MATH 415

Modern Algebra I

Lecture 6:
Cyclic groups (continued).
Cayley graphs.
Permutations.

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 $(0 \leq r < k)$. 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 $n_1a_1 + n_2a_2 + \cdots + n_ka_k$, 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 $h = a^2 b^{-1} c a^{-1}$. To compute gh, we need to find a path of the form (note the directions of edges)

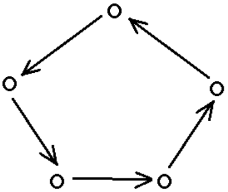
$$g \xrightarrow{a} g_1 \xrightarrow{a} g_2 \xleftarrow{b} g_3 \xrightarrow{c} g_4 \xleftarrow{a} g_5.$$

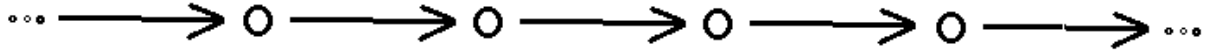
Such a path exists and is unique. Then $gh = g_5$.

Also, the Cayley graph can be used to find **relations** between generators, which are equalities of the form $g_1 g_2 \ldots g_k = 1_G$, where each g_i is a generator or the inverse of a generator. Any relation corresponds to a closed path in the graph.

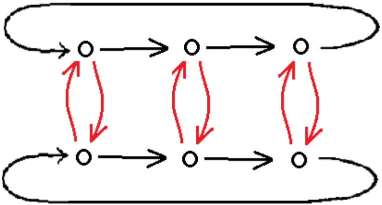
Examples of Cayley graphs

Group: $\mathbb{Z}_5$.
Generating set: $\{1\}$.





Group: $\mathbb{Z}$. Generating set: $\{1\}$.

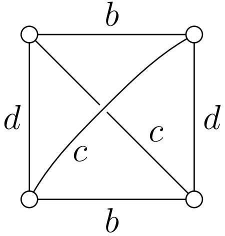


Group: $\mathbb{Z}_6$.
Generating set: $\{2, 3\}$.

Klein four-group

The **Klein four-group** $V = \{a, b, c, d\}$ is a group with the following Cayley table and Cayley graph:

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a



The group is abelian but not cyclic. The Cayley graph is relative to the generating set $\{b, c, d\}$ (a is the identity element). Since every generator is its own inverse, each directed edge $g \xrightarrow{s} gs$ is accompanied by another edge $g \xleftarrow{s} gs$. This allows to consider the Cayley graph as a graph with undirected edges.

Permutations

Let X be a nonempty set. A **permutation** of X is a bijective function $f : X \to X$.

Given two permutations π and σ of X, the composition $\pi\sigma$, defined by $\pi\sigma(x) = \pi(\sigma(x))$, is called the **product** of these permutations. In general, $\pi\sigma \neq \sigma\pi$, i.e., multiplication of permutations is not commutative. However it is associative: $\pi(\sigma\tau) = (\pi\sigma)\tau$.

All permutations of a set X form a group called the **symmetric group** on X. *Notation:* S_X, Σ_X, $\mathrm{Sym}(X)$.

All permutations of $\{1, 2, \ldots, n\}$ form a group called the **symmetric group on n symbols** and denoted S_n or $S(n)$.

Permutations of a finite set

The word "**permutation**" usually refers to transformations of finite sets.

Permutations are traditionally denoted by Greek letters (π, σ, τ, ρ,...).

Two-row notation. $\pi = \begin{pmatrix} a & b & c & \dots \\ \pi(a) & \pi(b) & \pi(c) & \dots \end{pmatrix}$,

where $a, b, c, \dots$ is a list of all elements in the domain of π. Rearrangement of columns does not change the permutation.

Example. The symmetric group S_3 consists of 6 permutations:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Theorem The symmetric group S_n has $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ elements.

Traditional argument: The number of elements in S_n is the number of different rearrangements $x_1, x_2, \dots, x_n$ of the list $1, 2, \dots, n$. There are n possibilities to choose x_1. For any choice of x_1, there are $n-1$ possibilities to choose x_2. And so on...

Alternative argument: Any rearrangement of the list $1, 2, \dots, n$ can be obtained as follows. We take a rearrangement of $1, 2, \dots, n-1$ and then insert n into it. By the inductive assumption, there are $(n-1)!$ ways to choose a rearrangement of $1, 2, \dots, n-1$. For any choice, there are n ways to insert n.

Product of permutations

Given two permutations π and σ, the composition $\pi\sigma$ is called the **product** of these permutations. Do not forget that the composition is evaluated from right to left: $(\pi\sigma)(x) = \pi(\sigma(x))$.

To find $\pi\sigma$, we write π underneath σ (in two-row notation), then reorder the columns so that the second row of σ matches the first row of π, then erase the matching rows.

Example. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$.

$$\begin{array}{l} \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \\ \pi = \begin{pmatrix} 3 & 2 & 1 & 5 & 4 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} \end{array} \implies \pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$$

To find π^{-1}, we simply exchange the upper and lower rows:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Cycles

A permutation π of a set X is called a **cycle** (or **cyclic**) of length r if there exist r distinct elements $x_1, x_2, \ldots, x_r \in X$ such that

$$\pi(x_1) = x_2,\ \pi(x_2) = x_3, \ldots,\ \pi(x_{r-1}) = x_r,\ \pi(x_r) = x_1,$$

and $\pi(x) = x$ for any other $x \in X$.

Notation. $\pi = (x_1\ x_2\ \ldots\ x_r)$.

The identity function is (the only) cycle of length 1. Any cycle of length 2 is called a **transposition**.

The inverse of a cycle is also a cycle of the same length. Indeed, if $\pi = (x_1\ x_2\ \ldots\ x_r)$, then $\pi^{-1} = (x_r\ x_{r-1}\ \ldots\ x_2\ x_1)$.

Example. Any permutation of $\{1, 2, 3\}$ is a cycle.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{id},\ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3),\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2),$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3),\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2),\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3).$$