MATH 433

Applied Algebra

Lecture 18:
Cyclic groups.
Cosets.
Lagrange's theorem.

Groups

Definition. A **group** is a set G, together with a binary operation $*$, that satisfies the following axioms:

(G1: closure)
for all elements g and h of G, $g * h$ is an element of G;

(G2: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in G$;

(G3: existence of identity)
there exists an element $e \in G$, called the **identity** (or **unit**) of G, such that $e * g = g * e = g$ for all $g \in G$;

(G4: existence of inverse)
for every $g \in G$ there exists an element $h \in G$, called the **inverse** of g, such that $g * h = h * g = e$.

The group $(G, *)$ is said to be **commutative** (or **Abelian**) if it satisfies an additional axiom:

(G5: commutativity) $g * h = h * g$ for all $g, h \in G$.

Order of an element

Let g be an element of a group G. We say that g has **finite order** if $g^n = e$ for some positive integer n.

If this is the case, then the smallest positive integer n with this property is called the **order** of g and denoted $o(g)$. Otherwise g is said to have the **infinite order**, $o(g) = \infty$.

Theorem 1 (i) If the order $o(g)$ is finite, then $g^r = g^s$ if and only if $r \equiv s \bmod o(g)$. In particular, $g^r = e$ if and only if $o(g)$ divides r.
(ii) If the order $o(g)$ infinite, then $g^r \neq g^s$ whenever $r \neq s$.

Theorem 2 If G is a finite group, then every element of G has finite order.

Theorem 3 Let G be a group and $g, h \in G$ be two commuting elements of finite order. Then gh also has a finite order. Moreover, $o(gh)$ divides $\operatorname{lcm}\big(o(g), o(h)\big)$.

Subgroups

Definition. A group H is a called a **subgroup** of a group G if H is a subset of G and the group operation on H is obtained by restricting the group operation on G.

Theorem Let H be a nonempty subset of a group G and define an operation on H by restricting the group operation of G. Then the following are equivalent:

(i) H is a subgroup of G;

(ii) H is closed under the operation and under taking the inverse, that is, $g, h \in H \implies gh \in H$ and $g \in H \implies g^{-1} \in H$;

(iii) $g, h \in H \implies gh^{-1} \in H$.

Corollary If H is a subgroup of G then **(i)** the identity element in H is the same as the identity element in G; **(ii)** for any $g \in H$ the inverse g^{-1} taken in H is the same as the inverse taken in G.

Examples of subgroups: • $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.

• $(\mathbb{Q} \setminus \{0\}, \times)$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \times)$.

• The alternating group $A(n)$ is a subgroup of the symmetric group $S(n)$.

• The special linear group $SL(n, \mathbb{R})$ is a subgroup of the general linear group $GL(n, \mathbb{R})$.

• Any group G is a subgroup of itself.

• If e is the identity element of a group G, then $\{e\}$ is the **trivial** subgroup of G.

Counterexamples: • $(\mathbb{R} \setminus \{0\}, \times)$ is not a subgroup of $(\mathbb{R}, +)$ since the operations do not agree.

• $(\mathbb{Z}_n, +)$ is not a subgroup of $(\mathbb{Z}, +)$ since $\mathbb{Z}_n$ is not a subset of $\mathbb{Z}$ (although every element of $\mathbb{Z}_n$ is a subset of $\mathbb{Z}$).

• $(\mathbb{Z} \setminus \{0\}, \times)$ is not a subgroup of $(\mathbb{R} \setminus \{0\}, \times)$ since $(\mathbb{Z} \setminus \{0\}, \times)$ is not a group.

Generators of a group

Theorem 1 Let H_1 and H_2 be subgroups of a group G. Then the intersection $H_1 \cap H_2$ is also a subgroup of G.

Proof: $g, h \in H_1 \cap H_2 \implies g, h \in H_1$ and $g, h \in H_2$ $\implies gh^{-1} \in H_1$ and $gh^{-1} \in H_2 \implies gh^{-1} \in H_1 \cap H_2$.

Theorem 2 Let H_α, $\alpha \in A$ be a collection of subgroups of a group G (where the index set A may be infinite). Then the intersection $\bigcap_\alpha H_\alpha$ is also a subgroup of G.

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 3 (i) The group $\langle S \rangle$ is the intersection of all subgroups of G that contain the set S.

(ii) The group $\langle S \rangle$ consists of all elements of the form $g_1 g_2 \dots g_k$, where each g_i is either a generator $s \in S$ or the inverse s^{-1} of a generator.

Cyclic groups

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

Cyclic group $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.

Any cyclic group is Abelian.

If g has finite order n, then $\langle g \rangle$ consists of n elements $g, g^2, \dots, g^{n-1}, g^n = e$.

If g is of infinite order, then $\langle g \rangle$ is infinite.

Examples of cyclic groups: $\mathbb{Z}$, $3\mathbb{Z}$, $\mathbb{Z}_5$, $S(2)$, $A(3)$.

Examples of noncyclic groups: any non-Abelian group, $\mathbb{Q}$ with addition, $\mathbb{Q} \setminus \{0\}$ with multiplication.

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: $g^n = 1$ whenever n is a multiple of $o(g)$.

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 notice that $o(G_p) = p - 1$.

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 notice that $o(G_n) = \phi(n)$.