MATH 433

Applied Algebra

Lecture 28:
Cyclic groups (continued).
Cosets.
Lagrange's Theorem.

Generators of a group

Let S be a nonempty subset of a group G. The **group generated by** S, denoted $\langle S \rangle$, is the smallest subgroup of G that contains the set S. The elements of the set S are called **generators** of the group $\langle S \rangle$.

Theorem 1 The group $\langle S \rangle$ is well defined. Namely, it is the intersection of all subgroups of G that contain the set S.

Theorem 2 The subgroup $\langle S \rangle$ consists of all elements of the form $g_1 g_2 \dots g_k$, where each $g_i = s$ or s^{-1} for some $s \in S$.

A **cyclic group** is a subgroup generated by a single element. Any cyclic group is Abelian.

Cyclic group: $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ (in multiplicative notation) or $\langle g \rangle = \{ng : n \in \mathbb{Z}\}$ (in additive notation).

If the generator g has finite order n, then $\langle g \rangle$ consists of n elements. If g is of infinite order, then $\langle g \rangle$ is infinite.

Subgroups of a cyclic group

Theorem Every subgroup of a cyclic group is cyclic as well.

Proof: Suppose that G is a cyclic group and H is a subgroup of G. Let g be the generator of G, $G = \{g^n : n \in \mathbb{Z}\}$. Denote by k the smallest positive integer such that $g^k \in H$ (if there is no such integer then $H = \{e\}$, which is a cyclic group). We are going to show that $H = \langle g^k \rangle$.

Take any $h \in H$. Then $h = g^n$ for some $n \in \mathbb{Z}$. We have $n = kq + r$, where q is the quotient and r is the remainder of n by k $(0 \leq r < k)$. It follows that $g^r = g^{n-kq} = g^n g^{-kq}$ $= h(g^k)^{-q} \in H$. By the choice of k, we obtain that $r = 0$. Thus $h = g^n = g^{kq} = (g^k)^q \in \langle g^k \rangle$.

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 order of the cyclic group $\langle g \rangle$, which is a subgroup of G.

Corollary 2 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 3 If G is a finite group, then $g^{o(G)} = 1$ for all $g \in G$.

Proof: We have $g^n = 1$ 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 4 (Fermat's Little Theorem) If p is a prime number then $a^{p-1} \equiv 1 \mod p$ for any integer a that is not a multiple of p.

Proof: $a^{p-1} \equiv 1 \mod p$ 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 3.

Corollary 5 (Euler's Theorem) If n is a positive integer then $a^{\phi(n)} \equiv 1 \mod n$ for any integer a coprime with n.

Proof: $a^{\phi(n)} \equiv 1 \mod n$ 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 3.