**Subgroups**

**Example.** The cyclic group of order 4 is

\[ \mathbb{Z}_4 = \{0, 1, 2, 3\} \]

with addition mod 4.

Look at the subset \( \{0, 2\} \). It is closed under the group operation: \( 0 + 0 = 0, 0 + 2 = 2, 2 + 2 = 0 \). It contains the identity element 0. And it is closed under taking inverses: \( 2 + 2 = 0 \) shows that 2 is its own inverse.

In other words, \( \{0, 2\} \) is a group *in its own right* using the operation it inherits from \( \mathbb{Z}_4 \).

**Example.** \( \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \), and these are all groups under ordinary addition. In each case, you can think of a given subset as “inheriting” the group operation from a superset. If you add elements of a subset (say \( \mathbb{Z} \)) according to the addition law in a superset (say \( \mathbb{Q} \)), you get a group. (In particular, the subset is closed under the addition, and contains the identity and inverses of elements.)

**Definition.** Let \( G \) be a group. A subset \( H \) of \( G \) is a **subgroup** of \( G \) if:

1. \( H \) is closed under the group operation: If \( a, b \in H \), then \( a \cdot b \in H \).
2. \( 1 \in H \).
3. If \( a \in H \), then \( a^{-1} \in H \).

Write \( H < G \) to mean that \( H \) is a subgroup of \( G \).

Notice that associativity is *not* part of the definition of a subgroup. Since associativity holds in the group, it holds automatically in any subset.

Look carefully at the identity and inverse axioms for a subgroup; do you see how they differ from the corresponding axioms for a group?

In verifying the identity axiom for a subgroup, the issue is not the existence of an identity; the group must have an identity, since that’s part of the definition of a group. The issue is whether the identity for the group is actually contained in the subgroup.
Likewise, for subgroups the issue of inverses is not whether inverses exist; every element of a group has an inverse. The issue is whether the inverse of an element in the subgroup is actually contained in the subgroup.

\[ x^{-1} \]

In a group, the question is: "Does every element have an inverse?"

In a subgroup, the question is: "Is the inverse of a subgroup element also a subgroup element?"

Example. \{1\} and \( G \) are always subgroups of \( G \). ☐

Example. Let \( n \in \mathbb{Z} \). Then

\[ n\mathbb{Z} = \{ nx \mid x \in \mathbb{Z} \} \]

is a subgroup of \( \mathbb{Z} \), the group of integers under addition.

\( n\mathbb{Z} \) consists of all multiples of \( n \).

First, I’ll show that \( n\mathbb{Z} \) is closed under addition. If \( nx, ny \in n\mathbb{Z} \), then

\[ nx + ny = n(x + y) \in n\mathbb{Z}. \]

Therefore, \( n\mathbb{Z} \) is closed under addition.

Next, the identity element of \( \mathbb{Z} \) is 0. Now \( 0 = n \cdot 0 \), so \( 0 \in n\mathbb{Z} \).

Finally, suppose \( nx \in \mathbb{Z} \). The additive inverse of \( nx \) in \( \mathbb{Z} \) is \( -nx \), and \( -nx = n(-x) \). This is \( n \) times something, so it’s in \( n\mathbb{Z} \). Thus, \( n\mathbb{Z} \) is closed under taking inverses.

Therefore, \( n\mathbb{Z} \) is a subgroup of \( \mathbb{Z} \).

By the way, notice that \( \mathbb{Z} \cup 3\mathbb{Z} \) is not a subgroup of \( \mathbb{Z} \), since it isn’t closed under addition. The union of subgroups need not be a subgroup. ☐

Example. \( \mathbb{Z} \) is a subgroup of \( \mathbb{Q} \), the group of rational numbers under addition.

If you add two integers, you get an integer: \( \mathbb{Z} \) is closed under addition.

The identity element of \( \mathbb{Q} \) is 0, and \( 0 \in \mathbb{Z} \).

Finally, if \( n \in \mathbb{Z} \), its additive inverse in \( \mathbb{Q} \) is \( -n \). But \( -n \) is also an integer, so \( \mathbb{Z} \) is closed under taking inverses.

Therefore, \( \mathbb{Z} \) is a subgroup of \( \mathbb{Q} \). ☐

Definition. If \( G \) is a group and \( g \) is an element of \( G \), the **subgroup generated by** \( g \) (or the **cyclic subgroup generated by** \( g \)) is

\[ \langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \}. \]
In other words, \(<g>\) consists of all (positive or negative) powers of \(g\).

This definition assumes multiplicative notation; if the operation is addition, the definition reads

\[\langle g \rangle = \{ k \cdot g \mid k \in \mathbb{Z}\}.
\]

In this case, you’d say that \(<g>\) consists of all (positive or negative) multiples of \(g\).

Be sure you understand that the difference between the two forms is simply notational: It’s the same concept.

Since I’m calling \(<g>\) a subgroup, I’d better verify that it satisfies the subgroup axioms.

**Lemma.** If \(G\) is a group and \(g \in G\), then \(<g>\) is a subgroup of \(G\).

**Proof.** For closure, note that if \(g^m, g^n \in \langle g \rangle\), then

\[g^m \cdot g^n = g^{m+n} \in \langle g \rangle.\]

\(1 = g^0 \in \langle g \rangle\). Finally, if \(g^n \in \langle g \rangle\), its inverse is \(g^{-n}\), which is also in \(<g>\).

Therefore, \(<g>\) is a subgroup of \(G\). \(\square\)

In fact, \(<g>\) is the smallest subgroup of \(G\) which contains \(g\).

---

**Example.** Consider \(U_{18} = \{1, 5, 7, 11, 13, 17\}\), the group of units in \(\mathbb{Z}_{18}\). (Remember that these are the elements in \(\{0, 1, 2, \ldots, 17\}\) which are relatively prime to 18, and the operation is multiplication mod 18).

The cyclic subgroup generated by \(7\) consists of all powers of \(7\):

\[7^0 = 1, \quad 7^1 = 7, \quad 7^3 = 13.\]

I can stop here, because \(7^3 = 343 = 1 \text{ mod } 18\). So

\[\langle 7 \rangle = \{1, 7, 13\}.\]

On the other hand, consider \(\mathbb{Z}_{20}\), the cyclic group of order 20. In this group, the operation is addition mod 20. Hence, the subgroup generated by an element — say \(8\) — consists of all multiples of \(8\):

\[0 \cdot 8 = 0, \quad 1 \cdot 8 = 8, \quad 2 \cdot 8 = 16, \quad 3 \cdot 8 = 4, \quad 4 \cdot 8 = 12.\]

I can stop here, because \(5 \cdot 8 = 0 \text{ mod } 20\). So

\[\langle 8 \rangle = \{0, 8, 16, 4, 12\}. \quad \square\]

---

**Example.** I’ll show later on that the only subgroups in a cyclic group are subgroups generated by single elements. So, for example, the subgroups of \(\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}\) are

\[\langle 0 \rangle = \{0\},\]

\[\langle 2 \rangle = \langle 6 \rangle = \{0, 2, 4, 6\},\]

\[\langle 4 \rangle = \{0, 4\},\]

\[\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7\}.\]
The way the subgroups are contained in one another can be pictured in a **subgroup lattice diagram**:

\[
\begin{array}{c}
\langle 0 \rangle \\
\langle 2 \rangle \\
\langle 1 \rangle \\
\langle 4 \rangle
\end{array}
\]

**Example.** If \( H < K \) and \( K < G \), then \( H < G \): A subgroup of a subgroup is a subgroup of the (big) group. To put it another way, the subgroup relationship is transitive. I’ll leave the (easy) proof to you. 

---

If you want to show that a subset \( H \) of a group \( G \) is a subgroup of \( G \), you can check the three properties in the definition. But here is a little shortcut.

**Lemma.** Let \( G \) be a group, and let \( H \) be a nonempty subset of \( G \). \( H < G \) if and only if \( a, b \in H \) implies \( a \cdot b^{-1} \in H \).

**Proof.** \((\Rightarrow)\) Suppose \( H < G \), and let \( a, b \in H \). Then \( b^{-1} \in H \) (since \( H \) is closed under inverses), hence \( a \cdot b^{-1} \in H \) (since \( H \) is closed under products).

\((\Leftarrow)\) Suppose that \( a, b \in H \) implies \( a \cdot b^{-1} \in H \). Since \( H \neq \emptyset \), take \( a \in H \). Then \( 1 = a \cdot a^{-1} \in H \).

If \( a \in H \), then \( a^{-1} = 1 \cdot a^{-1} \in H \) (since I already know \( 1 \in H \)). This shows \( H \) is closed under taking inverses.

Finally, suppose \( a, b \in H \). Then \( b^{-1} \in H \), so \( ab = a \cdot (b^{-1})^{-1} \in H \). Therefore, \( H < G \). 

---

**Example.** Let \( GL_2(\mathbb{R}) \) be the group of invertible \( 2 \times 2 \) matrices with real entries. Consider the set

\[
D = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbb{R} \text{ and } a \neq 0 \right\}.
\]

I’ll show that \( D \) is a subgroup of \( GL_2(\mathbb{R}) \).

First,

\[
\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in D.
\]

Therefore, \( D \) is nonempty.

Next, suppose \( \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \in D \) where \( a, b \in \mathbb{R} \) and \( a, b \neq 0 \). Note that

\[
\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}^{-1} = \begin{bmatrix} b^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix}.
\]
Then\
\[
\begin{bmatrix}
  a & 0 \\
  0 & a
\end{bmatrix}
\begin{bmatrix}
  b & 0 \\
  0 & b
\end{bmatrix}^{-1} =
\begin{bmatrix}
  a & 0 \\
  0 & a
\end{bmatrix}
\begin{bmatrix}
  b^{-1} & 0 \\
  0 & b^{-1}
\end{bmatrix} =
\begin{bmatrix}
  ab^{-1} & 0 \\
  0 & ab^{-1}
\end{bmatrix} \in D.
\]

Therefore, $D$ is a subgroup of $GL_2(\mathbb{R})$. 

\textbf{Example.} Let $G$ be a group. $a, b \in G$ commute if $ab = ba$.

The center $Z(G)$ of $G$ is the set of elements which commute with everything in $G$:

\[Z(G) = \{g \in G \mid gh = hg \text{ for all } h \in G\}.\]

I’ll show that $Z(G) \leq G$.

First, $1 \cdot g = g = g \cdot 1$ for all $g \in G$, so $1 \in Z(G)$. In particular, $Z(G) \neq \emptyset$.

Now suppose $a, b \in Z(G)$. I’ll show $a \cdot b^{-1} \in Z(G)$. To do this, I must show that $a \cdot b^{-1}$ commutes with everything in $G$. Let $g \in G$. Then

\[a \cdot b^{-1} \cdot g = a \cdot (g^{-1} \cdot b)^{-1} = a \cdot (b \cdot g^{-1})^{-1} = a \cdot g \cdot b^{-1} = g \cdot a \cdot b^{-1}.
\]

Therefore, $a \cdot b^{-1} \in Z(G)$, so $Z(G) < G$ by the preceding Lemma.

The union of subgroups is not necessarily a subgroup, but the intersection of subgroups is always a subgroup. Before I prove this, a word about notation.

In this result, I want to talk about a bunch of subgroups of a group $G$. How should I denote these subgroups? I don’t want to write $H_1, H_2, \ldots, H_n$, because I may want an infinite number of subgroups. Well, how about $H_1, H_2, \ldots$ (where I think of the sequence as continuing forever)?

The problem in the second case is that I might not be able to list the subgroups in a sequence. You may know that there are different kinds of “infinity” and some a bigger than others. I’ll discuss this idea later, but suffice it to say that I might have infinitely many subgroups, and so many that they can’t be arranged in a list.

I’ll use notation like $\{H_a\}_{a \in A}$ in situations like these. Each $H_a$ is a subgroup, and $A$ is an index set. In other words, $A$ is an unspecified set whose elements I use to subscript the $H$’s. Since $A$ could be arbitrarily big, this gets around the problems I had with the other notations.

Rather than get into technicalities, I will leave things at that and illustrate by example how you work with these humongous index sets.

\textbf{Lemma.} The intersection of a family of subgroups is a subgroup.

\textbf{Proof.} Let $G$ be a group, and let $\{H_a\}_{a \in A}$ be a family of subgroups of $G$. Let $H = \cap_{a \in A} H_a$. I claim that $H$ is a subgroup of $G$.

First, $1 \in H_a$ for all $a \in A$, because each $H_a$ is a subgroup. Hence, $1 \in \cap_{a \in A} H_a$, and the intersection is nonempty.

Next, let $g, h \in H$. I want to show that $g \cdot h^{-1} \in H$. Since $g, h \in H$, I know $g, h \in H_a$ for all $a$. Then $g \cdot h^{-1} \in H_a$ for all $a$, since each $H_a$ is a subgroup. This implies that $g \cdot h^{-1} \in H$, so $H < G$. 

Here is how I can use the preceding construction. Suppose $G$ is a group, and $S$ is a collection of elements of $G$. $S$ might not be a subgroup of $G$ — it might not contain 1, or it might be missing the inverses of some of its elements — but intuitively I ought to be able to add the “missing elements” and enlarge $S$ to a subgroup.

If you try to say precisely what you need to add to $S$, and how you will add it, you will quickly find yourself tied in knots. Do you add elements one at a time? If you throw in an element, you have to throw in the products of that element with everything else that is there (to ensure closure). If you do this sequentially, how do you know the process actually terminates?
Instead of building up the subgroup from $S$, I'll get at it "from above". Consider the set $S$ of all subgroups $\{H_a\}_{a \in A}$ such that $S \subseteq H_a$. $S$ is nonempty, because $G$ is a subgroup of $G$ and $S \subseteq G$.

Let $H = \cap_{a \in A} H_a$. $H$ is a subgroup of $G$, and $S \subseteq H$. $H$ is the subgroup generated by $S$. It is clearly the smallest subgroup of $G$ containing $S$, in the following sense: If $K$ is a subgroup of $G$ and $S \subseteq K$, then $H < K$.

It's common to write $\langle S \rangle$ for the subgroup generated by $S$. So in case $S = \{x_1, x_2, \ldots, x_n\}$ (a finite set), write $\langle x_1, x_2, \ldots, x_n \rangle$ for the subgroup generated by the $x$'s. In the case of a single element $x \in G$, the subgroup $\langle x \rangle$ generated by $x$ is the cyclic subgroup generated by $x$ that I discussed earlier.

**Example.** Let $G = \mathbb{Z}_6$, the cyclic group of order 6. Then

\[ \langle 2 \rangle = \{0, 2, 4\}, \quad \text{but} \quad \langle 2, 3 \rangle = \mathbb{Z}_6. \]

The first statement is obvious; what about the second?

By definition, $\langle 2, 3 \rangle$ is the smallest subgroup which contains 2 and 3. Since subgroups are closed under addition, $2 + 2 + 3 = 1$ must be in $\langle 2, 3 \rangle$ as well. But I can make any element of $\mathbb{Z}_6$ by adding 1 to itself, so $\langle 2, 3 \rangle$ must contain everything in $\mathbb{Z}_6$ — that is, $\langle 2, 3 \rangle = \mathbb{Z}_6$. \qed

**Example.** Let $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ denote the Cartesian product of $\mathbb{R}$ with itself. Elements of $\mathbb{R}^2$ consist of 2-dimensional vectors, which are added componentwise as usual. With this addition, $\mathbb{R}^2$ becomes a group. It is the set of points in the $x$-$y$ plane.

The sets

\[ A = \{(a, 0) \mid a \in \mathbb{R}\} \quad \text{and} \quad B = \{(0, b) \mid b \in \mathbb{R}\} \]

are subgroups of $\mathbb{R}^2$. (Check it yourself!)

However, the union $A \cup B$ is not a subgroup of $\mathbb{R}^2$. $A \cup B$ is the union of the $x$-axis and the $y$-axis. This set is not a subgroup because it's not closed under addition. For example, $(1, 0) \in A$ and $(0, 1) \in B$, but

\[ (1, 0) + (0, 1) = (1, 1) \not\in A \cup B. \]

This example shows that the union of subgroups need not be a subgroup. \qed