MATH 415

Modern Algebra I

Lecture 5:
Generators of a group.
Cyclic groups.
Cayley graphs.

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

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

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

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 integer $n > 0$.

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**.

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

Proposition 1 The inverse element g^{-1} has the same order as 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 $g^n = e$.

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 have the same remainder under division by n. In particular, $g^r = e$ if and only if the order n divides r.

Proposition 3 Let G be a group and $g \in G$ be an element of infinite order. Then $g^r \neq g^s$ whenever $r \neq s$.

Cyclic groups

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

Cyclic group: $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ (in multiplicative notation) or $\langle g \rangle = \{ng : n \in \mathbb{Z}\}$ (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: $\mathbb{Z}$, $3\mathbb{Z}$, $\mathbb{Z}_5$, $\mathbb{Z}_8$, $S(\{1, 2\})$.

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

Subgroups of a cyclic group

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

Examples

- Integers $\mathbb{Z}$ with addition.

The group is cyclic, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. 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 $\mathbb{Z}$.

- $\mathbb{Z}_5$ with addition modulo 5.

The group is cyclic, $\mathbb{Z}_5 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle$. The only proper subgroup is the trivial subgroup $\{0\} = \langle 0 \rangle$.

- $\mathbb{Z}_6$ with addition modulo 6.

The group is cyclic, $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$. Proper subgroups are $\{0\} = \langle 0 \rangle$, $\{0, 3\} = \langle 3 \rangle$ and $\{0, 2, 4\} = \langle 2 \rangle = \langle 4 \rangle$.

Greatest common divisor

Given two nonzero integers a and b, the **greatest common divisor** of a and b is the largest natural number that divides both a and b.

Notation: $\gcd(a, b)$.

Example. $a = 12$, $b = 18$.

Natural divisors of 12 are $1, 2, 3, 4, 6$, and 12.
Natural divisors of 18 are $1, 2, 3, 6, 9$, and 18.
Common divisors are $1, 2, 3$, and 6.
Thus $\gcd(12, 18) = 6$.

Notice that $\gcd(12, 18)$ is divisible by any other common divisor of 12 and 18.

Definition. Given nonzero integers $a_1, a_2, \dots, a_k$, the **greatest common divisor** $\gcd(a_1, a_2, \dots, a_k)$ is the largest positive integer that divides $a_1, a_2, \dots, a_k$.

Theorem (i) $\gcd(a_1, a_2, \dots, a_k)$ is the smallest positive integer represented as $n_1 a_1 + n_2 a_2 + \dots + n_k a_k$, where each $n_i \in \mathbb{Z}$ (that is, as an integral linear combination of $a_1, a_2, \dots, a_k$).

(ii) $\gcd(a_1, a_2, \dots, a_k)$ is divisible by any other common divisor of $a_1, a_2, \dots, a_k$.

Proof. Consider an additive subgroup H of $\mathbb{Z}$ generated by $a_1, a_2, \dots, a_k$. The subgroup H consists exactly of integral linear combinations of $a_1, a_2, \dots, a_k$. Note that H is not a trivial subgroup. By the above, $H = m\mathbb{Z}$ for some integer $m \geq 1$. Clearly, m is a common divisor of $a_1, a_2, \dots, a_k$. Since $m \in H$, it is an integral linear combination of $a_1, a_2, \dots, a_k$ and hence is divisible by any other common divisor.

Cayley graph

A finitely generated group G can be visualized via the **Cayley graph**. Suppose $a, b, \ldots, c$ is a finite list of generators for G. The Cayley graph is a directed graph (or digraph) with labeled edges where vertices are elements of G and edges show multiplication by generators. That is, every edge is of the form $g \xrightarrow{s} gs$. Alternatively, one can assign colors to generators and think of the Cayley graph as a graph with colored edges.

The Cayley graph can be used for computations in G. For example, let $h = a^2 b^{-1} c a^{-1}$. To compute gh, we need to find a path of the form (note the directions of edges)

$$g \xrightarrow{a} g_1 \xrightarrow{a} g_2 \xleftarrow{b} g_3 \xrightarrow{c} g_4 \xleftarrow{a} g_5.$$

Such a path exists and is unique. Then $gh = g_5$.