Reading: Sections 4 and 5.

Section 4 Problems: You should be able to work out all problems, except 20-21 and 38. However, as mentioned in lectures, you should read/study all the problems (even ones you skip), so you (i) know the statements/results contained therein, and (ii) learn how the author generates questions!

Section 5 Problems: You should be able to work out all problems.

The following problems are **due on 11:59pm Tuesday 10/2/2018**. Submit both LaTeX and pdf files to the appropriate D2L Dropbox.
Please name the files using the following format:

LastName_FirstName_MTH411_Fall2018_HW_3

You may discuss the problems with your classmates, but your write-up must be your own. Any problems marked with an asterisk (*) denote problems you can not discuss with anyone except for me.

Please include the statements of the problems in your HW submissions. For any Extra problems you can copy the statements from the LaTeX file that generated this pdf. However, you will have to transcribe the remaining problems from Fraleigh.

Section 4: 2, 4, 6, 10, 12, 18, 26, 32-35, 41[1]
Section 5: 8, 13, 22-25, 36, 37-38, 41, 44, 45, 52, 54, 55

[1]Hint for 34: Use the The pigeon-hole principle! I.e. if n items/pigeons are put into m containers/holes, with $n > m$, then at least one container must contain more than one item.

Excersise 4.2-4.6 Determine whether the binary operation $*$ gives a group structure on the given set. If no group results, give the first axiom in the order $\mathscr{G}_1, \mathscr{G}_2, \mathscr{G}_3$ from Definition 4.1 that does not hold.

4.02 Let $*$ be defined on $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$ by letting $a * b = a + b$.

Let $a, b, c \in 2\mathbb{Z}$. Consider $a * (b * c)$.

$$a * (b * c) = a * (b * c) = a + (b + c)$$

And

$$(a * b) * c = (a + b) * c = (a + b) + c = a + (b + c)$$

Thus, $*$ is associative under $2\mathbb{Z}$.

Consider $0 = 2 \cdot 0 \in 2\mathbb{Z}$. Let $a \in 2\mathbb{Z}$. Then

$$0 + a = a + 0 = a$$

Thus 0 is an identity element.

Let $a \in 2\mathbb{Z}$. If $a = 2n$ for some $n \in \mathbb{Z}$, then $-n \in \mathbb{Z}$, so $-2n = -a \in 2\mathbb{Z}$. Observe

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

Thus, for all $x \in 2\mathbb{Z}$ there exists an inverse element. Therefore, because $*$ is associative, there exists an identity element, and because for all $x \in 2\mathbb{Z}$ there exists an inverse element, $2\mathbb{Z}$ closed under addition is a group.

4.04 Let $*$ be defined on $\mathbb{Q}$ by letting $a * b = ab$ Let $a, b, c \in \mathbb{Q}$. Notice.

$$a * (b * c) = a * (bc) = abc$$

and

$$(a * b) * c = (ab) * c = abc$$

Thus, $*$ is associative. Consider 1 in $\mathbb{Q}$. Let $a \in \mathbb{Q}$

$$1 * a = a * 1 = a$$

Thus, 1 is an identity element.
Consider $0 \in \mathbb{Q}$. Then, $0 = \frac{0}{1}$. There must exist a 0^{-1} such that $0 * 0^{-1} = 0^{-1} * 0 = 1$. Then, $0^{-1} = \frac{1}{0}$. But this is a contradiction as $\frac{1}{0}$ is not defined. Thus $*$ under $\mathbb{Q}$ does not have an inverse for all elements.
Therefore, $\mathbb{Q}$ is not a group under multiplication as it fails axiom $\mathscr{G}$.

4.06 Let $*$ be defined on $\mathbb{C}$ by letting $a * b = |ab|$ Let $a, b, c \in \mathbb{C}$. Then,

$$(a * b) * c = |ab| * c = ||ab|c| = |a||b||c|$$

and

$$a * (b * c) = a * |bc| = |a|bc|| = |a||b||c|$$

Thus, $*$ is associative under $\mathbb{C}$.

Let $|e| = 1$ for some $e \in \mathbb{C}$. Then,

$$a * e = e * a = a$$

Thus, e is an identity element.

Let $a \in \mathbb{C}$ and $a' \in \mathbb{C}$ such that a' is the inverse of a. Then,

$$a * a' = |aa'| = |a||a'| = aa = 2a$$

Thus, $\mathbb{C}$ under $a * b = |ab|$ does not have an inverse.
Therefore, $\mathbb{C}$ under $a * b = |ab|$ is not a group as it fails axiom $\mathscr{G}$

4.10 Let n be a positive integer and let $n \in \mathbb{Z} = \{nm | m \in Z\}$

(a) Show that $< n\mathbb{Z}, + >$ is a group. Let $np, nq \in n\mathbb{Z}$. Then,

$$nr + ns = n(r + s) \in n\mathbb{Z}$$

Thus, $n\mathbb{Z}$ is closed under addition.

As addition is associative and $n\mathbb{Z} \subset \mathbb{Z}, n\mathbb{Z}$ must be associative.
Let $e \in n\mathbb{Z}$. Then $e = nm$. Let $m = 0$. Then, $e = n0 = 0$.

$$0 + a = a + 0 = a, \text{ for some } a \in n\mathbb{Z}$$

Thus, 0 is the identity.
Let $a, b \in n\mathbb{Z}$ such that $a = nm$ and $b = n(-m)$. Then,

$$a + b = nm + n(-m) = n(m - m) = n0 = 0$$

Thus, there exists an inverse for all elements.
Therefore, $< n\mathbb{Z}, + >$ is a group.

(b) Show that $< n\mathbb{Z}, + > \simeq < \mathbb{Z}, + >$ Let $\phi : n\mathbb{Z} \to \mathbb{Z}$ be defined by $\phi(mn) = n$ for $mn \in n\mathbb{Z}$. Let $nm, nm' \in \mathbb{Z}$ such that $\phi(nm) = \phi(nm')$. Then, $\phi(nm) = m$ and $\phi(nm') = m'$. As $m = m'$ must be true we have $nm = nm'$.
Thus, ϕ is injective.
Let $m \in \mathbb{Z}$. Let $nm \in n\mathbb{Z}$ such that $\phi(nm) = m$. Thus, ϕ is surjective.
Let $nm, nm' \in n\mathbb{Z}$. Then, $\phi(nm) = m$ and $\phi(nm') = m'$. Notice.

$$\phi(nm + nm') = \phi(n(m + m')) = m + m' = \phi(nm) + \phi(nm')$$

Thus, ϕ is homomorphic.
Therefore, $< n\mathbb{Z}, + > \simeq < \mathbb{Z}, + >$

4.12,4.18 Determine whether the given set of matrices under the specified operation is a group.

4.12 All $n \times n$ diagonal matrices under matrix multiplication. Let H be all $n \times n$ diagonal matrices. As H is a subset of all $n \times n$ matrices and $n \times n$ matrices are associative. Thus, H under matrix multiplication must be associative.
Let the identity matrix be the identity element of H. Then,

$$AI_n = I_nA = A \text{ for some } A \in H$$

Thus, H under matrix multiplication has an identity element.
Let $Z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Then, as $Z \in H$, there must exist an invertible matrix, Z^{-1}, but $\det(Z) = 0$. Thus, Z is not invertible. Therefore, all $n \times n$ diagonal matrices under matrix multiplication is not a group.

4.18 All $n \times n$ matrices with determinant either 1 or -1 under matrix multiplication. Let H be all $n \times n$ with determinant either 1 or -1 under matrix multiplication. As H is a subset of all $n \times n$ matrices and $n \times n$ matrices are associative, thus H under matrix multiplication must be associative.
Let the identity matrix be the identity element of H. As $\det(I_n) = 1 \in \mathbb{Z}$, then

$$AI_n = I_nA = A \text{ for some } A \in H$$

Thus, H under matrix multiplication has an identity element.

Since, every matrix in H has a determinant of 1 or -1, the matrices must all be invertible.
Therefore, all $n \times n$ matrices with determinant either 1 or -1 under matrix multiplication is a group.

4.26 Give a one sentence proof synopsis of the proof of the left cancellation law in Theorem 4.15 Given $a*b = a*c$ for some elements in a set with binary operation $*$ by associativity and the existence of an inverse of a, we get $b = c$.

4.32 Show that every group G with identity e such that $x * x = e$ for all $x \in G$ is abelian.

Proof. Let $a, b \in G$. Then, $(a * b) * (a * b) = e$ and $(a * a) * (b * b) = e$. Thus, $a * b * a * b = a * a * b * b$. By left and right cancellation, we have $b * a = a * b$.
Therefore, G is abelian. □

4.33 Let G be an abelian group and let $c^n = c * c * \cdots * c$ for n factors c, where $c \in G$ and $n \in \mathbb{Z}^+$. Give a mathematical induction proof that $(a * b)^n = (a^n) * (b^n)$ for all $a, b \in G$.

Proof. Let $n = 1$ and $a, b \in G$ Then,

$$(a * b)^n = (a * b)^1 = (a * b) = a^1 * b^1$$

Thus, n holds for 1. Assume n holds true for some k. That is $(a*b)^n = (a*b)^k$. We will now show that the expression holds true for $k+1$. Observe.

$$\begin{aligned}(a*b)^{k+1} &= (a*b)*(a*b)^k \\ &= (a*b)*(a^k*b^k) \\ &= a*a^k*b*b^k \\ &= a^{k+1}*b^{k+1}\end{aligned}$$

Therefore, by mathematical induction $(a*b)^n = (a^n)*(b^n)$ for all $a, b \in G$. □

4.34 Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$.

Proof. Let m be the number of elements in G. Consider $e, a, a^2, \cdots, a^m$. As G is closed, $e, a, a^2, \cdots, a^m$ are in G. As G has only m elements, we must have $a^i = a^j$ for some $i, j \in \{0, 1, 2, \cdots, m\}$ with $0 \leq i < j \leq m$.

Case 1: $i = 0$
Then, j is a positive integer with $a^j = e$

Case 2: $i \neq 0$
Then, $0 < i < j$ and thus $0 < j - i$. As, $a^i = a^j$, we can cancel i times to get $e = a^j - i$, where $j - i$ is a positive integer.

In all cases, there is a positive integer n such that $a^n = e$.
Therefore, for any $a \in G \exists n \in \mathbb{Z}^+$ such that $a^n = e$ □

4.35 Show that if $(a*b)^2 = a^2*b^2$ for a and b in a group G, then $a*b = b*a$.

Proof. Let $(a*b)^2 = a^2*b^2$ for a and b in a group G. Then, $(a*b)*(a*b) = a*a*b*b$. Notice.

$$b*a*b = a*b*b$$

$$b*a = a*b$$

Therefore, if $(a*b)^2 = a^2*b^2$ for a and b in a group G, then $a*b = b*a$ □

4.41 Let G be a group and let g be one fixed element of G. Show that the map i_8, such that $i_8(x) = gxg'$ for $x \in G$, is an isomorphism of G with itself. Assume $i_g(x) = i_g(y)$ for some $x, y \in G$. Then,

$$gxg' = gyg'$$

$$x = y$$

Thus, i_g is injective.
Let $y \in G$. Then, $g'yg$ is an element of G. Notice.

$$i_g(g'yg) = gg'ygg' = eye = y$$

Thus, i_g is surjective.
Let $x, y \in G$. Observe.

$$\begin{aligned} i_g(xy) &= g(xy)g' \\ &= g(xg'gy)g' \\ &= (gxg')(gyg') \end{aligned}$$

Thus, i_g is homomorphic.
Therefore, i_g is an isomorphism.

Ex 5.08,5.13 Determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.

5.08 The $n \times n$ matrices with determinant 2. Not a subgroup. Let for some A, B such that $\det(A) = \det(B) = 2$. Then $\det(AB) = \det(A)\det(B) = 4$. Thus, the set is not closed under multiplication.

5.13 The set of all $n \times n$ matrices A such that $(A^T)A = I_n$ Is a subgroup. Let H be the set of all $n \times n$ matrices A such that $(A^T)A = I_n$. Let $A, B \in H$. Then $A = A^T A = I_n$ and $B = B^T B$. Notice.

$$\begin{aligned} (AB)^T(AB) &= B^T A^T AB \\ &= B^T(A^T A)B \\ &= B^T I_n B \\ &= B^T B \\ &= I_n \end{aligned}$$

Thus, H is closed under multiplication.
Let $A \in H$. Then, $A = A^T A = I_n$. Observe.

$$\begin{aligned} (A^{-1})^T A^{-1} &= (A^T)^T(A^T) \\ &= (AA^T)^T \\ &= (I_n)^T \\ &= I_n \end{aligned}$$

Thus, $A^{-1} \in H$.
Therefore, H is a subgroup of $GL(n, \mathbb{R})$.

Ex 5.22-5.25 Find the order of the cyclic subgroup of $GL(2, \mathbb{R})$ generated by the given 2×2 matrix.

5.22

$$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$$

Let $A = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$ Notice.

$$A^2 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

Then, we have $A^{2n} = (A^2)^n = (I_2)^2 = I_2$ and $A^{2n+1} = A^{2n+1} = A^{2n}A = I_2A = A$ for all $n \in \mathbb{Z}$.
Therefore, $\langle A \rangle = \{A^n | n \in \mathbb{Z}\} = \{I_2, A\} = \{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix}\}$

5.23

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

Let $A = \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$. Then, $A^2 = \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix} = \begin{bmatrix}1 & 2\\0 & 1\end{bmatrix}$
Assume for some $n \geq 2, A^n = \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}$.
Then $A^{n+1} = A^nA = \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix} = \begin{bmatrix}1 & n+1\\0 & 1\end{bmatrix}$.
Thus, for all $n \geq 2, A^n = \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}$. Also, $A^0 = I_2 = \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}$ and $A^1 = \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}$.
Thus, for all $n \geq 0, A^n = \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}$
There must exist an $(A^n)^{-1} = \begin{bmatrix}1 & -n\\0 & 1\end{bmatrix}$. Thus, for all $n \in \mathbb{Z}, \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}$. Therefore, $\langle A \rangle = \{A^n | n \in \mathbb{Z}\} = \{\begin{bmatrix}1 & n\\0 & 1\end{bmatrix} | n \in \mathbb{Z}\}$

5.24

$$\begin{bmatrix}3 & 0\\0 & 2\end{bmatrix}$$

Let $A = \begin{bmatrix}3 & 0\\0 & 2\end{bmatrix}$.
As A is a diagonal matrix we have for all $n \geq 1, A^n = \begin{bmatrix}3^n & 0\\0 & 2^n\end{bmatrix}$.
Given $n \geq 1$, we have $\begin{bmatrix}3^n & 0\\0 & 2^n\end{bmatrix}\begin{bmatrix}3^{-n} & 0\\0 & 2^{-n}\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = I_2$
which implies $A^{-n} = (A^n)^-1 = \begin{bmatrix}3^{-n} & 0\\0 & 2^{-n}\end{bmatrix}$.
Thus, $A^0 = I_2 = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = \begin{bmatrix}3^0 & 0\\0 & 2^0\end{bmatrix}$.
Then, $A^n = \begin{bmatrix}3^n & 0\\0 & 2^n\end{bmatrix}$ for all $n \in \mathbb{Z}$.
Therefore, $\langle A \rangle = \{A^n | n \in \mathbb{Z}\} = \{\begin{bmatrix}3^n & 0\\0 & 2^n\end{bmatrix} | n \in \mathbb{Z}\ \}$

5.25

$$\begin{bmatrix}0 & -2\\-2 & 0\end{bmatrix}$$

Let $A = \begin{bmatrix} 0 & -2 \\ -2 & 0 \end{bmatrix}$ and let $B = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$

Then, $A = 2B$ and $B^2 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$

Thus, for all $k \in \mathbb{Z}$,

$$\begin{aligned} A^{2K} &= (2B)^{2k} \\ &= 2^{2k}B^{2k} \\ &= 2^{2k}(B^2)^k \\ &= 2^{2k}(I_2)^k \\ &= 2^{2k}I_2 \\ &= \begin{bmatrix} 2^{2k} & 0 \\ 0 & 2^{2k} \end{bmatrix} \end{aligned}$$

and

$$\begin{aligned} A^{2k+1} &= A^{2k}A \\ &= (2^{2k}I_2)(2B) \\ &= (2^{2k}2B) \\ &= 2^{k+1}B \\ &= \begin{bmatrix} 0 & -2^{k+1} \\ -2^{k+1} & 0 \end{bmatrix} \end{aligned}$$

Thus, if n is even we have $A^n = \begin{bmatrix} 2^n & 0 \\ 0 & 2^n \end{bmatrix}$

And if n is odd we have $A^n = \begin{bmatrix} 0 & -2^n \\ -2^n & 0 \end{bmatrix}$

Therefore, $\langle A \rangle = \{\begin{bmatrix} 2^n & 0 \\ 0 & 2^n \end{bmatrix} | n \text{ is even}\}$ or $\{\begin{bmatrix} 0 & -2^n \\ -2^n & 0 \end{bmatrix} | n \text{ is odd}$

5.36 (a) Complete Table 5.25 to give the group $\mathbb{Z}_6$ of 6 elements.

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

(b) Compute the subgroups$< 0 >, < 1 >, < 2 >, < 3 >, < 4 >$ and $< 5 >$ of the group $\mathbb{Z}_6$ given part (a)

As 0+0 =0, we have $< 0 >= \{0\}$.

As $1 + 1 = 3, 1 + 1 + 1 = 3, 1 + 1 + 1 + 1 = 4, 1 + 1 + 1 + 1 + 1 = 5$, and

$1+1+1+1+1+1=0$. We have$< 1 >= \{0,1,2,3,4,5\}$
As $2+2=4$ and $2+2+2=0$. We have $< 2 >= \{0,2,4\}$.
As $3+3=0$, we have $< 3 >= \{0,3\}$
As $4+4=2$ and $4+4+4=0$, we have $< 4 >= \{0,2,4\}$
As $5+5=4, 5+5+5=3, 5+5+5+5=2, 5+5+5+5+5=1$ and $5+5+5+5+5+5=0$, we have$< 5 >= \{0,1,2,3,4,5\}$

(c) Which elements are generators for the group $\mathbb{Z}_6$ of part (a)? We see the generators of $\mathbb{Z}_6$ are 1 and 5.

(d) Give the subgroup diagram for the part (b) subgroups of $\mathbb{Z}_6$.

$$\langle 1\rangle = \langle 5\rangle = \mathbb{Z}_6$$
$$/ \qquad \backslash$$
$$\langle 2\rangle = \langle 4\rangle \quad \langle 3\rangle$$
$$\backslash \qquad /$$
$$\langle 0\rangle$$

Ex 5.37-5.38 Correct the definition of the italicized term without reference to the text, if correction is needed.

5.37 A *subgroup* of a group G is a subset H of G that contains the identity element e of G and also contains the inverse of each of its elements.
A *subgroup* of a group G is a subset H of G that contains the identity element e of G,contains the inverse of each of its elements, and is closed under the operation of G.

5.38 A group G is *cyclic* if and only if there exists $a \in G$ such that $G = \{a^n | n \in \mathbb{Z}\}$.
Correct as stated.

5.41 Let $\phi : G \to G'$ be an isomorphism of a group $< G, * >$ with a group $< G', *' >$

Proof. Let H be a subgroup of G. Consider the set $\phi[H] = \{\phi(h) | h \in H\}$. As ϕ is an isomorphism and $H \subseteq G$, we have $\phi(h) = G'$ for some $h \in G$. Thus, $\phi[H] \subseteq G'$.
As ϕ is a isomorphism there must exist a $\phi(e) = e'$ which gives us $e' \in \phi[H]$.// Let $x, y \in \phi[H]$. There must exist a $h_1, h_2 \in H$ such that $x = \phi(h_1)$ and $y = \phi(h_2)$. Then,

$$x *' y = \phi(h_1) *' \phi(h_2)$$

and

$$\phi(h_1 * h_2) = \phi(h_1) *' \phi(h_2)$$

Thus, $x *' y = \phi(h_1 * h_2)$
Thus, $\phi[H]$ is closed under $*'$

Let $x \in \phi[H]$. There must exist an $h \in H$ such that $x = \phi(h)$. As H is a subgroup of G we have $h^{-1} \in H$.
Then,

$$phi(h) *' \phi(h^{-1} = \phi(h * h{-}1) = \phi(e) = e'$$

. As,

$$(\phi(h))^{-1} *' (\phi(h) *' \phi(h^{-1})) = (\phi(h))^{-1} *' e' = (\phi(h))^{-1}$$

Notice.

$$(\phi(h))^{-1} *' (\phi(h) *' \phi(h^{-1})) = ((\phi(h))^{-1} *' \phi(h)) *' \phi(h^{-1}) = e' *' (h^{-1}) = \phi(h^{-1})$$

We have that $\phi(h^{-1}) = (\phi(h))^{-1} = x^{-1}$
Thus, $x^{-1} \in \phi[H]$.

Therefore,$\phi[H]$ is a subgroup of G' □

5.44 Find the flaw in the following argument: "Condition 2 of Theorem 5.14 is redundant, since it can be derived from 1 and 3, for let $a \in H$. Then $a^{-1} \in H$ by 3, and by a, $aa^{-1} = e$ is an identity element of H, proving 2.
If H is an empty set, you can't pick any arbitrary element in H. In addition, H would not contain the identity element as it's an empty set.

5.45 Show that a nonempty subset H of a group G is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$.

Proof. Suppose that H is a subgroup of G. Then for $a, b \in H$, we have $b^{-1} \in H$ and $ab^{-1} \in H$ since H must be closed under the induced operation.
Let $ab^{-}1 \in H$ for some $a, b \in H$. As H is nonempty, there must exist an $a \in H$ such that $b = a$. Then, $aa^{-1} = e$ which is in H. Since $e \in H$, we see $ea^{-1} = a^{-1}e = a^{-1}$ Thus, there is an identity element.
Let $a, b \in H$. Then $b^{-1} \in H$. Then, $a(b^{-1})^{-1} = ab$ which is in H. Thus, there is an inverse.
Therefore, H is a subgroup of G.

□

5.52 Generalizing Exercise 51, let S be any subset of a group G.

(a) Show that $H_s = \{x \in G | xs = sx \text{ for all} s \in S\}$ is a subgroup of G. Assuming S is nonempty. Let $x, y \in H_s$. Then for some $s \in S, xs = sx$ and $ys = sy$. Notice.

$$(xy)s = x(ys) = x(sy) = (xs)y = (sx)y = s(xy)$$

Thus, $xy \in H_s$ and H_s is closed under the operation.
As $H \subseteq G$ and G has an identity element, e. Then, for all $s \in S, es = se = s$. We see that $e \in H_s$
Let $x \in H_s$ and $s \in S$. Then, $xs = sx$ and $x^{-1}(xs)x^{-1} = x^{-1}(sx)x^{-1}$. Observe.

$$x^{-1}(xs)x^{-1} = x^{-1}x(sx^{-1}) = e(sx^{-1}) = sx^{-1}$$

and

$$x^{-1}(sx)x^{-1} = (x^{-1}s)(xx^{-1}) = (x^{-1}se) = x^{-1}s$$

Thus, $x^{-1}s = sx^{-1}$.
Thus, $x^{-1} \in H_s$.
Therefore, H_s is a subgroup.

(b) In reference to part (a), the subgroup H_G is the **center of** G. Show that H_G is an abelian group.

Proof. Let $a, b \in H_G$. Then, $ax = xa$ and $bx = xb$ for all $x \in G$. Then for $a * b$ notice.

$$ba = (ba)x = x(ba) = x(ab) = ab$$

Thus, H_G is abelian. □

5.54 Show that if $H \leq G$ and $K \leq G$, then $H \cap K \leq G$. Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Because H and K are subgroups, we have $ab \in H$ and $ab \in H \cap K$. Thus, $H \cap K$ is closed under the operation of G.
As $H \leq G$ and $K \leq G$, then $e \in H$ and $e \in K$. Thus, $e \in H \cap K$
Let $x, y \in H \cap K$. Then, $x \in H$ and $x \in K$. As $H \leq G$ and $K \leq G$, we have an inverse for x, namely x^{-1}. Then, $x^{-1} \in H$ and $x^{-1} \in K$. Thus, $x^{-1} \in H \cap K$.
Therefore, $H \cap K \leq G$

5.55 Prove that every cyclic group is abelian.

Proof. Let G be a cyclic group and let a be a generator of G such that $G = \langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.
Let $x, y \in G$, there exist r and s such that $x = a^r$ and $y = a^s$. Then,

$$xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = xy$$

Therefore, G is abelian. □