MATH 433

Applied Algebra

Lecture 29:
Cosets.
Lagrange's Theorem.

Cosets

Definition. Let H be a subgroup of a group G. A **coset** (or **left coset**) of the subgroup H in G is a set of the form $aH = \{ah : h \in H\}$, where $a \in G$. Similarly, a **right coset** of H in G is a set of the form $Ha = \{ha : h \in H\}$, where $a \in G$.

Theorem Let H be a subgroup of G and define a relation R on G by $aRb \iff a \in bH$. Then R is an equivalence relation.

Proof: We have aRb if and only if $b^{-1}a \in H$.
Reflexivity: aRa since $a^{-1}a = e \in H$.
Symmetry: $aRb \implies b^{-1}a \in H \implies a^{-1}b = (b^{-1}a)^{-1} \in H$ $\implies bRa$. **Transitivity**: aRb and $bRc \implies b^{-1}a, c^{-1}b \in H$ $\implies c^{-1}a = (c^{-1}b)(b^{-1}a) \in H \implies aRc$.

Corollary The cosets of the subgroup H in G form a partition of the set G.

Proof: Since R is an equivalence relation, its equivalence classes partition the set G. Clearly, the equivalence class of g is gH.

Examples of cosets

- $G = \mathbb{Z}$, $H = n\mathbb{Z}$.

The coset of $a \in \mathbb{Z}$ is $[a]_n = a + n\mathbb{Z}$, the congruence class of a modulo n.

- $G = \mathbb{R}^3$, H is the plane $x + 2y - z = 0$.

H is a subgroup of G since it is a subspace. The coset of $(x_0, y_0, z_0) \in \mathbb{R}^3$ is the plane $x + 2y - z = x_0 + 2y_0 - z_0$ parallel to H.

- $G = S(n)$, $H = A(n)$.

There are only 2 cosets, the set of even permutations $A(n)$ and the set of odd permutations $S(n) \setminus A(n)$.

- G is any group, $H = G$.

There is only one coset, G.

- G is any group, $H = \{e\}$.

Each element of G forms a separate coset.

Lagrange's Theorem

The number of elements in a group G is called the **order** of G and denoted $o(G)$. Given a subgroup H of G, the number of cosets of H in G is called the **index** of H in G and denoted $[G : H]$.

Theorem (Lagrange) If H is a subgroup of a finite group G, then $o(G) = [G : H] \cdot o(H)$. In particular, the order of H divides the order of G.

Proof: For any $a \in G$ define a function $f : H \to aH$ by $f(h) = ah$. By definition of aH, this function is surjective. Also, it is injective due to the left cancellation property:
$f(h_1) = f(h_2) \implies ah_1 = ah_2 \implies h_1 = h_2$.
Therefore f is bijective. It follows that the number of elements in the coset aH is the same as the order of the subgroup H. Since the cosets of H in G partition the set G, the theorem follows.

Corollaries of Lagrange's Theorem

Corollary 1 If G is a finite group, then the order of any element $g \in G$ divides the order of G.

Proof: The order of $g \in G$ is the same as the order of the cyclic group $\langle g \rangle$, which is a subgroup of G.

Corollary 2 If G is a finite group, then $g^{o(G)} = e$ for all $g \in G$.

Proof: We have $g^n = e$ whenever n is a multiple of $o(g)$. By Corollary 1, $o(G)$ is a multiple of $o(g)$ for all $g \in G$.

Corollaries of Lagrange's Theorem

Corollary 3 (Fermat's Little Theorem) If p is a prime number then $a^{p-1} \equiv 1 \bmod p$ for any integer a that is not a multiple of p.

Proof: $a^{p-1} \equiv 1 \bmod p$ means that $[a]_p^{p-1} = [1]_p$.
a is not a multiple of p means that $[a]_p$ is in G_p, the multiplicative group of invertible congruence classes modulo p.
It remains to recall that $o(G_p) = p - 1$ and apply Corollary 2.

Corollary 4 (Euler's Theorem) If n is a positive integer then $a^{\phi(n)} \equiv 1 \bmod n$ for any integer a coprime with n.

Proof: $a^{\phi(n)} \equiv 1 \bmod n$ means that $[a]_n^{\phi(n)} = [1]_n$.
a is coprime with n means that the congruence class $[a]_n$ is in G_n. It remains to recall that $o(G_n) = \phi(n)$ and apply Corollary 2.

Corollary 5 Any group G of prime order p is cyclic.

Proof: Take any element $g \in G$ different from e. Then $o(g) \neq 1$, hence $o(g) = p$, and this is also the order of the cyclic subgroup $\langle g \rangle$. It follows that $\langle g \rangle = G$.

Corollary 6 Any group G of prime order has only two subgroups: the trivial subgroup and G itself.

Proof: If H is a subgroup of G then $o(H)$ divides $o(G)$. Since $o(G)$ is prime, we have $o(H) = 1$ or $o(H) = o(G)$. In the former case, H is trivial. In the latter case, $H = G$.

Corollary 7 The alternating group $A(n)$, $n \geq 2$, consists of $n!/2$ elements.

Proof: Indeed, $A(n)$ is a subgroup of index 2 in the symmetric group $S(n)$. The latter consists of $n!$ elements.

Theorem Let G be a cyclic group of finite order n. Then for any divisor d of n there exists a unique subgroup of G of order d, which is also cyclic.

Lemma Suppose that an element g has finite order m. Then for any integer $\ell \neq 0$ the power g^ℓ has order $m/\gcd(\ell, m)$.

Proof: Let N be a positive integer. Then $(g^\ell)^N = g^{\ell N}$. Hence $(g^\ell)^N = e$ if and only if ℓN is divisible by m. The smallest number N with this property is $m/\gcd(\ell, m)$.

Proof of the theorem: We have $G = \langle g \rangle$, where $o(g) = n$. Take any divisor d of n. By Lemma, $o(g^{n/d}) = d$. Therefore a cyclic group $H = \langle g^{n/d} \rangle$ has order d.

Now assume H' is another subgroup of G of order d. The group H' is cyclic since G is cyclic. We have $H' = \langle g^k \rangle$ for some $k \neq 0$. By Lemma, $o(g^k) = n/\gcd(k, n)$. On the other hand, $o(g^k) = d$. It follows that $\gcd(k, n) = n/d$. We know that $\gcd(k, n) = ak + bn$ for some $a, b \in \mathbb{Z}$. Then $g^{n/d} = g^{ak+bn} = g^{ka}g^{nb} = (g^k)^a(g^n)^b = (g^k)^a \in \langle g^k \rangle = H'$. Hence $H = \langle g^{n/d} \rangle \subset H'$. But $o(H) = o(H') = d$. Thus $H' = H$.