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 $\operatorname{lcm}\big(o(g), o(h)\big)$.