Abstract Algebra
Judson, Thomas J.

Notes by:
Clay Curry

5 Permutation Groups

Permutation groups are central to the study of geometric symmetries and to Galois theory, the study of finding solutions of polynomial equations. Permutation groups also provide abundant examples of non-abelian groups.

As an example, it was already shown that the symmetries of an equilateral triangle ΔABC actually consist of permutations of the three vertices, where a **permutation** of the set $S = \{A, B, C\}$ is any one-to-one and onto map $\pi : S \to S$.

5.1 Definitions and Notation

In general, let X be any set. Then the set of permutations of X form a group, S_X.

Definition: Symmetric Group

If X is finite, we can assume $X = \{1, 2, \ldots, n\}$. The set of bijective maps on X, can therefore be denoted by S_X or S_n. The set S_n is called the **symmetric group** on n letters, and the following theorem shows that S_n form a group under composition of relations.

Theorem: S_n is a group

The symmetric group on n letters, S_n, is a group with $n!$ elements, where the binary operation is the composition of maps.

Proof: $\square$

Definition: Permutation Group

Any subgroup $H \leqslant S_n$ is called a permutation group.

5.2 Cyclic Notation

The elementary notation used to represent permutations is often cumbersome. A more convenient method involved denoting a permuation by denoting the cycles of the permutation

Definition: Permutation Cycle

A permutation $\sigma \in S_X$ is a **cycle of length** k if there exists elements $a_1, a_2, \ldots, a_k \in X$ such that,

$$\begin{aligned} \sigma(a_1) &= a_2 \\ \sigma(a_2) &= a_3 \\ &\vdots \\ \sigma(a_k) &= a_1 \end{aligned}$$

and $\sigma(x) = x$ for all other elements $x \in X$. The following notation denotes the above cycle

$$\sigma := (a_1, a_2, \ldots, a_k)$$

Example: Cycle of length k

The permutation denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (162354)$$

is a cycle of length 6 and the permutation denoted by

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix} = (243)$$

is a cycle of length 3.

Example: 2^n

The following set and law of composition $(H, \cdot)$ is a subgroup of non-zero rationals $\mathbb{Q}^*$

$$H = \{2^n : n \in \mathbb{Z}\}$$

because $H \neq \emptyset$ and for all $2^n, 2^m \in H$, we have $2^n(2^m)^{-1} = 2^n 2^{-m} = 2^{n-m} \in H$. Therefore, H is a subgroup of $\mathbb{Q}^*$ determined by 2.

Theorem: Repeated composition forms a subgroup

Let G be a group and $a \in G$. Then the set

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G containing a.

Proof: If $a \in G$, then $a^0 = e \in G$ so $\langle a \rangle \neq \emptyset$. Also if $m, n \in \mathbb{Z}$ and $a^{m+n} = a^m a^n \in \langle a \rangle$, then $a^{m-n} = a^m a^{-n} \in \langle a \rangle$, concluding that $\langle a \rangle$ is a subgroup of $\mathbb{Q}^*$.

Since any group containing a must contain all the powers a^k of a, $\langle a \rangle$ is a subgroup of all groups containing a. Therefore, $\langle a \rangle$ is the smallest subgroup of G containing a. $\square$

Definition: Cyclic Groups

For $a \in G$, the set $\langle a \rangle$ is called the **cyclic subgroup** of G generated by a. If G contains some element of a such that $G = \langle a \rangle$, then G is a **cyclic group**. In this case a is called a **generator** of G.

Definition: Order

If a is an element of a group G, we define the **order** of a to be the smallest positive integer n such that $a^n = e$, and we write $|a| = n$. If there is no such integer, we write $|a| = \infty$.

In general, a cyclic group can have more than a single generator. Both 1 and 5 generate $\mathbb{Z}_6$; hence, $\mathbb{Z}_6$ is a cyclic group. In general, not every element in a cyclic group is necessarily a generator of the group. The order of $2 \in \mathbb{Z}_6$ is 3.

In the symmetry group of an equaliateral triangle S_3, each element forms a distinct cyclic subgroup of S_3; however, no single element of S_3 generates S_3.

Theorem:

Every cyclic group is abelian

Proof: Let G be a cyclic group; therefore, $\exists a \in G$ such that $G = \langle a \rangle$. Then for any two elements $g, h \in G$, since

$$gh = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = hg$$

G is abelian. $\square$

5.3 Subgroups of cyclic groups

One interesting question we can asks about any group G is, "which subgroups of G are cyclic?" Similarly, for any cyclic subgroup, we can ask, "which subgroups for some cyclic subgroup $H \leqslant G$ are cyclic?"

Theorem:

Every subgroup of a cyclic group is cyclic

Proof: Let G be a cyclic group generated by $g \in G$ and suppose $H \leqslant G$. If $H = \{e\}$ then e generates H. If some non-identity element $h = g^n \in H$, then $h^{-1} = g^{-n} \in H$, and either n or $-n$ is positive. Let $S = \{m \in \mathbb{N} : g^m \in H\}$. Notice $n \in S$ or $-n \in S$, implying $\emptyset \neq S \subset \mathbb{N}$, which means S has a least element $m = \min(S)$. Let $h' = g^m$

Claim: $\langle h' \rangle = H$.

Since $H \leqslant G$ and G is cyclic, $\forall h \in H, \exists k \in \mathbb{Z}$, such that $h = g^k$. By the division algorithm, $\exists q, r \in \mathbb{Z}$ where $0 \leq r < m$, such that

$$h = g^k = g^{mq+r} = (g^m)^q g^r \iff g^r = h(h')^{-q} \iff (g^r \in H) \wedge (r < m)$$

and since $m = \min(S)$, we know $r = 0$. Because

$$h = g^k = (g^m)^q = h'^q$$

for all $h \in H$, H is cyclic. $\square$

Theorem:

Let G be a cyclic group of order n and suppose that a is a generator for G. Then $a^k = e$ if and only if n divides k.

Proof: $\square$

Theorem:

Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d, where $d = \gcd(k, n)$.

Proof: $\square$