9-20-1993

Subgroups and Cosets.

Example. Let G be a group, and let $g \in G$. Consider the set of all powers of g:

$$\langle g \rangle = \{g^n | n \in \mathbb{Z}\}.$$

This set is a subgroup of G, the **subgroup generated by** g.

The identity is in $\langle g \rangle$, since $1 = g^0$. The set is closed under multiplication, since $g^m g^n = g^{m+n}$. Finally, since $(g^n)^{-1} = g^{-n}$, the set is closed under taking inverses.

$\langle g \rangle$ is the smallest subgroup of G containing g, in the sense in which we used this phrase earlier. To see this, suppose H is a subgroup of G containing g. Then since H is closed under multiplication and inverses, H must contain each power g^n, for $n \in \mathbb{Z}$ — that is, $\langle g \rangle \subset H$. Therefore, $\langle g \rangle$ is contained in every subgroup which contains g.

It's also important to note that $\langle g \rangle$ can be either finite or infinite. Obviously if G is finite and $g \in G$, then $\langle g \rangle$ is finite. On the other hand, take $G = \mathbb{Z}$ with addition as the group law and look at $2 \in \mathbb{Z}$. In additive notation, powers become multiples, so $\langle 2 \rangle = 2\mathbb{Z}$. Obviously, this subgroup is infinite. $\square$

Example. This is the operation table for V_4, the **Klein 4-group**.

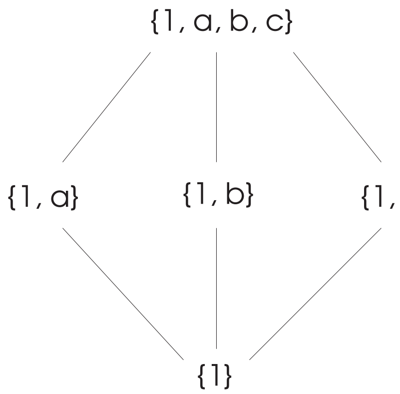
	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

There is one subgroup of order 1, namely $\{1\}$. There are three subgroups of order 2: $\{1, a\}$, $\{1, b\}$, $\{1, c\}$.

There are no subgroups of order 3. Such a subgroup must contain 1 and two of a, b, c. But two of a, b, c multiply to the third, so the subgroup would be forced to contain a fourth element by closure.

The only subgroup of order 4 is the whole group.

Here is a picture of the subgroups of V_4, arranged in a **subgroup lattice**. The lines denote the inclusion of a subgroup in another.



$\square$

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

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

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

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

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 $1 \in H$, $g \cdot 1 = g$ 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 $aH = bH$. □

Notation. The set of left cosets of H in G is denoted G/H. The set of right cosets of H in G is denoted $H\backslash G$.

Examples.

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

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

2. Consider the subgroup $H = \{0, 3\}$ of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. The cosets are

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

Notice that, e.g., $4 + h = \{4, 1\} = 1 + H$. There are three distinct cosets.

It is no coincidence that the number of cosets (3) times the order of the subgroup (2) equals the order of the group (6). This is true in general. □

3. $\mathbb{R}/\mathbb{Z} = S^1$, the circle group. Specifically, the cosets are

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

But there's an obvious way to wrap the half-open interval around the circle 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 — construct an inverse using the logarithm.

In fact, this is an example of an **isomorphism**. □

Lemma. Let G be a group, and let H be a subgroup of G. The following statements are equivalent:

1. a and b are elements of the same coset of H.

2. aH = bH.

3. $b^{-1}a \in H$.

Proof. To show that several statements are equivalent, I must show that any one of them follows from any other. To do this efficiently, I'll show that statement 1 implies statement 2, statement 2 implies statement 3, and statement 3 implies statement 1.

($1 \Rightarrow 2$) Suppose a and b are elements of the same coset gH of H. Since $a \in aH \cap gH$, and since cosets are either disjoint or identical, $aH = gH$. Likewise, $b \in bH \cap gH$ implies $bH = gH$. Therefore, $aH = bH$.

($2 \Rightarrow 3$) Suppose $aH = bH$. Since $1 \in H$, it follows that $a = a \cdot 1 \in aH = bH$. Therefore, $a = bh$ for some $h \in H$. Hence, $b^{-1}a = h \in H$.

($3 \Rightarrow 1$) Suppose $b^{-1}a = h \in H$. Then $b^{-1}aH = hH = H$, so $aH = bH$. Therefore, a and b are elements of the same coset of H, namely $aH = bH$. □

Example. Consider D_4, the group of symmetries of a square.

	id	r_1	r_2	r_3	m_+	m_-	m_x	m_y
id	id	r_1	r_2	r_3	m_+	m_-	m_x	m_y
r_1	r_1	r_2	r_3	id	m_y	m_x	m_+	m_-
r_2	r_2	r_3	id	r_1	m_-	m_+	m_y	m_x
r_3	r_3	id	r_1	r_2	m_x	m_y	m_-	m_+
m_+	m_+	m_x	m_-	m_y	id	r_2	r_1	r_3
m_-	m_-	m_y	m_+	m_x	r_2	id	r_3	r_1
m_x	m_x	m_-	m_y	m_+	r_3	r_1	id	r_2
m_y	m_y	m_+	m_x	m_-	r_1	r_3	r_2	id

The left cosets of the subgroup $\{\mathrm{id}, r_1\}$ are

$$\{\mathrm{id}, r_1\}, r_2\{\mathrm{id}, r_1\} = \{r_2, r_3\}, m_+\{\mathrm{id}, r_1\} = \{m_+, m_x\}, m_-\{\mathrm{id}, r_1\} = \{m_-, m_y\}.$$

The right cosets of $\{\mathrm{id}, r_1\}$ are

$$\{\mathrm{id}, r_1\}, \{\mathrm{id}, r_1\}r_2 = \{r_2, r_3\}, \{\mathrm{id}, r_1\}m_+ = \{m_+, m_y\}, \{\mathrm{id}, r_1\}m_- = \{m_-, m_x\}.$$

Notice that the left and right cosets are not the same.
On the other hand, the left cosets of the subgroup $\{\mathrm{id}, r_1, r_2, r_3\}$ are

$$\{\mathrm{id}, r_1, r_2, r_3\}, m_+\{\mathrm{id}, r_1, r_2, r_3\} = \{m_+, m_x, m_-, m_y\}.$$

The right cosets are

$$\{\mathrm{id}, r_1, r_2, r_3\}, \{\mathrm{id}, r_1, r_2, r_3\}m_+ = \{m_+, m_x, m_-, m_y\}.$$

In this case, the left and right cosets coincide. □

Lemma. Let H be a subgroup of G. Any two cosets of H may be put in 1-1 correspondence.

Proof. It suffices to show that a coset gH may be put in 1-1 correspondence with H. The map $\phi : H \to gH$ given by $h \mapsto gh$ has the map $\psi : gH \to H$ given by $gh \mapsto g^{-1}gh = h$ as its inverse. Hence, ϕ is a bijection. □

Notation. If S is a set, $|S|$ denotes the cardinality of S. (For now, I'll ignore the infinite case and observe that $|S|$ is the number of elements in S if S is finite.)

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

$$|G| = |G/H||H|.$$

Proof. The cosets G/H of H partition G, and each coset has the same number of elements as H. The result follows immediately. $\square$

Definition. Let G be a group, and let $g \in G$. The **order** of g is the smallest positive integer n such that $g^n = 1$. If there is no such n, g has **infinite order**. $o(g)$ denotes the order of g.

Corollary. Let G be a finite group, and let $g \in G$. Then $o(g) \mid |G|$.

Proof. Apply Lagrange's theorem with $H = \langle g \rangle$. $\square$

Example. The group of symmetries of a triangle D_3 has order 6, and all the nontrivial elements have order 2 or order 3. (The rotations have order 3 and the reflections have order 2.) Note that there is no element of order 6. Therefore, if $n \mid |G|$, it does not follow that there is an element of order n. $\square$

Example. Let p be prime. Consider the cyclic group $\mathbb{Z}_p$. Then every nontrivial element $k \in \mathbb{Z}_p$ must generate $\mathbf{Z}_p$, in the sense that $\langle k \rangle = \mathbb{Z}_p$. To see this, observe that $\langle k \rangle$ must have order dividing p, so if $k \neq 1$, the order must be p. This shows, in fact, that $\mathbb{Z}_p$ has no proper nontrivial subgroups. $\square$