7.12 *Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n-gon. Find the kernel of this action* (*label vertices as usual*).

Proof. Label the vertices as in Section 2 and let $n = 2m$. Then the pairs partition the set of vertices into $\{i, i+m\}$, for $1 \leq i \leq m$. Let s be the reflection that fixes the points that 1 and m are at originally. Assume sr^k is in the kernel for some $1 \leq k < n$. But, notice that then

$$sr^k \cdot \{1, m+1\} = r^{-k}s \cdot \{1, m+1\} = r^{n-k} \cdot \{1, m+1\} = \{n+1-k, n+1+m-k\},$$

where we let $n+1, n+2, ..., 2n$ be the same points as $1, 2, \ldots, n$. However, notice $n+1-k$ is not 1 or $m+1$ unless $k = n$ (i.e., $sr^k = s$) or $k = m$. In the former case, $s \cdot \{2, m+2\} = \{n-1, m\}$ so that s does not fix all vertices either. In the latter case, $sr^m \cdot \{2, m+2\} = r^{-m}s \cdot \{2, m+2\} = r^{-m} \cdot \{n-1, m\} = \{m-1, n\}$ so that sr^m does not fix all vertices either. Hence, no element of the form sr^k can be in the kernel of the action.

Now consider r^k for $1 \leq k < n$ with $k \neq m$. Then $r^k \cdot \{1, m+1\} = \{k+1, k+m+1\}$ so that these two sets are not equal unless $k = n$ (so that $r^k = 1$) or $k = m$. The former is the trivial case (the identity), so consider the latter. We have $r^m \cdot \{i, i+m\} = \{i+m, i+2m\} = \{i, i+m\}$ for each $1 \leq i \leq m$. Hence, r^k is in the kernel of the action. In conclusion, the kernel is $\{1, r^m\}$. Notice this also means the action is not faithful. □

Problem 1.7.13 *Find the kernel of the left regular action.*

Proof. Let $G \times G \to G$ be given by $g \cdot a = ga$ as group multiplication in G (for $a, g \in G$). Then the kernel of this left regular action is the set of $g \in G$ such that $ga = a$ for all $a \in G$. However, notice that for *any* $a \in G$, $ga = a$ implies by right cancellation that $g = 1$. Thus, the kernel of the left regular action is just the identity (so that it is a faithful action). □

Problem 1.7.14 *Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g, a \in G$ do* not *satisfy the axioms of a* (*left*) *group action of G on itself.*

Proof. If G is non-abelian, it has two non-commuting elements g_1, g_2. If the given map was a group action, then if we fix $a \in G$, $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (ag_2) = ag_2g_1$ should be equal to $(g_1g_2) \cdot a = ag_1g_2$. But this is saying $ag_2g_1 = ag_1g_2$ which by left cancellation implies $g_2g_1 = g_1g_2$, contradicting the fact g_1 and g_2 are non-commuting elements. □

Problem 1.7.15 *Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = ag^{-1}$ for all $g, a \in G$* do *satisfy the axioms of a* (*left*) *group action of G on itself.*

Proof. Let $g_1, g_2 \in G$. Then

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (ag_2^{-1}) = ag_2^{-1}g_1^{-1} = a(g_1g_2)^{-1} = (g_1g_2) \cdot a,$$

and if we let 1 be the identity in G, then $1 \cdot a = a(1^{-1}) = a$. □

Problem 1.7.16 *Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ for all $g, a \in G$* do *satisfy the axioms of a (left) group action (this action of G on itself is called* conjugation*).*

Proof. Let $g_1, g_2 \in G$. Then

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2ag_2^{-1}) = g_1g_2ag_2^{-1}g_1^{-1} = (g_1g_2)a(g_1g_2)^{-1} = (g_1g_2) \cdot a,$$

and if we let 1 be the identity in G, then $1 \cdot a = (1)a(1^{-1}) = a$. □

Problem 1.7.17 *Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by*

$$x \mapsto gxg^{-1}.$$

*For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself (*i.e., *is an automorphism of G). Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset A of G, $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1} \mid a \in A\}$).*

Proof. Let $x, y \in G$. Then $gxyg^{-1} = gxg^{-1}gyg^{-1} = (gxg^{-1})(gyg^{-1})$ so that conjugation is a homomorphism. Now assume $gxg^{-1} = gyg^{-1}$. Then right and left cancellation yield $x = y$. Finally, if $y \in G$, then if we conjugate $x = g^{-1}yg \in G$ we get $gxg^{-1} = g(g^{-1}yg)g^{-1} = y$. This shows conjugation is a bijection, so in conclusion it is an isomorphism from G to itself. From Problem 1.6.2, we know x and gxg^{-1} must have the same order for all x in G. Finally, if $x \in A$, then $x \in gAg^{-1}$ by definition. Conversely, if $x \in gAg^{-1}$, then by definition $x = gyg^{-1}$ for some $y \in A$ so that $y = g^{-1}xg$. But since $y \in A$, by definition $gyg^{-1} \in gAg^{-1}$; but $gyg^{-1} = g(g^{-1}xg)g^{-1} = x$. Hence, conjugation gives a bijection from A to gAg^{-1}. But since conjugation is a homomorphism on G, it must be a homomorphism on A, so that it is an isomorphism from A to gAg^{-1}. But if $A \cong gAg^{-1}$, then $|A| = |gAg^{-1}|$. □

Problem 1.7.18 *Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by*

$$a \sim b \quad \textit{if and only if} \quad a = hb \quad \textit{for some } h \in H$$

is an equivalence relation. (For each $x \in A$ the equivalence class of x under $\sim$ is called the orbit *of x under the action of H. The orbits under the action of H partition the set A).*

Proof. To show reflexivity, notice by one of the action axioms that $a = 1 \cdot a$, so that $a \sim a$. Now let $a, b \in A$ and assume $a \sim b$. Then $a = hb$ for some $h \in H$. But then $h^{-1}a = h^{-1}(hb) = (h^{-1}h)b = 1b = b$, so that $b \sim a$. Finally, assume $a, b, c \in A$ with $a \sim b$ and $b \sim c$. Then $a = hb$ for some $h \in H$ and $b = gc$ for some $g \in H$. Hence, $a = hb = h(gc) = (hg)c$ so that $a \sim c$. □

Examples. Since the book provides none, the following examples are given, intended to introduce a more intuitive understanding of the notion of an orbit.

(1) If $H = A = G$ for G a group, then for $a, b \in A$, $a = hb$ for some $h \in H$ if and only if $h = 1$. Therefore, the orbit of each element x for this action is just $\{x\}$. Call this the identity orbit. Then, for example, this implies the action given in Problems 1.7.2 induces the identity orbit on each element in $\mathbb{Z}$.

(2) The actions given in Problem 1.7.11 and 1.7.12 induce the orbit of the set itself for each element. In other words, all elements in this action are equivalent under the relation given in the previous problem (since we can "unrotate" and "unreflect" any rotation and reflection of the vertices). Additionally, if the group in

Problem 1.7.11 was taken to be the subgroup $\{1, r, r^2, r^3\} \subseteq D_8$, then the rotations of the square would be in one equivalence class (orbit), and the reflections would be in another (so that the action has two distinct orbits).

(3) If $H = (\mathbb{R}^\times, \times)$ and $A = \mathbb{R}^n$, then the orbit of $(a_1, ..., a_n) \in A$ is $\{\alpha(a_1, ..., a_n) : \alpha \in H\}$. Therefore, we can say if $n > 1$ then $A/\sim \cong \mathbb{RP}^{n-1}$(real projective space), where $\sim$ is the equivalence relation in the previous problem. □

Problem 1.7.19 *Let H be a subgroup of the finite group G and let H act on G (here $A = G$) by left multiplication. Let $x \in G$ and let $\mathcal{O}$ be the orbit of x under the action of H. Prove that the map*

$$H \to \mathcal{O} \quad \textit{defined by} \quad h \mapsto hx$$

is a bijection (hence all orbits have cardinality $|H|$). From this and the preceding exercise deduce Lagrange's Theorem:

if G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

Proof. Let $h, g \in H$. Then if $hx = gx$, right cancellation yields $h = g$. Hence the map is injective. Now assume that $y \in \mathcal{O}$. By definition of orbit there is an $h \in H$ so that $y = hx$, so that the map is also surjective. Therefore, it's a bijection. Since G is finite, H is finite, so that $|H| = |\mathcal{O}|$ for each orbit $\mathcal{O}$, since there is a bijection between them. Since the orbits partition G as a set by the previous exercise,

$$G = \bigcup_{x \in G} \mathcal{O}_x \quad \text{and the } \mathcal{O}_x \text{ are disjoint,}$$

where $\mathcal{O}_x$ is the orbit of x under the action. Hence,

$$|G| = \left| \bigcup_{x \in G} \mathcal{O}_x \right| = \sum_{x \in G} |\,\mathcal{O}_x| = n\,|\mathcal{O}| = n|H|$$

where n is the number of distinct orbits of the action and where the second equality follows from the fact the $\mathcal{O}_x$ are disjoint. Therefore, by definition $|H|$ divides $|G|$. □

For the problems below, *Geometry: Euclid and Beyond* by Robin Hartshorne is a useful very elementary further treatment on geometry.

Problem 1.7.20 *Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup of S_4.*

Proof. Denote the group by G. Earlier in the chapter, we showed that a group G acting on a set A induces a permutation $\forall g \in G$ given by $\sigma_g : A \to A$, $\sigma_g(a) = g \cdot a$, and that these permutations in turn induce a homomorphism $\varphi : G \to S_A$ given by $\varphi(g) = \sigma_g$. Now label the four vertices of the tetrahedron by $1, 2, 3$ and 4. Then if $A = \{1, 2, 3, 4\}$, we have an induced homomorphism $\varphi : G \to S_4$ given by how each rigid motion $g \in G$ permutes the vertices of the tetrahedron. By Problem 1.6.13, notice that $\varphi(G)$ is a subgroup of S_4. Moreover, since each rigid motion gives a distinct permutation of the vertices of a tetrahedron (and is completely determined by where it sends the vertices), φ is injective, so again by Problem 1.6.13, this means $G \cong \varphi(G)$. □

Problem 1.7.21 *Show that the group of rigid motions of a cube is isomorphic to S_4.*

Proof. Denote the group by G. Earlier in the chapter, we showed that a group G acting on a set A induces a permutation $\forall g \in G$ given by $\sigma_g : A \to A$, $\sigma_g(a) = g \cdot a$, and that these permutations in turn induce a homomorphism $\varphi : G \to S_A$ given by $\varphi(g) = \sigma_g$. Now label the four pairs of opposite vertices of the tetrahedron by $1, 2, 3$ and 4. Then if $A = \{1, 2, 3, 4\}$, we claim G acts on A. First, obviously the identity

rigid motion (not moving any points) preserves the vertices and hence the pairs, so that $1 \cdot i = 1$ for $1 \leq i \leq 4$. Now let $g_1, g_2 \in G$ be rigid motions. Let $i \in A$. Then if we first apply g_1 to i and then g_2 to the resulting pair, i will be mapped to the same pair as if we had applied $g_2 g_1$ (the successive motion given by first performing g_1 and then g_2). Hence, $g_2 \cdot (g_1 \cdot i) = (g_2 g_1) \cdot i$.

Since G acts on A, we have an induced homomorphism $\varphi : G \to S_4$ (as seen earlier) given by how each rigid motion $g \in G$ permutes the pairs of vertices of the tetrahedron. Since there is only one rigid motion that fixes all four pairs (namely, $1 \in G$), by Problem 1.7.6 the action of G on A is faithful, so that φ is injective. From Section 1.3 we know $|S_4| = 4! = 24$, and from Problem 1.2.10 we know $|G| = 24$, so that $|G| = |S_4|$. Then φ is also surjective (since the groups are finite), so $G \cong S_4$. □

Problem 1.7.22 *Show that the group of rigid motions of an octahedron is isomorphic to S_4.*[†] *Deduce that the groups of rigid motions of a cube and octahedron are isomorphic.*

Proof. Denote the group by G. Earlier in the chapter, we showed that a group G acting on a set A induces a permutation $\forall g \in G$ given by $\sigma_g : A \to A$, $\sigma_g(a) = g \cdot a$, and that these permutations in turn induce a homomorphism $\varphi : G \to S_A$ given by $\varphi(g) = \sigma_g$. Now label the four pairs of opposite faces of the octahedron by $1, 2, 3$ and 4. Then if $A = \{1, 2, 3, 4\}$, we claim G acts on A. First, obviously the identity rigid motion (not moving any points) preserves the vertices and hence the pairs, so that $1 \cdot i = 1$ for $1 \leq i \leq 4$. Now let $g_1, g_2 \in G$ be rigid motions. Let $i \in A$. Then if we first apply g_1 to i and then g_2 to the resulting pair, i will be mapped to the same pair as if we had applied $g_2 g_1$ (the successive motion given by first performing g_1 and then g_2). Hence, $g_2 \cdot (g_1 \cdot i) = (g_2 g_1) \cdot i$.

Since G acts on A, we have an induced homomorphism $\varphi : G \to S_4$ (as seen earlier) given by how each rigid motion $g \in G$ permutes the pairs of faces of the octahedron. Since there is only one rigid motion that fixes all four faces (namely, $1 \in G$), by Problem 1.7.6 the action of G on A is faithful, so that φ is injective. From Section 1.3 we know $|S_4| = 4! = 24$, and from Problem 1.2.11 we know $|G| = 24$, so that $|G| = |S_4|$. Then φ is also surjective (since the groups are finite), so $G \cong S_4$. By the previous exercise, the group of rigid motions of a cube is also isomorphic to S_4, and hence to the group of rigid motions of an octahedron. □

Problem 1.7.23 *Explain why the action of the group of rigid motions on the set of three pairs of opposite faces is not faithful. Find the kernel of this action.*

Proof. Last problem...will finish in a bit.

[†] The authors write "to a subgroup of S_4" and not "to S_4", but see the errata: www.emba.uvm.edu/~foote/errata_3rd_edition.pdf.