5.8

The set of $n \times n$ matrices with determinant 2 under matrix multiplication does not form a subgroup of $GL(n, \mathbb{R})$. Let A, B be $n \times n$ matrices with $\det(A) = \det(B) = 2$. Note then that $\det(AB) = \det(A)\det(B) = 4 \neq 2$. Therefore AB is not contained within the set, hence closure is not satisfied and not a subgroup.

5.15

Let F_0 denote the subset of all $f \in F$ such that $f(1) = 0$

Part A

F_0 does form a subgroup of F under addition.

> ***Proof.*** Let F_0 denote the subset of all $f \in F$ such that $f(1) = 0$. Let $f, g \in F_0$. Then $f(1) + g(1) = 0 + 0 = 0$, therefore F_0 is closed under functional addition. The identity element of F is the zero constant function, that is $e(x) = 0$. Note that $e(1) = 0$, therefore $e \in F_0$, hence the identity element of F is in F_0. Let $f \in F_0$. Let $f^{-1} = -f$, that is the negative of f. $-f \in F_0$ since $-f(1) = 0$. Additionally, $f + (-f) = 0 = e$, thefore every element of F_0 has an inverse. Therefore $F_0 \leq F$ under addition. ■

Part B

F_0 does not form a subgroup of $\tilde{F}$ under multiplication. Note that every element in F_0 by definition has a zero value at 1, hence $F_0 \not\subseteq \tilde{F}$, meaning F_0 cannot be a subgroup of $\tilde{F}$ under multiplication.

5.20

$$
\begin{aligned}
&G_i \leq G_i \text{ for } i = \{1, 2, \ldots, 9\} \\
&G_2 < G_8 < G_7 < G_1 < G_4 \\
&G_9 < G_3 < G_5 \\
&G_6 < G_5.
\end{aligned}
$$

5.21

Part A

$$\{\ldots, -50, -25, 0, 25, 50, \ldots\}.$$

Part B

$$\left\{\ldots, 4, 2, 0, \frac{1}{2}, \frac{1}{4}\ldots\right\}.$$

Part C

$$\left\{\ldots, \frac{1}{\pi^2}, \frac{1}{\pi}, 0, \pi, \pi^2\ldots\right\}.$$

5·33

Note that

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

And also that

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

Therefore the only elements that are generated by the matrix are the identity element and itself, hence the order of the subgroup is 2.

5·35

Note that

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

The inverse of the matrix is

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

which under repeated multiplication

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

Therefore the generated elements are the inverse of the matrix, the matrix itself, and the identity element. Hence the order of the subgroup is 3.

5.36

Part A

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.

Part B

$$\begin{aligned}
\langle 0\rangle &= \{0\} \\
\langle 1\rangle &= \{0,1,2,3,4,5\} \\
\langle 2\rangle &= \{0,2,4\} \\
\langle 3\rangle &= \{0,3\} \\
\langle 4\rangle &= \{0,2,4\} \\
\langle 5\rangle &= \{0,1,2,3,4,5\}.
\end{aligned}$$

Part C

Both 1 and 5 are generators for $\mathbb{Z}_6$.

Part D

$$\begin{tikzcd}
 & \langle 1\rangle = \langle 5\rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle 3\rangle \arrow[dr, dash] & & \langle 2\rangle = \langle 4\rangle \arrow[dl, dash] \\
 & \langle 0\rangle &
\end{tikzcd}$$

5.42

> ***Proof.*** Let $\langle G, *\rangle$ and $\langle G', *'\rangle$ be groups and let $\phi : G \to G'$ be an isomorphism between G and G'. Assume that G is a cylic group. Therefore there exists $g \in G$ such that $\langle g\rangle = G$. Examine $\phi(g)$ as a candidate for a generator of G'. Let $a' \in G'$. Since ϕ is an isomorphism, there is an $a \in G$ such that $\phi(a) = a'$. Since g is a generator, there is an $n \in \mathbb{Z}$ such that $a = g^n$. Therefore $a' = \phi(g^n)$. By repeated application of the

homorphism property of ϕ, $a' = \phi(g)^n$. There all elements of G' can be generated by $\phi(g)$, hence G' is cyclic.

■

5.46

Proof. Let G be a cyclic group and assume it has only one generator. Since G is cyclic there is an $a \in G$ such that

$$G = \{e, a, a^2, \dots, a^{n-1}\}.$$

Note that $a^{-1} = a^{n-1}$ is also a generator of G since for all k from 1 to $n-1$ since

$$(a^{-1})^k = (a^k)^{-1} = a^{n-k}.$$

Therefore if G has only one generator, $a = a^{n-1}$, or equivalently by examining the powers

$$\begin{aligned} n - 1 &= 1 \\ n &= 2. \end{aligned}$$

Therefore the group must be of size 2. Note that if $G = \{e\}$, it would also work. Hence if a cyclic group has a single generator it has an order of at most 2. ■

5.47

Proof. Let G be an abelian group. Define the set $H = \{x \in G : x^2 = e\}$. Let $a, b \in H$. Then

$$\begin{aligned} a^2b^2 &= e \\ aabb &= e \\ abab &= e && \text{(Since } G \text{ is abelian)} \\ (ab)(ab) &= e && \text{(By associativity)} \\ (ab)^2 &= e. \end{aligned}$$

Therefore $ab \in H$, meaning H is closed under the group operation of G. Consider the identity e of G. Since $ee = e$, it is in H. Let $a \in H$. Since $aa = aa = e$, a is its own inverse and therefore every element of H has an inverse. Therefore since H is closed under the group operation of G, has the identity of G, and has an inverse for every element, $H \leq G$. ■

5.49

Proof. Let G be a finite group and let $a \in G$. Consider the set $S = \{a, a^2, a^3, \ldots, a^m, a^{m+1}\}$ where $m = |G|$. Since there are $m+1$ elements in S, there has to be a repeat otherwise S would contain $m+1$ unique elements which is larger than $|G|$. Therefore there exists $\alpha, \beta \in \mathbb{Z}^+$ such that $\alpha \neq \beta$ and $a^\alpha = a^\beta$. Without loss of generality let $\alpha < \beta$. Then

$$\begin{aligned} a^\beta &= a^\alpha \\ a^{\beta-\alpha} &= e. \end{aligned}$$

Since $\alpha < \beta$, $\beta - \alpha > 0$ meaning $\beta - \alpha \in \mathbb{Z}^+$. Therefore for any $a \in G$ there exists a $n \in \mathbb{Z}^+$ such that $a^n = e$. ■

5.50

Proof. Let G be a finite group. Let $H \subseteq G$ where $|H| = m$ and m is finite and assume H is closed under the binary operation of G. Let $a \in H$. Consider the set $S = \{a, a^2, a^3, \ldots, a^m, a^{m+1}\}$. Every element of S is in H since H is closed. Since there are $m+1$ elements in S, there has to be a repeat otherwise S would contain $m+1$ unique elements which is larger than $|H|$. Therefore there exists $\alpha, \beta \in \mathbb{Z}^+$ such that $\alpha \neq \beta$ and $a^\alpha = a^\beta$. Without loss of generality let $\alpha < \beta$. Then

$$\begin{aligned} a^\beta &= a^\alpha \\ a^{\beta-\alpha} &= e. \end{aligned}$$

Since $\alpha < \beta$, $\beta - \alpha > 0$ meaning $\beta - \alpha \in \mathbb{Z}^+$. Therefore $e \in H$. Additionally every element of H has an inverse since

$$\begin{aligned} a^{\beta-\alpha-1}a &= a^{\beta-\alpha} \\ &= e. \end{aligned}$$

Therefore since H is closed under the group operation of G, has the identity of G, and has an inverse for every element, $H \leq G$. ■

5.51

Proof. Let G be a group and let $a \in G$. Define $H_a = \{x \in G : xa = ax\}$. Let $x, y \in H_a$. Then note that $xya = x(ya) = xay = (xa)y = axy$, therefore $xy \in H_a$. Note the identity of G is in H_a since $ea = a = ae$. Let $x \in H_a$. Then

$$\begin{aligned} xa &= ax \\ a &= x^{-1}ax \\ ax^{-1} &= x^{-1}a. \end{aligned}$$

Therefore $x^{-1} \in H_a$. Therefore since H is closed under the group operation of G, has the identity of G, and has an inverse for every element, $H \leq G$. ■

5·54

Proof. Let G be a group. Let H and K be sets such that $H \leq G$ and $K \leq G$. Consider $H \cap K$. Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Additionally since both are subgroups of G, $ab \in H$ and $ab \in K$ by closure. Therefore $ab \in H \cap K$. Since both H and K are subgroups of G, they both contain the identity element of G, and therefore $H \cap K$ contains the identity element. Let $a \in H \cap K$. Then $a^{-1} \in H$ and $a^{-1} \in K$ since both are subgroups and hence have inverses for every element. Therefore since a^{-1} is in H and K, $a^{-1} \in H \cap K$. Hence $H \cap K \leq G$. ■