Exercise 2.1: A group can be constructed by using the rotations and reflections of a regular pentagon into itself. The group operator is "followed" (e.g., a reflectionρ "followed by" a rotation ρ). This is a permutation group, as in Example 2.14.

1. How many elements are in this group?
2. Construct the group (i.e., show the "multiplication table" for the group)
3. Is it an Abelian group?
4. Find a subgropu uwith five elements anda subgroup with two elements.
5. Are there any subgroups with four elements? Why?

---

1. There are 10 elements, one for each possible rotation $(0-4)$ and one for each reflection (about a – e).
2. The multiplication table is constructed as follows:

$\circ$	r_0	r_1	r_2	r_3	r_4	r_a	r_b	r_c	r_d	r_e
r_0	r_0	r_1	r_2	r_3	r_4	r_a	r_b	r_c	r_d	r_e
r_1	r_1	r_2	r_3	r_4	r_0	r_c	r_d	r_e	r_a	r_b
r_2	r_2	r_3	r_4	r_0	r_1	r_e	r_a	r_b	r_c	r_d
r_3	r_3	r_4	r_0	r_1	r_2	r_b	r_c	r_d	r_e	r_a
r_4	r_4	r_0	r_1	r_2	r_3	r_d	r_e	r_a	r_b	r_c
r_a	r_a	r_d	r_b	r_e	r_c	r_0	r_2	r_4	r_1	r_3
r_b	r_b	r_e	r_c	r_a	r_d	r_3	r_0	r_2	r_4	r_1
r_c	r_c	r_a	r_d	r_b	r_e	r_1	r_3	r_0	r_2	r_4
r_d	r_d	r_b	r_e	r_c	r_a	r_4	r_1	r_3	r_0	r_2
r_e	r_e	r_c	r_a	r_d	r_b	r_2	r_4	r_1	r_3	r_0

   The pentagram is represented by five points, $a-e$. Rotations of length $0-4$ are given as $r_{0\,-\,4}$ and reflections about the points a through e are denoted as $r_{a\text{–}e}$.

3. This group is not Abelian because the multiplication table is not symmetric, i.e. $r_4 \circ r_a$ is not the same as $r_a \circ r_4$.
4. The set $\{r_0, r_1, r_2, r_3, r_4\}$ is a subgroup with five elements because it is a group and a subset of the group we constructed using the rotations and reflections of a regular pentagon. The set $\{r_0, r_a\}$ is a subgroup with two elements.
5. There are no subgroups of four elements because there are no sets of four elements which are closed.

Exercise 2.2: Show that only one group exists with three elements "up to isomorphism." that is, there is only one way of filling out a binary operation table that satisfies all the requirements of a group.

Let a, b, and c be the only elements in a group G and let a be the identity for this group (satisfying G2) so that our operation table becomes

*	a	b	c
a	a	b	c
b	b		
c	c		

Next, we determine the inverse for each element. Because a is the identity, it is self-inverse which is already inferred. For the element b, the two options are $b * b = a$, or $b * c = a$. We know that $b * c \neq c$ because $a * c = c$, and if $b * c = c$, then that would imply that $b = a$ which it is not. Therefore, $b * c = a$ and $b * b = c$. Therefore, $b * c = a$ and consequently that $c * b = a$, per the definition of an inverse so that

*	a	b	c
a	a	b	c
b	b		a
c	c	a	

Finally, we now that $b * b \neq a$ because $b * b = a$ and $b * c = a$ would imply that $b = c$ and so $b * b = c$. By that same logic, $c * c = b$ so that

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Exercise 2.3: Show that there are two groups with four elements "up to isomorphism." One of these groups is isomorphic to $\mathbb{Z}_4$. The other is called the Klein 4-group.

Let the group $G = \{a, b, c, d\}$ and let the identity be a so that the the operation table becomes

*	a	b	c	d
a	a	b	c	d
b	b			
c	c			
d	d			

Because G is a group, we know that each element must have an inverse. The inverse of a is itself, which leaves b, c, and d. Inverse values come in pairs because $ab = 1 \implies ba = 1$. Therefore, either b, c, and d must all be self inverse, or one is self inverse and the remaining two elements are inverse to each other. Without loss of generality, we all three to be self inverse so that

*	a	b	c	d
a	a	b	c	d
b	b	a		
c	c		a	
d	d			a

The remaining values are constrained so that each column includes all four elements. If a column has a repeated element, then we could show that the values in the group are not unique, which requires the remaining elements to be

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

If we select only one value to be self-inverse, then the remaining constraints require the group operator to act so that

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

Therefore, there are only two 4-element groups up to isomorphism. The first has four self-inverse elements, and the second has two with the remaining relationships defined by the definition of a group.

Exercise 2.4: Prove that in a group G, the identity element is unique.

Let a and b be identity elements in a group G. Because both are identitys, then $a * b = a = b$, which implies that

$a = b$. Therefore, if two elements are identitys, then they are equal and thus, the identity element is unique.

Exercise 2.6 Let $G = \langle \mathbb{Z}_{16}, + \rangle$, the group of integers modulo 16. Let $H = \langle 4 \rangle$, the cyclic gropu generated by the element

1. List the elements of H.
2. Determine the cosets of G/H.
3. Draw the "addition" table for G/H.
4. To what group is G/H isomorphic?

1. Recall that the cyclic sub-group $\langle a \rangle$ is the set of elements a^n such that $a^n \in G, n \in \mathbb{Z}$. By this definition, the set $H = \{0, 4, 8, 12\}$ because the group G is defined under addition.
2. The set G/H is the set of cosets of the cyclic group $H = \langle 4 \rangle$ in G under addition. A cyclic group $\langle n \rangle$ is the set of values n^i which are elements of G (as given in the previous part). Therefore, the set of cosets of H is $\{S_i = i * H = i + H | i \in G\} = \{\{0, 4, 8, 12\}, \{1, 5, 9, 13\}, \{2, 6, 10, 14\}, \{3, 7, 11, 15\}\} = \{S_0, S_1, S_2, S_3\}$
3. Addition of cosets is defined as one element from the first coset added to all elements in the second coset. By this definition, we can say that

$+$	S_0	S_1	S_2	S_3
S_0	S_0	S_1	S_2	S_3
S_1	S_1	S_2	S_3	S_0
S_2	S_2	S_3	S_0	S_1
S_3	S_3	S_0	S_1	S_2

4. The cosets of G/H are group isomorphic to $\langle \mathbb{Z}_4, + \rangle$ by the mapping $\phi : G/H \to \mathbb{Z}_4 = \{S_i = i | i \in \mathbb{Z}_4\}$.

Exercise 2.9 Let G be a cyclic group with generator a and let $\mathcal{G}$ be a group isomorphic to G. If $\phi : G \to \mathcal{G}$ is an isomorphism, show that for every $x \in G, x$ may be written as a^j (for some j, using multiplicative notation) and that $\phi(x)$ is determined by $\phi(a)$.

From Definition 2.19 in the book, *For any $a \in G$, the set $\{a^n | n \in \mathbb{Z}\}$ generates a subgroup of G called the cyclic subgroup. The element a is said to be the generator of the subgroup.* Therefore, by the definition, $x \in G \implies \exists j \in \mathbb{Z}^+ \ni x = a^n$. Therefore, for every $x \in G$, x may be written as a^j. Next we know that $\phi(x)$ is determined by $\phi(a)$. The mapping $\phi : G \to \mathcal{G}$ is an isomorphism implies that $\phi(a^n) = \phi(a)^n$. Therefore

$$\begin{aligned} \phi(x) &= \phi(a^n) \\ &= \phi(a)^n \end{aligned}$$

which implies that $\phi(x)$ is determined by $\phi(a)$.

Exercise 2.10 An automorphism of a group$G$ is an isomorphism of the group with itself, $\phi : G \to G$. Using Exercise 2.9, how many automorphisms are there of $\mathbb{Z}_2$? of $\mathbb{Z}_6$? of $\mathbb{Z}_8$? of $\mathbb{Z}_{17}$?

From Problem 2.9, we know that all sets G that are isomorphic to another set $\mathcal{G}$ are cyclic groups with some generator a. Let $\mathcal{G}$ be equal to G in this case so that $\phi : G \to G$ is an automorphism $\implies \forall g \in G, \exists i \in \mathbb{Z} \ni a \cdot i = g$, which can be rewritten as $a(a^{-1}b) = b$, where $i = a^{-1}b$. Therefore, if there exists a multiplicative identity for a, then a can be used as a generator in this case. The set of automomorphisms is then the set of mappings between elements with multiplicative identity, or unit, in G.

In $\mathbb{Z}_2$, the only unit which exists is 1, and so the only automorphism is the trivial case where 1 maps to 1, and 0 maps to 0.

In $\mathbb{Z}_6$, the units are elements which are relatively prime to 6: 1, 3, 5. Therefore, there are three automorphisms: $1 \to 1$, $1 \to 3$, and $1 \to 5$. We need not include mappings between any other elements such as $3 \to 5$ because they are equivalent to $3 \to 1 \to 5$ which we have already addressed.

In $\mathbb{Z}_8$, the units are elements which are relatively prime to 8: 1, 3, 5, and 7. Therefore, there are four automorphisms: $1 \to 1$, $1 \to 3$, $1 \to 5$ and $1 \to 7$. We don't include mappings from other elements because a mapping from $3 \to 7$ is the same as $3 \to 1 \to 7$ which we have already addressed.

The set Z_{17} is a finite field because 17 is prime. Therefore, every non-zero element in $\mathbb{Z}_{17}$ is a unit so that there are 16 units in all. Therefore, there are also 16 automorphisms by the same logic as $\mathbb{Z}_8$.

Exercise 2.17 Show tha tif G, G', and G'' are groups and $\phi : G \to G'$ and $\psi : G' \to G''$ are homomorphisms, then the composite function $\psi \circ \phi : G \to G''$ is a homomorphism.

Let $a_1, a_2 \in G$ and recall that $\phi : G \to G'$ is a homomorphism so that

$$\phi(a_1 * a_2) = \phi(a_1) \cdot \phi(a_2)$$

Because $\phi(a_1), \phi(a_2) \in G'$, G' is closed under $\cdot$ and $\psi : G' \to G''$ is a homomorphism, then we can say that

$$\begin{aligned} &\psi(\phi(a_1) \cdot \phi(a_2)) = \psi(\phi(a_1)) \circ \psi(\phi(a_2)) \\ \implies &\psi(\phi(a_1 * a_2)) = \psi(\phi(a_1) \cdot \phi(a_2)) \\ \implies &\psi(\phi(a_1 * a_2)) = \psi(\phi(a_1)) \circ \psi(\phi(a_2)) \end{aligned}$$

which satisfies the definition of homomorphism.

Exercise 2.18 Consider the set $S = 0, 1, 2, 3$ with the operations

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Is this a field? if not, why not?

One property that all elements in a field must satisfy is the distributive property which states: $a, b, c \in S \implies a \cdot (b + c) = a \cdot b + a \cdot c$. We proceed by way of contradiction and assume the distributive property holds. Consider the case where $a = b = c = 2$ from the problem statement so that

$$\begin{aligned} &a \cdot (b + c) = a \cdot b + a \cdot c \\ \implies &2 \cdot (2 + 2) = 2 \cdot 2 + 2 \cdot 2 \\ \implies &2 \cdot 0 = 2 \cdot 2 + 2 \cdot 2 \\ \implies &0 = 3 + 3 \\ \implies &0 = 2 \end{aligned}$$

which is false. Therefore, the distributive property does not hold and hence, the set S is not a field.

Exercise 2.19 Construct the addition and multiplication tables for $\langle \mathbb{Z}_4, +, \cdot \rangle$ and comapre to the tables in equation (2.4). Does $\langle \mathbb{Z}_4, +, \cdot \rangle$ form a field?

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

These tables differ from those given for GF(4) in Equation 2.4 and do not represent a field because there is no multiplicative inverse for 2.

Exercise 2.20 Use the representation of GF(4) in (2.4) to solve the following pair of equations:

$$\begin{aligned} 2x + y &= 3 \\ x + 2y &= 3 \end{aligned}$$

By applying the usual algebraic methods, we can solve for x as

$$\begin{aligned} x &= (1 + (-2) \cdot 2)^{-1} \cdot (3 + ((-2) \cdot 3)) \\ &= (1 + 2 \cdot 2)^{-1} \cdot (3 + 2 \cdot 3) && \text{The additive inverse of 2 is 2, per (2.4)} \\ &= (1 + 3)^{-1} \cdot (3 + 1) && 2 \cdot 2 = 3 \text{ and } 2 \cdot 3 = 1 \text{ per (2.4)} \\ &= 1 && \text{Multiplication by a multiplicative inverse is 1} \end{aligned}$$

By substituting the value for x into one of the original expressions, we can show that

$$\begin{aligned} 2 \cdot 1 + y = 3 &\implies y = 3 + (-(2 \cdot 1)) && \text{additive inverse of } 2 \cdot 1 \\ &\implies y = 2 + (-2) && \text{1 is the multiplicative identity} \\ &\implies y = 3 + 2 && \text{The additive identity of 2 is 2 per 2.4} \\ &\implies y = 1 && 2 + 3 = 1 \text{ per 2.4} \end{aligned}$$

Exercise 2.22 Let $G = \{\mathbf{v}_1, \mathbf{v}_2 \ldots, \mathbf{v}_k\}$ be a basis for a vector space B. Show that for every vector $\mathbf{v} \in V$, there is a *unique* representation for $\mathbf{v}$ as a linear combination of the vectors i n G.

Let $\mathbf{a}, \mathbf{b} \in G \ni \mathbf{a} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 \ldots a_k\mathbf{v}_k$ and $\mathbf{b} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 \ldots b_k\mathbf{v}_k$. We will show that the representation for any vector is unique by demonstrating that $\mathbf{a} - \mathbf{b} = \mathbf{0}, \implies a_i = b_i \forall i \in 1, 2, \ldots k$ and thus that the representation for $\mathbf{a}$ and $\mathbf{b}$ is unique.

$$\mathbf{a} - \mathbf{b} = \mathbf{0} \implies (a_1 - b_1)\mathbf{v}_1 + (a_2 - b_2)\mathbf{v}_2 + \ldots + (a_k - b_k)\mathbf{v}_k = \mathbf{0}$$

The definition of linear independence states that two vectors $\mathbf{v}_i$ and $\mathbf{v}_j$ are linearly independent when $d_i\mathbf{v}_i + d_j\mathbf{v}_j = \mathbf{0} \implies d_i = d_j = 0$. Because the vectors $\mathbf{v}_k$ form a basis for a bector space B, they are linearly independent and thus, $a_i - b_i$ must equal zero, implying that $a_i = b_i$. Thus, if $\mathbf{a} - \mathbf{b} = 0$, then $\mathbf{a} = \mathbf{b}$ so that their representation as a linear combination of the basis vectors in G is unique.

Exercise 2.24 Let V be a vector space, and let $W \subset V$ be a subspace. The dual space $W^\perp$ of W is the set of vectors in V which are orthogonal to everyvector in W. Show that the dual space $W^\perp$ is a subspace of V.

The two primary requirements the set $W^\perp$ must satisfy to be considered a subspace is are

1. $W^\perp \subset V$
2. $W^\perp$ is a vector space

Fortunately, the problem statement has indicated that $W^\perp$ is a set of vectors in V which satisfies the first requirement. Therefore, we need only concern ourselves with the second. In showing that a set is a vector space, we need only concern ourselves with requirements related to closure and the existence of the zero vector because all other properties are inherited from the parent set V.

1. *Claim:* The set $W^{\perp}$ is closed under addition

   Proof: Let $\mathbf{a}, \mathbf{b} \in W^{\perp}$ and $\mathbf{c} \in W$,

$$\begin{aligned} &\implies \langle \mathbf{a}, \mathbf{c}\rangle = \langle \mathbf{b}, \mathbf{c}\rangle = 0 && \text{By the deffinition of orthogonality} \\ &\implies \langle \mathbf{a}, \mathbf{c}\rangle + \langle \mathbf{b}, \mathbf{c}\rangle = 0 && 0+0=0 \\ &\implies \langle \mathbf{a}+\mathbf{b}, \mathbf{c}\rangle = 0 && \text{Per distributivity with inner products in definition 2.60} \\ &\implies \mathbf{a}+\mathbf{b} \in W^{\perp} \end{aligned}$$

2. *Claim:* The set $W^{\perp}$ is closed under scalar multiplication

   Proof: Let $\mathbf{a} \in W^{\perp}$, $\mathbf{b} \in W$, and $c \in \mathbb{R}$.

$$\begin{aligned} &\implies \langle c \cdot \mathbf{a}, \mathbf{b}\rangle = c \cdot \langle \mathbf{a}, \mathbf{b}\rangle && \text{Per the definition of associativity in Definition 2.60} \\ &\implies c \cdot \langle \mathbf{a}, \mathbf{b}\rangle = c \cdot 0 && \mathbf{a} \perp \mathbf{b} \text{ by definition} \\ &\implies c \cdot 0 = 0 && 0 \text{ is the additive identity in the field } \mathbb{R} \end{aligned}$$

   therefore, the set $W^{\perp}$ is closed under scalar multiplication.

3. *Claim:* The zero vector, $\mathbf{0}$ is an element of $W^{\perp}$ *Proof:* Let $\mathbf{a} \in W$. This implies that $\langle \mathbf{a}, \mathbf{0}\rangle = 0$. Therefore, the zero vector is an element of $W^{\perp}$.

The remaining requirements are satisfied by $W^{\perp}$ being a subset of V and hence, adhere to the remaining properties which comprise a vector space. The set $W^{\perp}$ therefore is both a subset of V and a vectorspace, making it a subspace of V.

Exercise 2.25 Show that the set of binary polynomials (i.e., polynomials with binary coefficients, with operations in $GF(2)$) with degree less than r forms a vector space over $GF(2)$ with dimension r.

Let $f(x)$ be some polynomial with degree less than r so that $f(x) = a_0 + a_1 x + a_2 x^2 \dots a_{r-1}x^{r-1}$, where the coefficients are binary. We define a vector $\mathbf{a}$ such that

$$\mathbf{a} = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{r-1} \end{bmatrix}$$

which we use to represent $f(x)$. We will show that the span of all possible vectors $\mathbf{a}$, denoted V, is a vector space.

Claim: **V1:** V forms a commutative group under addition

Proof: The requirements for a commutative group are as follows:

1. **G1:** The operator + is associative: $\forall\ a, b \in V \implies (a+b)+c = a+(b+c)$

   Proof: The elements in V are made up of $\{0, 1\}$, which is a subset of the commutative ring with identity $\mathbb{Z}$. Because addition operates on an element-by-element basis, each pair-wise elements will adhere to this property and thus, the entire vector will as well.

2. **G2:** There exists an identity element $\mathbf{0}$ in V such that $\mathbf{v} \in V \implies \mathbf{v} + \mathbf{0} = \mathbf{v}$.

   Proof: Because the components in each vector come from the set $\{0, \}1$, 0 is the additive identity from $\mathbb{Z}$, and 1 is an element in $\mathbb{Z}$, then each vector element will adhere to this property, that is, $a_i + 0 = a_i$ where a_i is the ith component of some vector in V. Because addition operates on each vector on an element-by-element basis, then the same property holds for each vector. Therefore, $\mathbf{0} + \mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$.

3. **G3:** $\forall\ \mathbf{v} \in V, \exists \mathbf{a}^{-1} \in V \ni \mathbf{a} + \mathbf{a}^{-1} = \mathbf{0}$.

   Proof: We will prove that this property holds by showing that it holds for each element of the vector and that because addition operates on an element by element basis, that it also holds for addition on a pair of vectors. Each element of a vector is an element of $GF(2) = \{0, 1\}$. In the case of 1, $1+1=0$, and $0+0=0$. Therefore, for each vector element, there exists an additive inverse and therefore, there is an additive inverse for each vector as well.

Claim: **V2:** $\forall\ \mathbf{v} \in V,\ a \in GF(2),\ a \cdot \mathbf{v} \in V$

Proof: Note that scalar multiplication operates on each vector element independently. Therefore, it is sufficient to show that $GF(2)$ is closed under multiplication, which holds because $GF(2)$ is a field.

Claim: **V3:** $\forall\ \mathbf{v} \in V,\ a, b \in GF(2),\ (a+b) \cdot \mathbf{V} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$.

Proof: Note that scalar multiplication and addition occur on an element by element basis. Therefore, if each element adheres to this property, then the vectors will as well. Let v_i be the ith element in a vector $\mathbf{v} \in V$ and let $a, b \in GF(2)$. We know that $v_i \in GF(2)$ as all vector elements are binary per the definition of V. Therefore, we know that $(a+b) \cdot v_i = a \cdot v_1 + b \cdot v_1$ because $GF(2)$ is a field.

Claim: **V4:** $\forall\ \mathbf{v} \in V,\ a, b \in GF(2),\ (a \cdot b) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$.

Proof: By the same logic as **V3**, the elements in V and $GF(2)$ adhere to this property. Therefore, the elements in V adhere to all the properties of a vector space.

Exercise 2.28 Let $S = \{\mathbf{v}_1, \mathbf{v}_2, , \ldots, \mathbf{v}_n\}$ be an arbitrary basis for the vector space V. Let $\mathbf{v}$ be an arbitrary vector in V; it may be expressed as the linear combination

$$\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_n\mathbf{v}_n.$$

Develop an expression for computing the coefficients $\{a_i\}$ in this representation.

We pose the problem of finding the coefficients $\mathbf{a}$ (where a_i is the ith element in $\mathbf{a}$) as a linear set of equations [1] where

$$\begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ \mathbf{v}_1 & \mathbf{v}_2 & \ldots & \mathbf{v}_n \\ \downarrow & \downarrow & & \downarrow \end{bmatrix} \begin{bmatrix} \uparrow \\ \mathbf{a} \\ \downarrow \end{bmatrix} = \begin{bmatrix} \uparrow \\ \mathbf{v} \\ \downarrow \end{bmatrix}$$

which we resolve using a pseudo-inverse so that

$$(V^T V)^{-1} V^T \mathbf{v} = \mathbf{a}$$

where V is the matrix of basis vectors.[2]

Exercise 2.30 Let V be a vector space and let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$. Show that span$(\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\})$ is a vector space.

Because $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \in V$, then we know that they follow the usual behavior for vector spaces. The only constraints we need prove are those related to closure. In the following proofs, we define $\mathcal{S}$ as the set of vectors in the span of $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$.

Claim: $\mathcal{S}$ is closed under addition.

Proof: Let V be a matrix where each column[1] is a basis vector so that every element in $\mathcal{S}$ can be represented as a linear combination of the basis vectors in V. $\mathbf{a}_1, \mathbf{a}_2 \in V \implies \exists \mathbf{b}_1, \mathbf{b}_2 \ni V\mathbf{b}_1 = \mathbf{a}_1$ and $V\mathbf{b}_2 = \mathbf{a}_2$. Therefore, $\mathbf{a}_1 + \mathbf{a}_2 = V\mathbf{b}_1 + V\mathbf{b}_2 = V(\mathbf{b}_1 + \mathbf{b}_2)$ Because there exists a vector such that $V(\mathbf{b}_1 + \mathbf{b}_2) = \mathbf{a}_1 + \mathbf{a}_2$, then $\mathbf{a}_1 + \mathbf{a}_2$ must be in the span of the basis vectors. Therefore, the set $\mathcal{S}$ is closed under addition.

Claim: $\mathcal{S}$ is closed under scalar multiplication

Proof: Let $\mathbf{a} \in \mathcal{S} \ni \exists \mathbf{b} \ni V\mathbf{b} = \mathbf{a}$. Also let c be a scalar value so that $c \cdot \mathbf{a} = c \cdot (V\mathbf{b}) = V(c \cdot \mathbf{b})$ Because $c \cdot \mathbf{a} = V(c \cdot \mathbf{b})$, then there exists a linear combination of basis vectors from the span of $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_3\}$ which is equal to $c \cdot \mathbf{a}$, $\implies c \cdot \mathbf{a} \in \mathcal{S}$.

[1] Note the use of column vector notation with vectors multiplied on the right of matrices. There are those who prefer a row-vector notation, and even though they are wrong and should be dutifully corrected, they are a rather obstinate bunch and it just isn't worth it. Such correction will have to take place during the millenium (weeping, wailing, burning of text, etc.).

[2] Full disclosure: Because I am finishing these problems after the due date, I overheard several classmates talking about one of the last problems they missed. They mentioned that they needed to use a pseudo-inverse to solve the problem and had missed points because they did not take this approach. As I first worked through this problem, I used a one dimensional projection approach and would likely have missed points for the same reason. When I realized that I hadn't come accross anything that required a pseudo-inverse, I reexamined this problem and reformulated it as seen above. Upon further inspection, I realize that a full inverse needs to be used to account for redundencies in the basis vectors. The inverse formulation provides the needed rotation/separation so that we work with orthogonal vectors when finding the projections. Furthermore a pseudo-inverse accounts for scenarios where the basis is rank-deficient although by definition I don't know if that is really necessary in this case.

Claim: $\mathcal{S}$ contains the zero vector.

Proof: From the previous proof, we know that $\mathcal{S}$ is closed under scalar multiplication. Let $\mathbf{a} \in \mathbf{S}$. Then $0 \cdot \mathbf{a} \in \mathcal{S} \implies \mathbf{0} \in \mathcal{S}$.