1-16-2018

Subgroups

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

(a) (Closure) H is closed under the group operation: If $a, b \in H$, then $a \cdot b \in H$.

(b) (Identity) $1 \in H$.

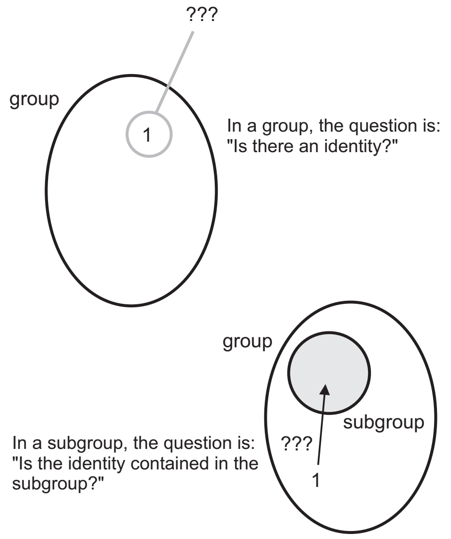
(c) (Inverses) If $a \in H$, then $a^{-1} \in H$.

The notation $H < G$ means that H is a subgroup of G.

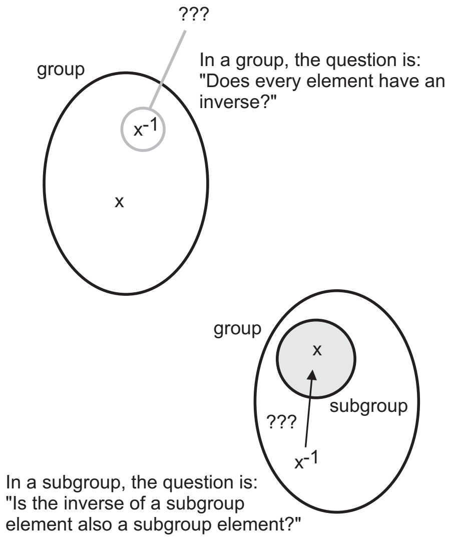
Notice that associativity is *not* part of the definition of a subgroup. Since associativity holds in the group, it holds automatically in any subset.

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 question is whether the identity for the group is actually contained in the subgroup.*


???
group
1
In a group, the question is:
"Is there an identity?"
group
subgroup
In a subgroup, the question is:
"Is the identity contained in the
subgroup?"
???
1

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.


???
group
In a group, the question is: "Does every element have an inverse?"
x^{-1}
x
group
x
subgroup
???
x^{-1}
In a subgroup, the question is: "Is the inverse of a subgroup element also a subgroup element?"

Lemma. Let G be a group. Then $\{1\}$ and G are subgroups of G.

$\{1\}$ is called the **trivial subgroup**.

Proof. The proofs are almost too easy! Consider $\{1\}$. The only possible multiplication is $1 \cdot 1 = 1$, which shows $\{1\}$ is closed.

$\{1\}$ obviously contains the identity 1.

$\{1\}$ is closed under taking inverses, since $1^{-1} = 1$.

The proof that G is a subgroup is equally easy; I'll let you do it. □

Example. (**Subgroups of the integers**) Let $n \in \mathbb{Z}$. Let

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}.$$

Show that $n\mathbb{Z}$ 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 $\mathbb{Z}$.

I'll show later that every subgroup of the integers has the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Notice that $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subgroup of $\mathbb{Z}$. I have $2 \in 2\mathbb{Z}$ and $3 \in 3\mathbb{Z}$, so 2 and 3 are elements of the union $2\mathbb{Z} \cup 3\mathbb{Z}$. But their sum $5 = 2 + 3$ is not an element of $2\mathbb{Z} \cup 3\mathbb{Z}$, because 5 is neither a multiple of 2 nor a multiple of 3.

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

Example. (**A subset that isn't closed under inverses**) $\mathbb{Z}$ is a group under addition. Consider $\mathbb{Z}^{\geq 0}$, the set of nonnegative integers. Check each axiom for a subgroup. If the axiom holds, prove it. If the axiom doesn't hold, give a specific counterexample.

If $m, n \in \mathbb{Z}^{\geq 0}$, then $m \geq 0$ and $n \geq 0$, so $m + n \geq 0$. Therefore, $m + n \in \mathbb{Z}^{\geq 0}$, and the set is closed under addition.

0 is a nonnegative integer, so $0 \in \mathbb{Z}^{\geq 0}$.

However, $3 \in \mathbb{Z}^{\geq 0}$, but the inverse -3 is not an element of $\mathbb{Z}^{\geq 0}$. Therefore, $\mathbb{Z}^{\geq 0}$ is not closed under taking inverses, so it's not a subgroup of $\mathbb{Z}$. □

Example. (**The integers as a subgroup of the rationals**) Show that the set of integers $\mathbb{Z}$ 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 $\mathbb{Q}$. □

Example. (**A subgroup under multiplication**) Let $\mathbb{Q}^*$ be the group of nonzero integers under multiplication. Consider the set

$$H = \left\{ \frac{1}{2^m} \;\middle|\; m \in \mathbb{Z} \right\}.$$

Is H a subgroup of $\mathbb{Q}^*$?

Let $\dfrac{1}{2^m}, \dfrac{1}{2^n} \in H$, where $m, n \in \mathbb{Z}$. Then

$$\frac{1}{2^m} \cdot \frac{1}{2^n} = \frac{1}{2^{m+n}} \in H.$$

Thus, H is closed under multiplication.

The identity of $\mathbb{Q}^*$ is 1, and $1 = \dfrac{1}{2^0} \in H$.

Finally, let $\dfrac{1}{2^m} \in H$. Then $\left(\dfrac{1}{2^m}\right)^{-1} = \dfrac{1}{2^{-m}}$, and $\dfrac{1}{2^{-m}} \in H$. Therefore, H is closed under taking inverses.

Therefore, H is a subgroup of $\mathbb{Q}^*$. □

Example. $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ denotes the set of pairs of integers:

$$\mathbb{Z}^2 = \{(m, n) \mid m, n \in \mathbb{Z}\}.$$

It is a group under "vector addition"; that is,

$$(a, b) + (c, d) = (a + c, b + d).$$

The identity is $(0, 0)$ and the inverse of (m, n) is $-(m, n) = (-m, -n)$.

Taking this for granted, consider the set

$$H = \{(x, y) \mid x + y \geq 0\}.$$

Check each axiom for a subgroup. If the axiom holds, prove it. If the axiom doesn't hold, give a specific counterexample.

In words, an element (x, y) is in H if the sum of its components is nonnegative.

Suppose $(a, b), (c, d) \in H$. This means

$$a + b \geq 0 \quad \text{and} \quad c + d \geq 0.$$

Then

$$(a + c) + (b + d) = (a + b) + (c + d) \geq 0 + 0 = 0.$$

Therefore,

$$(a, b) + (c, d) = (a + c, b + d) \in H.$$

Thus, H is closed under addition.
Since $0 + 0 = 0 \geq 0$, I have $(0, 0) \in H$.
$(1, 2) \in H$, because $1 + 2 = 3 \geq 0$. But $-(1, 2) = (-1, -2) \notin H$, because

$$-1 + (-2) = -3 \ngeq 0.$$

Thus, the inverse axiom fails (so H is not a subgroup). □

Definition. If G is a group and g is an element oϒf 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, $\langle g \rangle$ 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 $\langle g \rangle$ 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 $\langle g \rangle$ a *subgroup*, I'd better verify that it satisfies the subgroup axioms.

Lemma. If G is a group and $g \in G$, then $\langle g \rangle$ 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 $\langle g \rangle$.
Therefore, $\langle g \rangle$ is a subgroup of G. □

In fact, $\langle g \rangle$ is the *smallest* subgroup of G which contains g.

Example. (**Subgroups of a finite cyclic group**) List the elements of the subgroups generated by elements of $\mathbb{Z}_8$.

$$\langle 0 \rangle = \{0\},$$

$$\langle 2 \rangle = \langle 6 \rangle = \{0, 2, 4, 6\},$$

$$\langle 4 \rangle = \{0, 4\},$$

$$\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7\}.$$

The way the subgroups are contained in one another can be pictured in a **subgroup lattice diagram**:

$$\begin{tikzcd}
\langle 1\rangle = \{0,1,2,3,4,5,6,7\} \arrow[d, dash] \\
\langle 2\rangle = \{0,2,4,6\} \arrow[d, dash] \\
\langle 4\rangle = \{0,4\} \arrow[d, dash] \\
\langle 0\rangle = \{0\}
\end{tikzcd}$$

□

The following result is easy, so I'll leave the proof to you. It says that the subgroup relationship is transitive.

Lemma.(**Subgroup transitivity**) If $H < K$ and $K < G$, then $H < G$: A subgroup of a subgroup is a subgroup of the (big) group. □

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, $H < G$. □

Note: In order to use this criterion, *you have to show that the set in question is nonempty* before doing the "$a \cdot b^{-1} \in H$" check. Usually you show the set is nonempty by showing that it contains the identity element. So you really have to do two checks, not just one.

Example. (**A subgroup of a matrix group**) Let $GL(2, \mathbb{R})$ be the set of invertible 2×2 matrices with real entries.

(a) Show that $GL(2, \mathbb{R})$ is a group under matrix multiplication.

(b) Show that the following set is a subgroup of $GL(2, \mathbb{R})$:

$$D = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \,\middle|\, a \in \mathbb{R} \quad \text{and} \quad a \neq 0 \right\}.$$

(a) If $A, B \in GL(2, \mathbb{R})$, then $\det A \neq 0$ and $\det B \neq 0$. Hence,

$$\det(AB) = (\det A)(\det B) \neq 0.$$

Therefore, AB is invertible, so matrix multiplication is a binary operation on $GL(2, \mathbb{R})$. (The point is that the set is *closed* under the operation.)

From linear algebra, I know that matrix multiplication is associative.

The 2×2 identity matrix is invertible, so it's in $GL(2, \mathbb{R})$. It's the identity for $GL(2, \mathbb{R})$ under matrix multiplication.

Finally, if $A \in GL(2, \mathbb{R})$, then A^{-1} exists. It's also an element of $GL(2, \mathbb{R})$, since its inverse is A.

This proves that $GL(2, \mathbb{R})$ is a group under matrix multiplication. $\square$

(b) 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 $GL(2, \mathbb{R})$. $\square$

Definition. 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:

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

Lemma. $Z(G) < G$.

Proof. Suppose $a, b \in Z(G)$. I'll show $ab \in Z(G)$. To do this, I must show that ab commutes with everything in G.

Let $g \in G$. Then

$$\begin{aligned} (ab)g &= a(bg) && \text{(Associativity)} \\ &= a(gb) && \text{(Since } b \in Z(G)) \\ &= (ag)b && \text{(Associativity)} \\ &= (ga)b && \text{(Since } a \in Z(G)) \\ &= g(ab) && \text{(Associativity)} \end{aligned}$$

Therefore, $ab \in Z(G)$

Next, $1 \cdot g = g = g \cdot 1$ for all $g \in G$, so $1 \in Z(G)$.

Finally, let $a \in Z(G)$. I need to show that $a^{-1} \in Z(G)$. Let $g \in G$. I need to show that $ga^{-1} = a^{-1}g$. I have

$$\begin{aligned} ag^{-1} &= g^{-1}a && \text{(Since } a \in Z(G)) \\ (ag^{-1})^{-1} &= (g^{-1}a)^{-1} && \text{(Take inverses of both sides)} \\ (g^{-1})^{-1}a^{-1} &= a^{-1}(g^{-1})^{-1} && \text{(Inverse of a product formula)} \\ ga^{-1} &= a^{-1}g && \text{(Properties of inverses)} \end{aligned}$$

Therefore, $a^{-1} \in Z(G)$.

Hence, $Z(G)$ is a subgroup of G. $\square$

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, ..., H_n, because I may want an infinite number of subgroups. Well, how about H_1, H_2, ... (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. Specifically, if the number of subgroups under consideration is not **countable**, I can't list them as "H_1, H_2, ...".

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 infinite index sets. If the next proof confuses you, try writing out the proof for two subgroups: That is, if H and K are subgroups of a group G, then $H \cap K$ is a subgroup of G.

Lemma. The intersection of a family of subgroups is a subgroup.

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 collection of all subgroups $\{H_a\}_{a \in A}$ such that $S \subset H_a$. The collection is nonempty, because G is a subgroup of G and $S \subset G$.

Let $H = \cap_{a \in A} H_a$. H is a subgroup of G, and $S \subset H$. 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 $S \subset K$, 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. (**Subgroups generated by elements**) Let $G = \mathbb{Z}_6$, the cyclic group of order 6. Show

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

The first statement is easy: $2 + 2 = 4$, $2 + 2 + 2 = 0$.

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 enough times, so $\langle 2, 3 \rangle$ must contain everything in $\mathbb{Z}_6$ — that is, $\langle 2, 3 \rangle = \mathbb{Z}_6$. □

Example. $\mathbb{R}^2$ is a group under vector addition. Give an example of two subgroups $\mathbb{R}^2$ whose union is not a subgroup.

$\mathbb{R}^2$ consists of the points in the x-y-plane, or equivalently 2-dimensional vectors with real components.

Two elements of $\mathbb{R}^2$ are added as 2-dimensional vectors:

$$(a, b) + (c, d) = (a + c, b + d).$$

The following sets are subgroups of $\mathbb{R}^2$:

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

A is the x-axis, and B is the y-axis.

For example, I'll verify that A is a subgroup of $\mathbb{R}^2$. It's closed under addition: If $(a_1, 0), (a_2, 0) \in A$, then

$$(a_1, 0) + (a_2, 0) = (a_1 + a_2, 0) \in A.$$

The identity for $\mathbb{R}^2$ is $(0, 0)$, which is contained in A.

If $(a, 0) \in A$, then

$$-(a, 0) = (-a, 0) \in A.$$

Try writing out the proof for B 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

$$(1, 0) + (0, 1) = (1, 1) \notin A \cup B.$$

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