MATH 415

Modern Algebra I

Lecture 8: Cyclic groups. Cayley graphs.

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.

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.

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, $G = \{g^n \mid n \in \mathbb{Z}\}$. 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 $H = \langle g^k \rangle$.

Since $g^k \in H$, it follows that $\langle g^k \rangle \subset H$. Let us show that $H \subset \langle g^k \rangle$. 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 after division of n by k $(0 \le r < k)$. 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 $n_1 a_1 + n_2 a_2 + \cdots + n_k a_k$, 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 the smallest positive element of H and 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. Namely, 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 $h = a^2b^{-1}ca^{-1}$. 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 $gh = g_5$.

Also, the Cayley graph can be used to find **relations** between generators, which are equalities of the form $g_1g_2 \ldots g_k = 1$, where each g_i is a generator or the inverse of a generator. Any relation corresponds to a closed path in the graph.