MATH 433

Applied Algebra

Lecture 17:
Order of an element in a group.
Subgroups.

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 $g, h \in G$.

Basic properties of groups

- The identity element is unique.
- The inverse element is unique.
- $(g^{-1})^{-1} = g$. In other words, $h = g^{-1}$ if and only if $g = h^{-1}$.
- $(gh)^{-1} = h^{-1}g^{-1}$.
- $(g_1 g_2 \dots g_n)^{-1} = g_n^{-1} \dots g_2^{-1} g_1^{-1}$.
- **Cancellation properties**: $gh_1 = gh_2 \implies h_1 = h_2$ and $h_1 g = h_2 g \implies h_1 = h_2$ for all $g, h_1, h_2 \in G$.

Indeed, $gh_1 = gh_2 \implies g^{-1}(gh_1) = g^{-1}(gh_2)$
$\implies (g^{-1}g)h_1 = (g^{-1}g)h_2 \implies eh_1 = eh_2 \implies h_1 = h_2$.
Similarly, $h_1 g = h_2 g \implies h_1 = h_2$.

Equations in groups

Theorem Let G be a group. For any $a, b, c \in G$,

- the equation $ax = b$ has a unique solution $x = a^{-1}b$;
- the equation $ya = b$ has a unique solution $y = ba^{-1}$;
- the equation $azc = b$ has a unique solution $z = a^{-1}bc^{-1}$.

Problem. Solve an equation in the group $S(5)$: $(1\ 2\ 4)(3\ 5)\pi(2\ 3\ 4\ 5) = (1\ 5)$.

Solution: $\pi = \big((1\ 2\ 4)(3\ 5)\big)^{-1}(1\ 5)(2\ 3\ 4\ 5)^{-1}$
$= (3\ 5)^{-1}(1\ 2\ 4)^{-1}(1\ 5)(2\ 3\ 4\ 5)^{-1}$
$= (5\ 3)(4\ 2\ 1)(1\ 5)(5\ 4\ 3\ 2) = (1\ 3)(2\ 4\ 5)$.

Powers of an element

Let g be an element of a group G. The positive **powers** of g are defined inductively:

$$g^1 = g \ \text{ and } \ g^{k+1} = g \cdot g^k \ \text{ for every integer } \ k \geq 1.$$

The negative powers of g are defined as the positive powers of its inverse: $g^{-k} = (g^{-1})^k$ for every positive integer k. Finally, we set $g^0 = e$.

Theorem Let g be an element of a group G and $r, s \in \mathbb{Z}$. Then

(i) $g^r g^s = g^{r+s}$,
(ii) $(g^r)^s = g^{rs}$,
(iii) $(g^r)^{-1} = g^{-r}$.

Idea of the proof: First one proves the theorem for positive r, s by induction (induction on r for (i) and (iii), induction on s for (ii)). Then the general case is reduced to the case of positive r, s.

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

Proof: Let $g \in G$ and consider the list of powers: $g, g^2, g^3, \dots$. Since all elements in this list belong to the finite set G, there must be repetitions within the list. Assume that $g^r = g^s$ for some $0 < r < s$. Then $g^r e = g^r g^{s-r}$ $\implies g^{s-r} = e$ due to the cancellation property.

Theorem 1 Let G be a group and $g \in G$ be an element of finite order n. Then $g^r = g^s$ if and only if $r \equiv s \mod n$. In particular, $g^r = e$ if and only if the order n divides r.

Theorem 2 Let G be a group and $g \in G$ be an element of infinite order. Then $g^r \neq g^s$ whenever $r \neq s$.

Theorem 3 Let g and h be two commuting elements of a group G: $gh = hg$. Then

(i) the powers g^r and h^s commute for all $r, s \in \mathbb{Z}$,

(ii) $(gh)^r = g^r h^r$ for all $r \in \mathbb{Z}$.

Theorem 4 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 $\mathrm{lcm}\big(o(g), o(h)\big)$.

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.