To get a better understanding of groups we look for certain nonempty subsets of a group that may be groups with respect to the binary operations of the "mother" group.

Definitions. A nonempty subset $H$ of a group $G$ is a subgroup of $G$ if $H$ is itself a group under the binary operation in $G$.

Every group has two subgroups: the trivial subgroup $H = \{e\}$, and the whole group $H = G$.

All other subgroups of $G$, if they exist, are called proper subgroups of $G$.

Examples. (a) The subset $H = \{1, 9\}$ of $U_{10} = \{1, 3, 7, 9\}$ is a subgroup of $U_{10}$ because $1 \cdot 1 = 1$, $1 \cdot 9 = 9$, $9 \cdot 1 = 9$, and $9 \cdot 9 = 1$.

(b) The subset

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

of $S_3$ is a subgroup.

When checking if a nonempty subset of a group is a subgroup or not, we need not check the associativity Axiom.

Indeed, we need only check one condition (this differs from Theorem 7.10 (Ed.2) 7.11 (Ed.3) in the book).

Theorem. 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 $H$ is a subgroup of $G$.

For any $b \in H$, we have $b^{-1} \in H$ because $H$ being a group contains the inverses of its elements.

Then for any $a \in H$ we have $ab^{-1} \in H$ by closure of the binary operation.

Now suppose that $H$ is a nonempty subset of $G$ for which $ab^{-1} \in H$ for all $a, b \in H$.

For any $a \in H$ we have $e = aa^{-1} \in H$.

Then for any $b \in H$ we have $b^{-1} = eb^{-1} \in H$, so that $H$ contains the inverses of all of its elements.

For $a, b \in H$ we know that $b^{-1} \in H$, so that $ab = a(b^{-1})^{-1} \in H$.

Hence $H$ is closed under the operation of $G$, so that $H$ is a subgroup.

Example. The nonabelian Heisenberg group

$$G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, x \in \mathbb{R} \right\}$$

arises in the description of one-dimensional quantum mechanics.
Is the nonempty subset \( H = \left\{ \begin{bmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : y \in \mathbb{R} \right\} \) a subgroup of \( H \)?

For \( a = \begin{bmatrix} 1 & 0 & y_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 & y_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \), we have

\[
ab^{-1} = \begin{bmatrix} 1 & 0 & y_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -y_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & y_1 - y_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in H.
\]

So \( H \) is a subgroup of \( G \).

Not every group is abelian, but does every group have an abelian subgroup?

Definition. The center of a group \( G \) is the subset

\[
Z(G) = \{ a \in G : ag = ga \text{ for all } g \in G \}.
\]

This asks for which elements of \( G \) commute with every element of \( G \).

When \( G \) is abelian, we have \( Z(G) = G \); when \( G \) is nonabelian we have \( Z(G) \) is a proper subset of \( G \).

Theorem 7.13. The center \( Z(G) \) of a group \( G \) is a subgroup of \( G \).

Proof. First we show that \( Z(G) \) is nonempty: the identity element \( e \in G \) satisfies \( eg = ge \) for all \( g \in G \), and so \( e \in Z(G) \).

Last we show that \( Z(G) \) satisfies: for all \( a, b \in Z(G) \) we have \( ab^{-1} \in Z(G) \), and apply the previous Theorem to show that \( Z(G) \) is a subgroup of \( G \).

With \( a, b \in G \) we have \( ag = ga \) and \( bg = gb \) for all \( g \in G \).

We multiply on both the left and the right of the two sides of \( bg = gb \) by \( b^{-1} \) to get for all \( g \in G \) that

\[
bg^{-1} = b^{-1}bg^{-1} = b^{-1}gbb^{-1} = b^{-1}g.
\]

Then for all \( a, b \in Z(G) \) we have for all \( g \in G \) that

\[
ab^{-1}g = agb^{-1} = gab^{-1},
\]

showing that \( ab^{-1} \in Z(G) \), and so \( Z(G) \) is a subgroup of \( G \). \( \square \)

Example. The subgroup \( H \) of the Heisenberg group \( G \) above is \( Z(G) \).

There are also other kinds of abelian subgroups of a group.

Notation. For a group \( G \) and an element \( a \in G \), we set

\[
\langle a \rangle = \{ a^n : n \in \mathbb{Z} \}.
\]

Theorem 7.14. For a group \( G \) and \( a \in G \), the subset \( \langle a \rangle \) is a subgroup of \( G \).
Proof. The subset \( \langle a \rangle \) is nonempty because it contains \( a = a^1 \).
For \( g, h \in \langle a \rangle \) there are \( i, j \in \mathbb{Z} \) such that \( g = a^i \) and \( h = a^j \).
Then \( h^{-1} = a^{-j} \), so that \( gh^{-1} = a^i a^{-j} = a^{i-j} \in \langle a \rangle \).
Thus \( \langle a \rangle \) is a subgroup of \( G \).
\( \square \)

Definitions. For a group \( G \) and \( a \in G \), the subgroup \( \langle a \rangle \) is called the cyclic subgroup of \( G \) generated by \( a \).

If \( G = \langle a \rangle \) for some \( a \in G \), then we say that \( G \) is a cyclic group.

Observe that every cyclic group (or subgroup) is abelian because for all \( i, j \in \mathbb{Z} \), there holds \( a^i a^j = a^{i+j} = a^{j+i} = a^j a^i \).

Example. The group \( U_{10} = \{1, 3, 7, 9\} \) is cyclic because \( U_{10} = \langle 3 \rangle \), that is \( 3^1 = 3, 3^2 = 9, 3^3 = 7, \) and \( 3^4 = 1 \).
Notice also that \( U_{10} = \langle 7 \rangle \) because \( 7^1 = 7, 7^2 = 9, 7^3 = 3, \) and \( 7^4 = 1 \).

Theorem 7.15. Let \( G \) be a group and \( a \in G \).

(1) If \( a \) has infinite order, then \( \langle a \rangle \) is an infinite subgroup consisting of the distinct elements \( a^k \) of \( k \in \mathbb{Z} \).

(2) If \( a \) has finite order \( n \), then \( \langle a \rangle \) is a subgroup of order \( n \) and
\[
\langle a \rangle = \{a^0 = e, a^1, a^2, \ldots, a^{n-1}\}.
\]
Proof. (1) When \( a \in G \) has infinite order, then \( a^k \) for \( k \in \mathbb{Z} \) are all distinct, and hence \( \langle a \rangle \) is an infinite subgroup of \( G \).

(2) For an element \( a^i \) of \( \langle a \rangle \), we have \( i \) is congruent modulo \( n \) to one of \( 0, 1, 2, \ldots, n-1 \).
Thus \( a^i \) is equal to one of the \( n \) elements \( a^0 = e, a^1, a^2, \ldots, a^{n-1} \).
No two of \( a^0, a^1, a^2, \ldots, a^{n-1} \) can be the same since no two of the integers \( 0, 1, 2, \ldots, n-1 \) are congruent modulo \( n \).
Therefore \( \langle a \rangle = \{a^0, a^1, a^2, \ldots, a^{n-1}\} \) which has order \( n \). \( \square \)

What is the structure of subgroups of a cyclic group?

Theorem 7.17. Every subgroup of cyclic subgroup is itself cyclic.

Idea of Proof. Let \( H \) be a subgroup of \( G = \langle a \rangle \).

Then \( H \) contains positive powers of \( a \), and the set of positive powers has a smallest power, say \( k \).
One shows that \( H = \langle a^k \rangle \) by showing that each element of \( H \) is a power of \( a^k \).
This is done by taking \( a^m \in H \) and writing \( m = kq + r \) with \( 0 \leq r < k \), so that \( a^r = a^m (a^k)^{-q} \in H \).
By the minimality of \( k \), we have \( r = 0 \), so that \( m = kq \). \( \square \)

Example. Is \( U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\} \) cyclic?
We have \( \langle 2 \rangle = \{2, 4, 8, 11\}, \langle 4 \rangle = \{4, 1\}, \langle 7 \rangle = \{7, 4, 13, 1\}, \langle 8 \rangle = \{8, 4, 2, 1\} = \langle 2 \rangle, \langle 11 \rangle = \{11, 1\}, \langle 13 \rangle = \{13, 4, 7, 1\} = \langle 7 \rangle, \) and \( \langle 14 \rangle = \{1, 14\} \).
So \( U_{15} \) is not cyclic, and notice that \( \langle 4 \rangle \) is a subgroup of \( \langle 2 \rangle \).