Cosets and Lagrange's Theorem

Our current goal is to generalize the Fundamental Theorem for Cyclic Groups, which said that a cyclic group of order $|G| = n$ has a single subgroup of order $|H| = d$ for each divisor d of n. This statement has three parts.

1. Order of subgroups divides order of cyclic groups.
2. There **exists** a subgroup with $|H| = d$ for each divisor d of $|G|$.
   (In particular, there is an **element** of order d for each divisor.)
3. There is **only one** such H.

Generalizing the first of these to all groups is done by **Lagrange's Theorem**, proven using **cosets**.

Definition. For each $\boldsymbol{g} \in G$, a subgroup $H < G$ has

left coset $\boldsymbol{g}H = \{\boldsymbol{g}h \mid h \in H\}$ and **right coset** $H\boldsymbol{g} = \{h\boldsymbol{g} \mid h \in H\}$

We'll usually focus on **left** cosets. If we say just "coset" then we mean "**left** coset".

Remark. Sometimes in set theory people say "co-set" to mean "complementary set" (i.e. everything other than the set). **This is different!** Our "coset" is more like a "parallel set".

Example. In $\mathbb{Z}_6$ consider the subgroup $\langle 3\rangle = \{0, 3\}$. This has the following (three) cosets.

- $\mathbf{0} + \langle 3\rangle = \{\mathbf{0}, 3\}$
- $\mathbf{1} + \langle 3\rangle = \{\mathbf{1}, 4\}$
- $\mathbf{2} + \langle 3\rangle = \{\mathbf{2}, 5\}$
- $\mathbf{3} + \langle 3\rangle = \{\mathbf{3}, 0\} = 0 + \langle 3\rangle$
- $\mathbf{4} + \langle 3\rangle = \{\mathbf{4}, 1\} = 1 + \langle 3\rangle$
- $\mathbf{5} + \langle 3\rangle = \{\mathbf{5}, 2\} = 2 + \langle 3\rangle$

Example. In $\mathbb{Z}_6$ consider the subgroup $\langle 2\rangle = \{0, 2, 4\}$. This has the following (two) cosets.

- $\mathbf{0} + \langle 2\rangle = \{\mathbf{0}, 2, 4\}$
- $\mathbf{1} + \langle 2\rangle = \{\mathbf{1}, 3, 5\}$
- $\mathbf{2} + \langle 2\rangle = \{\mathbf{2}, 4, 0\} = 0 + \langle 3\rangle$
- $\mathbf{3} + \langle 2\rangle = \{\mathbf{3}, 5, 1\} = 1 + \langle 3\rangle$
- $\mathbf{4} + \langle 2\rangle = \{\mathbf{4}, 0, 2\} = 0 + \langle 3\rangle$
- $\mathbf{5} + \langle 2\rangle = \{\mathbf{5}, 3, 1\} = 1 + \langle 3\rangle$

Example. In S_3 consider the subgroup $\langle(1\ 2)\rangle = \{(1),\ (1\ 2)\}$. This has the following (three) cosets.

- $\mathbf{(1)}\ \langle(1\ 2)\rangle = \{\ \mathbf{(1)},\ \ (1\ 2)\}$
- $\mathbf{(1\ 3)}\ \langle(1\ 2)\rangle = \{\mathbf{(1\ 3)},\ (1\ 2\ 3)\}$
- $\mathbf{(2\ 3)}\ \langle(1\ 2)\rangle = \{\mathbf{(2\ 3)},\ (1\ 3\ 2)\}$
- $\mathbf{(1\ 2)}\ \langle(1\ 2)\rangle = \{\ \mathbf{(1\ 2)},\ \ (1)\}$
- $\mathbf{(1\ 2\ 3)}\ \langle(1\ 2)\rangle = \{\mathbf{(1\ 2\ 3)},\ (1\ 3)\}$
- $\mathbf{(1\ 3\ 2)}\ \langle(1\ 2)\rangle = \{\mathbf{(1\ 3\ 2)},\ (2\ 3)\}$

Example. In S_3 consider the subgroup $\langle(1\ 2\ 3)\rangle = \{(1),\ (1\ 2\ 3),\ (1\ 3\ 2)\}$. This has the following two cosets.

- $\mathbf{(1)}\ \langle(1\ 2\ 3)\rangle = \{\ \mathbf{(1)},\ (1\ 2\ 3),\ (1\ 3\ 2)\} = \mathbf{(1\ 2\ 3)}\ \langle(1\ 2\ 3)\rangle = \mathbf{(1\ 3\ 2)}\ \langle(1\ 2\ 3)\rangle$
- $\mathbf{(1\ 2)}\ \langle(1\ 2\ 3)\rangle = \{\mathbf{(1\ 2)},\ \ (2\ 3),\ \ (1\ 3)\} = \mathbf{(2\ 3)}\ \langle(1\ 2\ 3)\rangle = \mathbf{(1\ 3)}\ \langle(1\ 2\ 3)\rangle$

Example. In $\mathbb{Z}$ consider the subgroup $4\mathbb{Z} = \{\dots, -4, 0, 4, 8, \dots\}$. This has the following four cosets.

- $\mathbf{0} + 4\mathbb{Z} = \{\dots, -4, \mathbf{0}, 4,\ 8, \dots\} = \mathbf{4} + 4\mathbb{Z} = \mathbf{8} + 4\mathbb{Z} = \cdots$
- $\mathbf{1} + 4\mathbb{Z} = \{\dots, -3, \mathbf{1}, 5,\ 9, \dots\} = \mathbf{5} + 4\mathbb{Z} = \mathbf{9} + 4\mathbb{Z} = \cdots$
- $\mathbf{2} + 4\mathbb{Z} = \{\dots, -2, \mathbf{2}, 6, 10, \dots\} = \mathbf{6} + 4\mathbb{Z} = \mathbf{10} + 4\mathbb{Z} = \cdots$
- $\mathbf{3} + 4\mathbb{Z} = \{\dots, -1, \mathbf{3}, 7, 11, \dots\} = \mathbf{7} + 4\mathbb{Z} = \mathbf{11} + 4\mathbb{Z} = \cdots$

Note. (Nontrivial) **cosets are not subgroups!!!**

Looking at these examples, we can deduce some basic properties of cosets. **Class presentations!**

Proposition. *$gH = H$ if and only if $g \in H$.*

Proof sketch. H is a subgroup. □

Proposition. *$aH = bH$ if and only if $a \in bH$.*

Proof sketch. If $a = bh$ then $aH \subset bH$. Also $ah^{-1} = b$, so $b \in aH$ and thus $bH \subset aH$. □

Proposition. *$aH = bH$ if and only if $aH \cap bH \neq \emptyset$.*

Proof sketch. If $ah_1 = bh_2$ then $a = bh_2h_1^{-1} \in bH$. □

Proposition. *$aH = bH$ if and only if $a^{-1}b \in H$.*

Proof sketch. If $a^{-1}b = h$ then $b = ah \in aH$. □

Remark. Left cosets are usually not right cosets... But we can say a bit about this relationship.

Proposition. *$aH = bH$ if and only if $Ha^{-1} = Hb^{-1}$.*

Proof. Consider the following string of equivalent statements.

$$\begin{aligned} aH &= bH \\ ah_1 &= bh_2 \\ (ah_1)^{-1} &= (bh_2)^{-1} \\ h_1^{-1}a^{-1} &= h_2^{-1}b^{-1} \\ Ha^{-1} &= Hb^{-1} \end{aligned}$$

□

Corollary. *The number of left cosets = number of right cosets.*

Using essentially the same argument we can show the following.

Proposition. *Numbers of elements also match: $|gH| = |Hg|$.*

We'll look again at when left and right cosets are equal when we discuss **normal subgroups**.

Let's get down to business! We want to show that orders of subgroups divide orders of groups. This generalizes the first part of the Fundamental Theorem of Cyclic Groups. I'll present a slick proof which does not rely on your class presentations.

Proposition. *Cosets are equivalence classes for an equivalence relation: $a \sim b$ if $a = bh$ for some $h \in H$.*

Proof outline. Show reflexive, symmetric, and transitive. □

Corollary. *Cosets partition their group G.*

Proof. Equivalence classes always partition their set. □

Proposition. *All cosets have the same order $|gH| = |H|$.*

Proof. The left multiplication map, $\lambda_g : H \to gH$ has inverse $\lambda_{g^{-1}}$ so it is a bijection. □

Theorem [Lagrange]. *The order of a subgroup divides the order of its group.*

Proof. G is partitioned by cosets of H, which all have order $|H|$. So $|G| = |H| + \cdots + |H| = m\,|H|$. □

Definition. The **index** of a subgroup H in a group G is $[G : H] = \dfrac{|G|}{|H|}$ = "number of cosets of H in G".

Lagrange's Theorem has a number of immediate implications.

Corollary. *For any element of any group, $|g|$ divides $|G|$.*

Proof. $|g| = |\langle g\rangle|$ and $\langle g\rangle$ is a subgroup of G. $\square$

Corollary. *For any element of any group, $g^n = e$ for $n = |G|$.*

Proof. $n = m\,|g|$, so $g^n = g^{m\,|g|} = \left(g^{|g|}\right)^m = (e)^m = e$. $\square$

Corollary (Fermat's Little Theorem). *For any integer n and prime p, we have $n^p \equiv n \pmod p$*

Proof sketch. If n and p are relatively prime, then n generates $\mathbb{Z}_p^{\neq 0}$ multiplicatively. But $\left|\mathbb{Z}_p^{\neq 0}\right| = p-1$. $\square$

Example. We use Fermat's Little Theorem to compute $5^{15} \pmod 7$ as follows.

$$5^{15} \;=\; 5^7\cdot 5^7\cdot 5 \;\equiv\; 5\cdot 5\cdot 5 \;=\; 5\cdot 25 \;\equiv\; 5\cdot 4 \;=\; 20 \;\equiv\; 6 \pmod 7$$

Example. We use Fermat's Little Theorem to compute $7^{13} \pmod{11}$ as follows.

$$7^{13} \;=\; 7^{11}\cdot 7^2 \;\equiv\; 7\cdot 49 \;\equiv\; 7\cdot 5 \;=\; 35 \;\equiv\; 2 \pmod{11}$$

Corollary. *If G has finite prime order, then G is cyclic!*

Proof. If $|G|$ has no divisors, then all elements $g \neq e$ must have order $|G|$. Thus $G = \langle g\rangle$ for any $g \neq e$. $\square$

Corollary. *If $K < H < G$ then $[G:K] = [G:H]\cdot[H:K]$.*

The third part of the Fundamental Theorem of Cyclic Groups was about **counting** the **number** of subgroups of a given order (only 1 for cyclic groups). This is a bit tricky for general groups, but there is a standard tool for getting an upper bound on the number of subgroups with a given order.

Definition. Given subgroups $H, K < G$ the **product set** is $HK = \{hk \in G \mid h \in H,\ k \in K\}$.

Note. This is not a group! This is only a set! But we can still use it for counting elements, since $HK \subset G$.

Proposition [Product Formula]. *The following relationship holds among orders of sets.*

$$|HK|\cdot|H\cap K| = |H|\cdot|K|$$

Proof. Given an $hk \in HK$, every element $x \in H\cap K$ gives a different alternate expression $hk = (hx)(x^{-1}k)$ as a product of $hx \in H$ and $x^{-1}k \in K$. So $|HK|\cdot|H\cap K| \leq |H|\cdot|K|$.

These account for all such rewritings since $h_1k_1 = h_2k_2$ implies $h_2^{-1}h_1 = k_2k_1^{-1} = x \in H\cap K$ such that $h_1k_1 = (h_2x)(x^{-1}k_2)$. So $|HK|\cdot|H\cap K| = |H|\cdot|K|$. $\square$

Corollary. *If H and K are subgroups of G then* $\dfrac{|H|\cdot|K|}{|H\cap K|} = |HK| \leq |G|$

We can use this to show **non-existence** of certain subgroups.

Example. A group of order $|G| = n\,p^m$ where p is prime and $n < p$ has at most one subgroup of order p^m.

Proof. If H, K were both subgroups of order p^m then $|H\cap K| \leq p^{m-1}$ ($H\cap K < H$ so order divides p^m). So

$$|G| \;\geq\; |HK| \;=\; \frac{|H|\cdot|K|}{|H\cap K|} \;\geq\; \frac{p^m\,p^m}{p^{m-1}} \;=\; p\,p^m$$

But $|G| = n\,p^m < p\,p^m$. $\square$

Example. If $H < G$ where $|H| = 25$ and $|G| = 100$, then any element $g \in G$ with order 5 must be in H.

Proof. If not, then $H \cap \langle g \rangle = \{e\}$. In this case

$$|G| \;\geq\; |H\langle g \rangle| \;=\; \frac{|H| \cdot |\langle g \rangle|}{|H \cap \langle g \rangle|} \;=\; \frac{25 \cdot 5}{1} \;=\; 125 \;>\; 100$$

□

The second part of the Fundamental Theorem of Cyclic Groups was about **existence**. In cyclic groups, for every divisor of $|G|$ there was a subgroup; however, for general groups this is **NOT TRUE**!

Example. The alternating group A_4 has order $|A_4| = \frac{4!}{2} = 12$... but it has **no** subgroup of order 6.

Proof sketch. First show that any subgroup of index 2 must be **normal**, that is $gH = Hg$ for all $g \in G$ (apply fact that $gH = H$ if and only if $g \in H$). In particular, $gHg^{-1} = H$ for all $g \in G$.

The problem is that there are too many 3-cycles in A_4! There are 8 in all: $(1\ 2\ 3)$ and $(1\ 3\ 2)$ fixing 4, and 6 others fixing 1, 2, or 3. If H has order 6, then it contains at least one of these. Applying $gHg^{-1} = H$ then immediately yields five more. But that means $|H| \geq 7$. □

As far as existence of subgroups goes, we can say the following. (We won't prove these theorems until near the end of the semester.)

Theorem [Cauchy]. *There is an element $g \in G$ with order p for every **prime** divisor p of $|G|$.*

Corollary. *In particular, there is a (cyclic) subgroup $\langle g \rangle$ of order p for each **prime** divisor p of $|G|$.*

Theorem [Sylow 1]. *There is a subgroup of order p^k where p^k is the highest power of p dividing $|G|$.*

We could prove Cauchy's Theorem at this point using "orbit / stabilizer" counts, which is very similar to the coset idea we just discussed.

Definition. Given a permutation group $G < S_X$ define the **orbit** of $x \in X$ to be $\mathrm{orbit}_G(x) = \{\sigma(x) \mid \sigma \in G\}$.

Definition. Given $G < S_X$ define the **stabilizer subgroup** of $x \in X$ to be $\mathrm{stab}_G(x) = \{\sigma \in G \mid \sigma(x) = x\}$.

Theorem [Orbit-Stabilizer]. *In this situation $|G| = |\mathrm{orbit}_G(x)| \cdot |\mathrm{stab}_G(x)|$*