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. Insert response here:
2. Insert response here:
3. Insert response here:
4. Insert response here:
5. Insert response here:

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 $|a|$ is the set of elements a^n such that $a^n \in G, n \in \mathbb{Z}$. By this definition, the elements of $H = \{0, 4, 8, 12\}$ because the group G is defined under addition.

2. The cosets of G/H are defined as the sets $a * H$ for all $a \in H$. Therefore, our cosets are H plus $0, 1, 2$, and 3 because afterwords, all other cosets are equivalent to one of these four. This gives $S_0 = \{0, 4, 8, 12\}, S_1 = \{1, 5, 9, 13\}, S_2 = \{2, 6, 10, 14\}$, and $S_3 = \{3, 7, 11, 15\}$.

3.

4. Insert response here:

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 $\phi(a)$.

Insert response here:

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 $\mathbb{Z}_{17}$?

Insert response here:

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.

Insert response here:

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

$\cdot$	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?

Insert response here:

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?

Insert response here:

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

$$2x + y = 3$$
$$x + 2y = 3$$

Insert response here:

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 **v** as a linear combination of the vectors i n G.

Insert response here:

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.

Insert response here: