MATH 433

Applied Algebra

Lecture 27:
Subgroups (continued).
Cyclic groups.

Order of an element in a group

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 $r \equiv s \mod o(g)$. 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 $\operatorname{lcm}\big(o(g), o(h)\big)$.

Theorem 4 $o(g^{-1}) = o(g)$ for all $g \in G$.

Proof: $(g^{-1})^n = g^{-n} = (g^n)^{-1}$ for any integer $n \geq 1$. Since $e^{-1} = e$, it follows that $(g^{-1})^n = e$ if and only if $g^n = e$.

Definition. Given $g_1, g_2 \in G$, we say that the element g_1 is **conjugate** to g_2 if $g_1 = hg_2h^{-1}$ for some $h \in G$. The **conjugacy** is an equivalence relation on the group G.

Theorem 5 Conjugate elements have the same order.

Proof: Let $g_1, g_2 \in G$ and suppose g_1 is conjugate to g_2, $g_1 = hg_2h^{-1}$ for some $h \in G$. Then $g_1^2 = hg_2h^{-1}hg_2h^{-1} = hg_2^2h^{-1}$. By induction, $g_1^n = hg_2^nh^{-1}$ for all $n \geq 1$. If $g_2^n = e$ then $g_1^n = heh^{-1} = hh^{-1} = e$. It follows that $o(g_1) \leq o(g_2)$. Since g_2 is conjugate to g_1 as well, we also have $o(g_2) \leq o(g_1)$. Thus $o(g_1) = o(g_2)$.

Corollary $o(gh) = o(hg)$ for all $g, h \in G$.

Proof: The element gh is conjugate to hg, $gh = g(hg)g^{-1}$.

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.

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.

Theorem The symmetric group $S(n)$ is generated by two permutations: $\tau = (1\ 2)$ and $\pi = (1\ 2\ 3\ \dots\ n)$.

Proof: Let $H = \langle \tau, \pi \rangle$. We have to show that $H = S(n)$.

First we obtain that $\alpha = \tau\pi = (2\ 3\ \dots\ n)$. Then we observe that $\sigma(1\ 2)\sigma^{-1} = (\sigma(1)\ \sigma(2))$ for any permutation σ.
In particular, $(1\ k) = \alpha^{k-2}(1\ 2)(\alpha^{k-2})^{-1}$ for $k = 2, 3 \dots, n$.
It follows that the subgroup H contains all transpositions of the form $(1\ k)$.

Further, for any integers $2 \le k < m \le n$ we have $(k\ m) = (1\ k)(1\ m)(1\ k)$. Therefore the subgroup H contains all transpositions. Finally, every permutation in $S(n)$ is a product of transpositions, therefore it is contained in H.
Thus $H = S(n)$.

Remark. Although the group $S(n)$ is generated by two elements, its subgroups need not be generated by two elements.

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.

Subgroups of $\mathbb{Z}$

Integers $\mathbb{Z}$ with addition form a cyclic group, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. The proper cyclic subgroups of $\mathbb{Z}$ are: the trivial subgroup $\{0\} = \langle 0 \rangle$ and, for any integer $m \geq 2$, the group $m\mathbb{Z} = \langle m \rangle = \langle -m \rangle$. These are all subgroups of $\mathbb{Z}$.

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 $h = g^n = g^{kq} = (g^k)^q \in \langle g^k \rangle$.