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

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

since $2 \not| \, bd$; 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 $G = \{x \in \mathbb{R} \,|\, 0 \leq x < 1\}$ 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* $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

(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 $g_i g_j = g_j g_i$. The j, i entry in its group table is the group element $g_j g_i = g_i g_j$. 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, $g_i g_j = g_j g_i$. However, this holds for any two elements $g_i, g_j \in G$ so that $g_i g_j = g_j g_i$ for all elements of G. This is precisely the definition of an abelian group. $\square$

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

Solution. The group is $\mathbb{Z}/12\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{11}\}$. 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. $\square$

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] $= x^1 x^1$. 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 $x^{k+1}x = \big(x^k x\big)x = x^k(xx) = x^k x^2$ [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] $= x^{(k+1)+q+1}x = x^{(k+1)+(q+1)}$. $\square$

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

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

(c) Let a be any integer. Then $x^{a+0} = x^{0+a} = x^a = x^0 x^a = x^a x^0$, and $x^{0 \cdot a} = x^{a \cdot 0} = 1^a = (x^0)^a = 1^0 = (x^a)^0$. 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 $\big(x^{-(a+b)}\big)^{-1} = \big(x^{-b}x^{-a}\big)^{-1}$ and using part (b) and Proposition 1.1.1(4), this yields $x^{-(-(a+b))} = (x^{-a})^{-1}\big(x^{-b}\big)^{-1} = x^{-(-a)}x^{-(-b)}$ so that $x^{a+b} = x^a x^b$. 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, $x^a x^b = x^{(a+b)-b}x^b = x^{a+b}x^{-b}x^b = x^{a+b}$. 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, $x^a x^b = x^{a+b}x^{-b}x^b = x^{a+b}$. $\square$

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, $(x^{-1})^n = x^{-n} = (x^n)^{-1} = 1^{-1} = 1$. 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 $(x^{-1})^m = 1$. Then $(x^m)^{-1} = 1$ so that $\big((x^m)^{-1}\big)^{-1} = x^m = 1^{-1} = 1$. However, this would contradict the assumption $|x| = m$. Hence, $|x^{-1}| = n$. Now assume $|x| = \infty$. Suppose x^{-1} has finite order, n. Then

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

$(x^{-1})^n = (x^n)^{-1} = 1$ so again $\left((x^n)^{-1}\right)^{-1} = x^n = (1^{-1}) = 1$. 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 $x = (x^2)^k$ 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, $(x^{-1})^m = 1$ so that $(x^{-1})^m = (x^{-1})^{2m+1} = (x^{-1})^{2m}x^{-1} = 1$. Multiplying by x on the right hand side, $(x^{-1})^{2m}x^{-1}x = (x^{-1})^{2m} = (x^{2m})^{-1} = x$. Then $\left((x^{2m})^{-1}\right)^{-1} = x^{2m} = x^{-1}$. 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. First, we will show $(g^{-1}xg)^n = g^{-1}x^n g$. 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 $(g^{-1}xg)^{k+1} = (g^{-1}xg)^k(g^{-1}xg) = \left(g^{-1}x^k g\right) \cdot (g^{-1}xg) = g^{-1}x^k(gg^{-1})xg = g^{-1}x^k xg = g^{-1}x^{k+1}g$. Hence, $(g^{-1}xg)^n = g^{-1}x^n g$. 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 $|x| = n$. Hence, $|g^{-1}xg| = n = |x|$. Let $x = ab$ and $g = b^{-1}a$. Then $|ab| = |(ba^{-1})(ab)(b^{-1}a)| = |ba|$. □

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 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. 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. □

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

$$\begin{aligned}(a_1, b_1)[(a_2, b_2)(a_3, b_3)] &= (a_1, b_1)(a_2 \star a_3, b_2 \diamond b_3) = (a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3)) \\ &= ((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3) = (a_1 \star a_2, b_1 \diamond b_2)(a_3, b_3) \\ &= [(a_1, b_1)(a_2, b_2)](a_3, b_3).\end{aligned}$$

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 $(a, b)(a^{-1}, b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (1, 1) = (a^{-1} \star a, b^{-1} \diamond b) = (a^{-1}, b^{-1})(a, b)$. □

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. □

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 $\gamma = \mathrm{lcm}(m,n)$ 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 $n \not| \, \delta$ 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 $n \,|\, \delta$. Similarly, $m \,|\, \delta$. But then by definition $\delta \geq \mathrm{lcm}(m,n) = \gamma$, a contradiction. Hence, $|a,b| = \mathrm{lcm}(m,n)$. □

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 $H = \{g \in G \,|\, g \neq g^{-1}\}$. 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, $|x| = 2$. □

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 $|G| \geq n = |x|$. □

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.