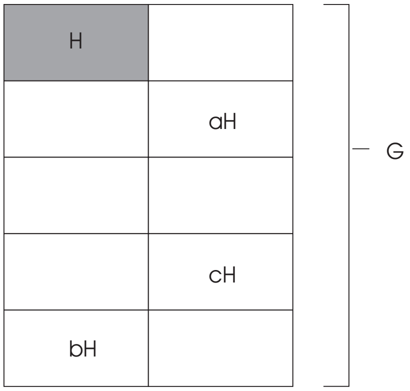
3-17-2018

Cosets

If H is a subgroup of G, you can break G up into pieces, each of which looks like H:



These pieces are called **cosets** of H, and they arise by "multiplying" H by elements of G.

Definition. Let G be a group and let $H < G$. A **left coset** of H in G is a subset of the form

$$gH = \{gh \mid h \in H\} \quad \text{for some} \quad g \in G.$$

The element g is a **representative** of the coset gH. The collection of left cosets is denoted G/H.

Likewise, a **right coset** is a subset of the form

$$Hg = \{hg \mid h \in H\} \quad \text{for some} \quad g \in G.$$

The set of right cosets is denoted $H\backslash G$.

Thus, the left coset gH consists of g times everything in H; Hg consists of everything in H times g.

I've written everything as if the operation in the group was "multiplication". The case when the operation is "addition" is discussed in an example below.

Example. (**Listing the elements of cosets**) (a) List the elements of U_{28} and the elements of the cyclic subgroup generated by 9.

(b) List the elements of the cosets of $\langle 9 \rangle$ in U_{28}.

(a)

$$U_{28} = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}.$$

$$\langle 9 \rangle = \{1, 9, 25\}. \quad \Box$$

(b) The subgroup is always a coset. I'll list that first:

$$\langle 9 \rangle = \{1, 9, 25\}.$$

Take an element of U_{28} which is not in the subgroup — say 3. Multiply the subgroup by the element:

$$3 \cdot \langle 9 \rangle = 3 \cdot \{1, 9, 25\} = \{3 \cdot 1, 3 \cdot 9, 3 \cdot 25\} = \{3, 27, 19\}.$$

Take an element of U_{28} which is not in either of the two known cosets — say 5. Multiply the subgroup by the element:

$$5 \cdot \langle 9 \rangle = 5 \cdot \{1, 9, 25\} = \{5 \cdot 1, 5 \cdot 9, 5 \cdot 25\} = \{5, 17, 13\}.$$

Notice that all the cosets have 3 elements — the same as the number of elements in the subgroup.

At this point, there are only 3 elements which aren't in any of the known cosets. These elements make up the last coset: $\{11, 15, 23\}$. You can check that

$$11 \cdot \langle 9 \rangle = \{11, 15, 23\}.$$

3 represents the coset $3 \cdot \langle 9 \rangle$, but a given coset can be represented by *any* of its elements. For example,

$$19 \cdot \langle 9 \rangle = 19 \cdot \{1, 9, 25\} = \{19 \cdot 1, 19 \cdot 9, 19 \cdot 25\} = \{19, 3, 27\} = 3 \cdot \langle 9 \rangle. \quad \square$$

Example. (**Listing the elements of cosets**) List the elements of the cosets of $2\mathbb{Z}$ in $\mathbb{Z}$.

$\mathbb{Z}/2\mathbb{Z}$ consists of two cosets: the even numbers $2\mathbb{Z}$ and the odd numbers. Explicitly,

$$0 + 2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} \quad \text{and} \quad 1 + 2\mathbb{Z} = \{\ldots, -3, -1, 1, 3, \ldots\}.$$

Notice that when the operation in the group is $+$, a coset of a subgroup H is written $a + H$. □

Example. (**Listing the elements of cosets**) List the elements of the cosets of the subgroup $\{1, -1\}$ of the group of quaternions.

Here is the table for the group of quaternions:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Consider the subgroup $\{1, -1\}$. Its cosets are

$$1 \cdot \{1, -1\} = \{1, -1\}, \quad (-1) \cdot \{1, -1\} = \{-1, 1\} = \{1, -1\},$$

$$i \cdot \{1, -1\} = \{i, -i\}, \quad (-i) \cdot \{1, -1\} = \{-i, i\} = \{i, -i\},$$
$$j \cdot \{1, -1\} = \{j, -j\}, \quad (-j) \cdot \{1, -1\} = \{-j, j\} = \{j, -j\},$$
$$k \cdot \{1, -1\} = \{k, -k\}, \quad (-k) \cdot \{1, -1\} = \{-k, k\} = \{k, -k\}.$$

There are four distinct cosets. Notice that $2 \cdot 4 = 8$. This is a special case of **Lagrange's theorem**: The order of a subgroup times the number of cosets of the subgroup equals the order of the group. □

Example. (**Identifying a set of cosets with another set**) Show that the set of cosets $\mathbb{R}/\mathbb{Z}$ can be identified with S^1, the group of complex numbers of modulus 1 under complex multiplication.

The cosets $\mathbb{R}/\mathbb{Z}$ are

$$x + \mathbb{Z} \quad \text{where} \quad 0 \le x < 1.$$

Thus, there is one coset for each number in the half-open interval $[0, 1)$.

On the other hand, you can "wrap" the half-open interval around the circle S^1 in the complex plane: Use $f(t) = e^{2\pi i t}$, $0 \le t < 1$. It's easy to show this is a bijection by constructing an inverse using the logarithm.

Thus, there is a bijection from the set of cosets $\mathbb{R}/\mathbb{Z}$ to the circle S^1.

In fact, this is an example of an **isomorphism** of groups. $\square$

Theorem. Let G be a group and let $H < G$. The left cosets of H in G form a partition of G.

Proof. I need to show that the union of the left cosets is the whole group, and that different cosets do not overlap.

Let $g \in G$. Since $1 \in H$, it follows that $g \cdot 1 = g$ is in gH. This shows that every element of G lies in some coset of H, so the union of the cosets is all of G.

Next, suppose aH and bH are two cosets of H, and suppose they are not disjoint. I must show they're identical: $aH = bH$. As usual, I can show two sets are equal by showing that each is contained in the other.

Since aH and bH are not disjoint, I can find an element $g \in aH \cap bH$. Write $g = ah_1 = bh_2$ for $h_1, h_2 \in H$. Then

$$a = bh_2h_1^{-1}.$$

Now let $ah \in aH$. Then

$$ah = bh_2h_1^{-1}h.$$

The element on the right is in bH, since it is b times something in H. Therefore, $ah \in bH$, and $aH \subset bH$. By symmetry, $bH \subset aH$, so $aH = bH$. $\square$

Theorem. Any two left cosets have the same number of elements.

Proof. Let H be a subgroup of a group G, and let $a, b \in G$. I must show that aH and bH have the same number of elements. *By definition*, this means that I must construct a bijective map from aH to bH.

An element of aH looks like ah, for some $h \in H$. So it is tempting to simply define $f : aH \to bH$ by

$$f(ah) = bh.$$

But how do you know this is *well-defined*? How do you know that the *same element* of aH might not be expressed as both ah and ah', where h and h' are *different* elements of H?

Fortunately, this can't happen; if $ah = ah'$, then

$$a^{-1}ah = a^{-1}ah', \qquad \text{so} \qquad h = h'.$$

Thus, it's legitimate for me to define a function f as above.

Likewise, I can define $g : bH \to aH$ by

$$g(bh) = ah \quad \text{for} \quad bh \in bH.$$

This is well-defined, just as f was.

Since f and g are clearly inverses, f (or g) is a bijection, and aH and bH have the same number of elements. $\square$

Definition. If G is a group and $H < G$, $|G/H|$ is called the **index** of H in G, and is denoted $(G : H)$.

The way I've defined it, the index of H in G is the number of *left* cosets of H. It turns out that this is the same as the number of right cosets.

Theorem. (**Lagrange's theorem**) Let G be a finite group and let H be a subgroup of G. Then

$$(G : H) = \frac{|G|}{|H|}.$$

Proof. The cosets of H partition G into $(G : H)$ pieces, and each piece contains $|H|$ elements. So the total number of elements in the $(G : H)$ pieces is $(G : H) \cdot |H|$, but this is all of G:

$$(G : H) \cdot |H| = |G|.$$

Now divide both sides by $|H|$. □

Note that this result implies that *the order of a subgroup divides the order of the group*. Thus, a group of order 14 *could* have subgroups of order 1, 2, 7, or 14, but *could not* have a subgroup of order 5.

Example. (**A specific example of Lagrange's theorem**) Verify Lagrange's theorem for the subgroup $H = \{0, 3\}$ of $\mathbb{Z}_6$.

The cosets are

$$0 + H = \{0, 3\}, \quad 1 + H = \{1, 4\}, \quad 2 + H = \{2, 5\}.$$

Notice there are 3 cosets, each containing 2 elements, and that the cosets form a partition of the group. □

Example. (**A specific example of Lagrange's theorem**) List the elements of the cosets of $\langle (2, 2) \rangle$ in $\mathbb{Z}_4 \times \mathbb{Z}_6$.

First, list the elements of the subgroup:

$$\langle (2, 2) \rangle = \{(0, 0), (2, 2), (0, 4), (2, 0), (0, 2), (2, 4)\}.$$

The subgroup is a coset.
The subgroup has 6 elements and the group has 24. By Lagrange's theorem, there are 4 cosets.
$(1, 1)$ isn't in the subgroup; add it to the subgroup:

$$(1, 1) + \langle (2, 2) \rangle = \{(1, 1), (3, 3), (1, 5), (3, 1), (1, 3), (3, 5)\}.$$

$(2, 1)$ isn't in either of the known cosets; add it to the subgroup:

$$(2, 1) + \langle (2, 2) \rangle = \{(2, 1), (0, 3), (2, 5), (0, 1), (2, 3), (0, 5)\}.$$

The remaining elements make up the fourth coset. I can find them by noting that $(1, 2)$ isn't in the three known cosets, so the fourth coset is represented by $(1, 2)$:

$$(1, 2) + \langle (2, 2) \rangle = \{(1, 2), (3, 4), (1, 0), (3, 2), (1, 4), (3, 0)\}.$$

Notice that there are 4 cosets, each containing 6 elements, and the cosets form a partition of the group. □

Corollary. Every group of prime order is cyclic.

Proof. Suppose G is a group of order p, where p is prime. Let $g \in G$, $g \neq 1$. $\langle g \rangle$ is a subgroup of G, and since $g \neq 1$, $|\langle g \rangle| \neq 1$.

But $|\langle g\rangle|$ divides $|G|$ by Lagrange's theorem, and the only positive numbers which divide $|G| = p$ are 1 and p. Therefore, $|\langle g\rangle| = p$, which means that $\langle g\rangle$ is all of G. That is, G is cyclic with generator g. □

For example, this means that the only group of order 17 is the cyclic group of order 17.

I noted earlier that the number of left cosets equals the number of right cosets; here's the proof.

Proposition. Let G be a group, $H < G$. The set of left cosets G/H may be put in 1-1 correspondence with the set of right cosets $H\backslash G$.

Proof. Define $\phi : G/H \to H\backslash G$ by $\phi(gH) = Hg^{-1}$. I need to show ϕ is well-defined.

Suppose $aH = bH$. Then $a = a \cdot 1 \in aH = bH$, so $a = bh$ for some $h \in H$. Then

$$\phi(aH) = Ha^{-1} = H(bh)^{-1} = Hh^{-1}b^{-1} = Hb^{-1} = \phi(bH).$$

Next, define $\psi : H\backslash G \to G/H$ by $\psi(Hg) = g^{-1}H$. A computation similar to the one I just did shows ψ is well-defined. ϕ and ψ are inverses, so either one gives a bijection of G/H with $H\backslash G$. □

While there are the same *number* of left and right cosets, the left and right cosets may be different as sets. In fact, if the left and right cosets are the same as sets, the subgroup is said to be **normal**. It's a very important condition on a subgroup, since it will allow us to turn the set of left (or right) cosets into a **quotient group**.

Example. (**A subgroup whose left and right cosets are different**) List the elements of the left cosets and the right cosets of the subgroup $\{\text{id}, (1\ 2)\}$ of S_3.

The left cosets are

$$\{\text{id}, (1\ 2)\}, \quad (1\ 3)\{\text{id}, (1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\}, \quad (2\ 3)\{\text{id}, (1\ 2)\} = \{(2\ 3), (1\ 3\ 2)\}.$$

The right cosets are

$$\{\text{id}, (1\ 2)\}, \quad \{\text{id}, (1\ 2)\}(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}, \quad \{\text{id}, (1\ 2)\}(2\ 3) = \{(2\ 3), (1\ 2\ 3)\}.$$

The left and right cosets aren't the same, though there are the same number of left and right cosets. □
