Chapter 6 Cosets and Lagrange's Theorem.

Cosets.

Suppose that G is a group and H is a subgroup of G.

Definition: The left coset of H with representative g is the set

$$gH = \{gh \mid h \in H\}.$$

The right coset of H with representative g is

$$Hg = \{hg \mid h \in H\}.$$

Example: Consider the group S_3 of permutations of $\{1,2,3\}$. Using cycle notation, we can list all elements:

$$S_3 = \{id, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}.$$

Consider the cyclic subgroup of S^3 generated by $(1,2,3)$. It is

$$\{id, (1,2,3), (1,3,2)\} = \langle (1,2,3) \rangle = H.$$

The left cosets of H are:

$(1,2)H = \{(1,2), (1,2)(1,2,3), (1,2)(1,3,2)\}$

$= \{(1,2), (2,3), (1\ 3)\}$

In fact, we find the same for other cosets:

$(2,3)H = \{(2,3), (2,3)(1,2,3), (2,3)(1,3,2)\}$

$= \{(2,3), (1\ 3), (1,2\}$

Same for $(1,3)H$. Note that whenever $g \in H$, $gH = H$. So for all other elements of S_3, the corresponding left coset is H. One finds that the right cosets are the same:

$Hg = H$ if $g \in H$, and

$Hg = \{(1,2),(2,3),(1,3)\}$ if $g \notin H$.

This is not always the case. Consider the subgroup

__Example__: $\{id, (1,2)\} \subset S_3$, call it K.

Its left cosets are:

$(2,3)K = (1,3,2)K = \{(2,3), (1,3,2)\}$

$(1,3)K = (1,2,3)K = \{(1,3), (1,2,3)\}$

$id\ K = (1,2)K = \{id, (1,2)\}$

and the right cosets are

$K(2,3) = K(1\,2\,3) = \{(2,3), (1,2,3)\}$

$K(1,3) = K(1,3,2) = \{(1,3), (1,3,2)\}$

$K(1,2) = K\,id = \{id, (1,2)\}$

So left and right cosets are different.

Observation: If G is abelian, then

$$gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg,$$

so left and right cosets agree.

When are two cosets equal?

Lemma (6.3 in text) If $g_1, g_2 \in G$ and H is a subgroup, then the following are either all true or all false:

(i) $g_1 H = g_2 H$

(ii) $Hg_1^{-1} = Hg_2^{-1}$

(iii) $g_1 H \subseteq g_2 H$

(iv) $g_1 \in g_2 H$

(v) $g_1^{-1} g_2 \in H$.

Proof: Mostly left as an exercise. But we can do some examples:

(i) $\Rightarrow$ (iv).

If $g_1H = g_2H$, then $g_1 \cdot id = g_1 \in g_1H = g_2H$. so (iv) holds.

(iv) $\Rightarrow$ (i). If $g_1 \in g_2H$ then $g_1 = g_2h_0$ for some $h_0 \in H$. Now let $g_2h \in g_2H$ be given. Then

$$g_2h = (g_2h_0)(\underbrace{h_0^{-1}h}_{\in H}) = g_1(\text{element of } H) \in g_1H.$$

So $g_2H \subseteq g_1H$. Conversely since $g_1h_0^{-1} = g_2$ we can argue: Given $g_1h \in g_1H$, then

$$g_1h = g_1h_0^{-1}(\underbrace{h_0h}_{\in H}) = g_2(\text{element of } H) \in g_2H,$$

so $g_1H \subseteq g_2H$ and $g_1H = g_2H$.

== other cases left as exercises. ==

<u>Theorem</u>: Let $H \leq G$ be a subgroup. Then the left cosets of H partition G.

<u>Proof</u>: Let g_1H and g_2H be two left cosets. We must show that either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$. Suppose $g_1H \cap g_2H \neq \emptyset$, and choose $a \in g_1H \cap g_2H$. Then $\exists\, h_1, h_2 \in H$ so that $g_1h_1 = a = g_2h_2$. But then $g_1h_1 = g_2h_2 \Rightarrow g_1 = g_2h_2h_1^{-1} \Rightarrow g_1 \in g_2H$.

Therefore $g_1 H = g_2 H$ by the previous Lemma.

Last, observe that $\bigcup_{g \in G} gH = G$, since $g \in gH$ for all $g \in G$.

<u>Remark</u>: Right cosets behave the same way as the previous Lemma and theorem, ie. they also partition G.

<u>Definition</u>: Let G be a group and H a subgroup of G. The number of left cosets of H in G will be denoted $[G:H]$, it is called the <u>index</u> of H in G.

<u>Example</u>: If $G = S_3$ and $H = \langle (1,2) \rangle$ then $[G:H] = 3$. If $G = S_3$ and $H = \langle (1,2,3) \rangle$ then $[G:H] = 2$.

<u>Theorem</u>: Let G be a group, and H a subgroup. Then the number of left cosets of H in G is the same as the number of right cosets of H in G.

<u>Proof</u>: Give names to the two collections of cosets,

$\mathcal{L}_H$ = left cosets, $\mathcal{R}_H$ = right cosets.

Define $\phi : \mathcal{L}_{e_H} \to R_H$ as follows:

$$\phi(gH) = Hg^{-1}.$$

This map is well-defined, in the sense that if $gH = g'H$ then $\phi(gH) = Hg^{-1}$ and $\phi(g'H) = H(g')^{-1}$ are equal, by point (ii) of the previous lemma.

It is one-to-one since

$$Hg_1^{-1} = Hg_2^{-1} \Rightarrow g_1H = g_2H \ (\to \text{By lemma, part (ii)})$$

$$\phi(g_1H) = \phi(g_2H)$$

and it is surjective since $\phi(g^{-1}H) = Hg$ for all $g \in G$.

<u>Proposition</u>: Let H be a subgroup of G and let $g \in G$ be any element. Define a map $\phi : H \to gH$ by $\phi(h) = gh$. Then ϕ is bijective, so H and gH have the same number of elements for all $g \in G$.

<u>Proof</u>: First, ϕ is 1-to-1 since

$$\phi(h_1) = \phi(h_2) \Rightarrow gh_1 = gh_2 \Rightarrow h_1 = h_2.$$

Second, ϕ is surjective since every element of gH is of the form gh for some $h \in H$, and thus

$$\phi(h) = gh \text{ maps onto it.}$$

Theorem (Lagrange). Suppose G is finite and $H \leq G$ is a subgroup. Then $|G| = |H| \cdot [G:H]$. In particular, $|H|$ must divide $|G|$.

Proof: The group G is partitioned into $[G:H]$ left (or right) cosets of H, each having $|H|$ elements.

Corollary: Suppose that G is a finite group. Then the order of any $g \in G$ must divide the order $|G|$.

Proof: The order of $g \in G$ is the size of the cyclic subgroup $\langle g \rangle$, which must divide $|G|$ by Lagrange's theorem.

Corollary: If $|G| = p$, p a prime, then G is cyclic and every element is a generator.

Proof: Since p is prime, by Lagrange's theorem the only subgroups can be of size 1 and p. Let $g \in G$ be any nonidentity element. Then $|\langle g \rangle| > 1$ since $id, g \in \langle g \rangle$. Thus $|\langle g \rangle| = p$, forcing $G = \langle g \rangle$.

Remark: So groups of prime order are basically $\mathbb{Z}_p$??

(i) First note that every 3-cycle in S_4 is actually contained in A_4, since

$$(a,b,c) = (c\,b)(a\,c).$$

There are 8 3-cycles in S_4, so 8 3-cycles in A_4.

(ii) If $H \subset A_4$ and $|H| = 6$, H must therefore contain at least one 3-cycle.

(iii) Since $[A_4 : H] = 2$, left and right cosets of H are equal, meaning $gH = Hg \Rightarrow gHg^{-1} = H$ for all $g \in A_4$. So $ghg^{-1} \in H$ for all $h \in H$ and $g \in A_4$.

Thus we can choose a 3-cycle, WLOG say $(1,2,3) \in H$. Then $g(1,2,3)g^{-1} \in H$ and $g(1,2,3)^{-1}g^{-1} \in H$ for all $g \in A_4$.

So H contains $\underline{id}$, $\underline{(1,2,3)}$, $\underline{(1,3,2)}$, also

$$(1,2,4)(1,2,3)(1,2,4)^{-1} = \underline{(2,4,3)} \text{ and } \underline{(2,4,3)^{-1}}$$

$$(2,4,3)(1,2,3)(2,4,3)^{-1} = \underline{(1,4,2)} \text{ and } \underline{(1,4,2)^{-1}}.$$

So H now contains 7 elements! (underlined above).

Thus $|H| = 12$.

Corollary: Suppose that H and K are both subgroups of G, and $K \subset H \subset G$. Then

$$[G:K] = \underbrace{[G:H][H:K]}_{\text{multiplication of numbers}}$$

Proof: Using the previous theorem,

$$[G:K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G:H][H:K].$$

The converse of Lagrange's theorem is not true. That is, if $|G| = n$ and m is a divisor of n, there doesn't have to be a subgroup of size n (This is why problem 3 on the exam is remarkable: The converse of Lagrange's theorem is true for cyclic groups).

Example: $|A_4| = \frac{4!}{2} = 12$, so A_n can have subgroups of size $1, 2, 3, 4$ and 6. However there's no subgroup of size 6. Here is why:

The calculations in the last example used a special case of the following theorem.

<u>Theorem</u>: Two cycles $\tau, \mu \in S_n$ ~~are~~ have the same length if and only if there exists $\sigma \in S_n$ such that

$$\mu = \sigma \tau \sigma^{-1}.$$

<u>Proof</u>: If $\tau = (a_1, \ldots, a_k)$ and $\mu = (b_1, \ldots, b_k)$, then set $\sigma(a_i) = b_i$ for $i = 1, \ldots, k$. Then we check that $\mu = \sigma\tau\sigma^{-1}$, since, for example,

$$\mu(b_i) = b_{(i+1) \bmod k}, \quad \text{while}$$

$$\sigma\tau\sigma^{-1}(b_i) = \sigma\tau(a_i) = \sigma(a_{(i+1) \bmod k}) = b_{(i+1) \bmod k}.$$

On the other hand, if σ satisfies $\mu = \sigma\tau\sigma^{-1}$ for some cycles μ, τ, then μ & τ have the same length. Here's why: If $\tau = (a_1, \ldots, a_k)$ then set $\sigma(a_i) = b_i$. We calculate

$$\sigma\tau\sigma^{-1}(b_i) = \sigma\tau(a_i) = \sigma(a_{(i+1) \bmod k}) = b_{(i+1) \bmod k},$$

so $\mu = \sigma\tau\sigma^{-1} = (b_1, \ldots, b_k)$, a cycle the same length as τ.

We'll need this result later.

Two significant results from number theory are actually special applications of Lagrange's theorem.

First, define $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ as follows. Set $\phi(1) = 1$, and set (for $n > 1$)

$$\phi(n) = |U(n)| \quad \text{(size of the group of units)}$$
$$= \text{number of } m \text{ with } 1 \le m < n \text{ and } \gcd(m,n) = 1.$$

(this equality is because we get $U(n)$ from $\mathbb{Z}_n$ by discarding elements whose gcd with n is > 1).

E.g. $\phi(8) = 4$ since $U(8) = \{1, 3, 5, 7\}$.

Theorem: These two definitions of $\phi(n)$:

(i) $\phi(n) = |U(n)|$

(ii) $\phi(n) = \#$ of m with $1 \le m < n$ and $\gcd(m,n) = 1$

are equivalent.

Proof: Follows from previous material.

Theorem: (Euler's Theorem)

Let a, n be integers with $n > 0$ and $\gcd(a,n) = 1$. Then $a^{\phi(n)} \equiv 1 \bmod n$.

Proof: Consider the element $a \in U(n)$. Since $U(n)$ is a group of order $\phi(n)$, every element in $U(n)$ satisfies $a^{\phi(n)} = \text{identity}$. In $U(n)$ the identity is

1, so this gives $a^{\phi(n)} = 1$ (in $U(n)$). In modular arithmetic notation, $a^{\phi(n)} \equiv 1 \mod n$.

<u>Theorem</u> (Fermat's Little theorem).
If p is prime and p does not divide a, then

$$a^{p-1} \equiv 1 \mod p, \text{ further } b^p \equiv b \mod p \ \forall b.$$

<u>Proof</u>: If p is prime, then $\phi(p) = p-1$. So in this case, Euler's theorem gives $a^{p-1} \equiv 1 \mod p$. We need that a does not divide p to get $\gcd(a,n)=1$.

This is the backbone of modern RSA cryptography. Here is a quick explanation of how it works:
We prepare for someone to send us a message as follows:
Choose enormous prime numbers p and q. From these numbers, calculate:

$n = pq$ (just multiply them)

$\phi(n) = m = (p-1)(q-1)$ (just multiply).

Choose E with $\gcd(E,n) = 1$, and use the Euclidean algorithm to calculate D with $DE \equiv 1 (\mod m)$.

i.e. write $DE = 1 + km$ for some k

or $-km + DE = 1$, this is possible since

$\gcd(n, E) = 1$.

This is easy for us to do since we know the factors of n, so we can just compute $m = (p-1)(q-1)$.

Now we tell the numbers E, n to the whole world. Someone wants to tell ~~us~~ us a secret number X with $1 \leq X < n$. They do it by computing

$X^E \pmod{n}$ and sending us the result.

We decode their message by computing

$$(X^E)^D = X^{DE} = X^{1+k\phi(n)}$$

$$= X \cdot (X^{\phi(n)})^k$$

$$= X \cdot 1 = X \pmod{n}, \text{ by Fermat's theorem.}$$

Even if somebody intercepts the message X^E in transit, they will not be able to figure ~~of~~ out the secret number x unless they also have D. Computing D required us to know $m = (p-1)(q-1)$, i.e. we need to know the two big prime factors of m.

Fact: Factoring large numbers is very, very hard.

Exercises: 1, 3, 5(a), (b), (e), (f); 8, 11, 13, 18.