MATH 415

Modern Algebra I

Lecture 5:
Subgroups.
Order of an element in a group.
Cyclic groups.

Groups

Definition. A **group** is a binary structure $(G, *)$ that satisfies the following axioms:

(G0: closure)
for all elements g and h of G, $g * h$ is an element of G;

(G1: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in G$;

(G2: 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 $g \in G$;

(G3: 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:

(G4: commutativity) $g * h = h * g$ for all $g, h \in G$.

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. Notation: $H \leq G$.

Proposition 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.

Theorem Let H be a 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 contains e and 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) H is nonempty and $g, h \in H \implies gh^{-1} \in H$.

Examples of subgroups:

- $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$.
- If V_0 is a subspace of a vector space V, then it is also a subgroup of the additive group V.
- 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:

- $(\mathbb{R}^+, \cdot)$ is not a subgroup of $(\mathbb{R}, +)$ since the operations do not agree (even though the groups are isomorphic).
- $(\mathbb{Z}_n, +_n)$ is not a subgroup of $(\mathbb{Z}, +)$ since the operations do not agree (even though they do agree sometimes).
- $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$ since $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a group (it is a **subsemigroup**).

Intersection of subgroups

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: The identity element e of G belongs to every subgroup. Hence $e \in H_1 \cap H_2$. In particular, the intersection is nonempty. Now for any elements g and h of the group G,

$g, h \in H_1 \cap H_2 \implies g, h \in H_1$ 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 nonempty collection of subgroups of the same group G (where the index set A may be infinite). Then the intersection $\bigcap_\alpha H_\alpha$ is also a subgroup of G.

Generators of a group

Let S be a set (or a list) of some elements 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. Indeed, it is the intersection of all subgroups of G that contain S.

Note that we have at least one subgroup of G containing S, namely, G itself. If it is the only one, i.e., $\langle S \rangle = G$, then S is called a **generating set** for the group G.

Theorem 2 If S is nonempty, then 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.

Powers of an element in a group

A **cyclic group** is a subgroup generated by a single element. The cyclic group $\langle g \rangle$ consists of all powers of the element g (in multiplicative notation).

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

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

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)** $g^r g^s = g^{r+s}$ and **(ii)** $(g^r)^s = g^{rs}$.

Corollary All powers of g commute with one another: $g^r g^s = g^s g^r$ for all $r, s \in \mathbb{Z}$.

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. Otherwise g is said to be of **infinite order**. The order of g can be denoted $|g|$ or $o(g)$.

Proposition 1 Let G be a group and $g \in G$ be an element of infinite order. Then $g^r \neq g^s$ whenever $r \neq s$.

Proposition 2 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 and s leave the same remainder after division by n. In particular, $g^r = e$ if and only if the order n divides r.

Corollary 1 The order of an element g equals the number of distinct powers of g.

Corollary 2 Every element of a finite group has finite order.

Order of an element

Lemma Suppose $g^r = g^s$ for some $g \in G$ and $r, s \in \mathbb{Z}$, where $r \neq s$. Then the element g has finite order. Moreover, the order of g divides the difference $s - r$.

Proof: Using properties of the powers, we obtain

$$g^{s-r} = g^s g^{-r} = g^s (g^r)^{-1} = g^s (g^s)^{-1} = e.$$

Further, $g^{r-s} = g^{(s-r)(-1)} = (g^{s-r})^{-1} = e^{-1} = e$. Since $r \neq s$, one of the numbers $s - r$ and $r - s$ is a positive integer. It follows that g has finite order. Let n denote that order. Dividing $s - r$ by n, we obtain $s - r = nq + t$, where $q, t \in \mathbb{Z}$, $0 \leq t < n$. Then

$$g^t = g^{s-r-nq} = g^{s-r} g^{-nq} = g^{s-r} (g^n)^{-q} = ee^{-q} = e$$

since $e^k = e$ for all $k \in \mathbb{Z}$. By definition of the order, the remainder t cannot be positive (as $t < n$). Therefore $t = 0$. Thus $s - r$ is divisible by n.

Order of an element

Proposition 1 Let G be a group and $g \in G$ be an element of infinite order. Then $g^r \neq g^s$ whenever $r \neq s$.

Proof: This follows directly from the lemma.

Proposition 2 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 and s leave the same remainder after division by n. In particular, $g^r = e$ if and only if the order n divides r.

Proof: The "only if" part follows directly from the lemma. Let us prove the "if" part. Assume r and s leave the same remainder after division by n. Then the difference $s - r$ is divisible by n, that is, $s - r = nq$ for some $q \in \mathbb{Z}$. It follows that

$$g^r = g^s g^{r-s} = g^s g^{-nq} = g^s (g^n)^{-q} = g^s e^{-q} = g^s e = g^s.$$

Proposition 3 The inverse g^{-1} has the same order as g.

Proof: $(g^{-1})^n = g^{-n} = (g^n)^{-1}$ for any integer $n > 0$. Since $e^{-1} = e$, it follows that $(g^{-1})^n = e$ if and only if $g^n = e$. As a consequence, g^{-1} and g are of the same order.

Proposition 4 Suppose that an element g has finite order n. Then for any integer $k \neq 0$ the power g^k has order $\dfrac{n}{\gcd(k, n)}$.

Proof: Let N be a positive integer. Then $(g^k)^N = g^{kN}$. Hence $(g^k)^N = e$ if and only if kN is divisible by n. The smallest number N with this property is $n/\gcd(k, n)$.

Proposition 5 If an element g has infinite order, then for any integer $k \neq 0$ the power g^k has infinite order as well.

Proof: We have that $g^r \neq g^s$ whenever $r \neq s$. In particular, $(g^k)^n = g^{kn} \neq g^0 = e$ for any integer $n > 0$.

Cyclic groups

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

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

Any cyclic group is abelian since $g^n g^m = g^{n+m} = g^m g^n$ for all $m, n \in \mathbb{Z}$.

If g has finite order n, then the cyclic group $\langle g \rangle$ 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: $\mathbb{Z}$, $3\mathbb{Z}$, $\mathbb{Z}_5$, $\mathbb{Z}_8$.

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