9-9-1993

Subgroups.

Examples. 1. 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 $\mathbb{Z}_4$. $\square$

2. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, 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.) $\square$

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.

Examples. 0. $\{1\}$ and G are always subgroups of G. $\square$

1. Let $n \in \mathbb{Z}$. Then

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

Note, however, that $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subgroup of $\mathbb{Z}$, since it isn't closed under addition. The union of subgroups need not be a subgroup. $\square$

2. If $H < K$ and $K < G$, then $H < G$. $\square$

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. 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, $H < G$. $\square$

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 $Z(G) < G$.

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.

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 set S of all subgroups $\{H_a\}_{a \in A}$ such that $S \subset H_a$. S 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.

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

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