# Section 2.3-3.1 Notes

Scribe: Heidi Bronson
09/08/2025

## 1. Section 2.3

**Theorem 1.** Every permutation can be written as a product of transpositions.

Idea of a proof: We can represent any permutation as a product of cycles so we just have to check if a cycle is the product of transpositions. Any cycle $(a_1, a_2, ..., a_k) = (a_k, a_1)(a_{k-1}, a_1)...(a_2, a_1)$.

**Example 1.** Write $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 1 & 8 & 4 & 6 & 2 & 3 \end{pmatrix}$ as a product of transpositions.
$\sigma = (6)(2\ 7)(1\ 5\ 4\ 8\ 3)$ (cycle notation)
$\sigma = (2\ 7)(1\ 3)(1\ 8)(1\ 4)(1\ 5)$ (order doesn't matter)
$= (2\ 7)(3\ 1)(8\ 1)(4\ 1)(5\ 1)$ (see what number 1-8 does 1 go to)
Check: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 1 & 8 & 4 & 6 & 2 & 3 \end{pmatrix}$

The inverse of a permutation is just the inverse function written $\sigma^{-1}$
$\sigma(\sigma^{-1}) =$ identity permutation.
$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 8 & 5 & 1 & 6 & 2 & 4 \end{pmatrix}$ (use the bottom row of the original permutation)

**Definition 1.** The order of a permutation is the smallest integer greater than 0 such that $\sigma^n =$ identity where $\sigma^n$ represents composing $\sigma$ with itself n times.

$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 5 & 3 & 8 & 6 & 7 & 1 \end{pmatrix}$ (trace through original permutation twice)
$\sigma^4 = (\sigma^2)^2$

**Proposition 1.** If $\sigma$ is a cycle of length n then its order is n.

If $\sigma$ is any permutation of order n then $\sigma^k =$ identity iff k is a multiple of n.

**Theorem 2.** If $\sigma$ is a permutation with cycle lengths $n_1, n_2, ..., n_k$ then the order of $\sigma$ is $LCM(n_1, n_2, ..., n_k)$.

*Proof.* Suppose the cycles of $\sigma$ are $\sigma_1, \sigma_2, ..., \sigma_k$. $\sigma = \sigma_1 \circ \sigma_2 \circ ... \circ \sigma_k$. If n is the order of $\sigma$ then $\sigma^n =$ identity. So $(\sigma_1 \circ \sigma_2 ... \sigma_k) \circ (\sigma_1 \circ \sigma_2 ... \sigma_k)(\sigma_1 ...)$ (n times) $= \sigma_1^n \circ \sigma_2^n ... \sigma_k^n)$. In each case $\sigma_i^n =$ identity so n is a multiple of the order of $\sigma_1$, which we called $n_i$. n is the least such number so that's the least common multiple of $n_1, n_2, ..., n_k$. □

If f, g and h are any 3 functions, then their composition $f \circ g \circ h$ is associative, that is, $(f \circ g) \circ h = f \circ (g \circ h)$. Since this is true for any function, it is true in particular for permutations.

If S is any set we write Sym(S) for the set of all permutations of S. We write $S_n = Sym(1, 2, ..., n)$. This is called the set the <u>symmetric group on n elements</u>.

## 2. Section 3.1

Given a set S we define a binary operation $*$ (placeholder symbol) to be a function $* : S \times S \to S$. Inputs 2 elements of S and outputs 1 element of S.

**Example 2.** Addition on the integers $a + b = +(a, b)$. The "function" addition takes as input two numbers and outputs are integers.

We generally assume our operation is closed meaning it returns something in the same set as our inputs.

Closure is important because we need it to make sure repeated composition is always defined.

Non-example: $S = \{a, b\}$ define $a * b = a$, $a * a = c$, $b * b = c$, and $b * a = b$.
Not closed so not a binary operation on S.
Compute $(a * a) * a = c * a$. This is not defined.

If $*$ is a binary operation (closed) on a set S then we call the set S together with $*$ a magma.
Whenever S is finite its useful to write down a composition table for S.

Write down a table with rows and columns for each element of S then compose two elements. "first element" is the row, "second element" is the column.

**Example 3.** $S = \{a, b, c\}$ Compute $c * a = c$. Any such table gives us a magma.

| $*$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $a$ | $b$ |
| $b$ | $b$ | $b$ | $c$ |
| $c$ | $c$ | $b$ | $a$ |

We typically want our operations $*$ to be associative.
$(a * b) * c = a * (b * c)$ for any a,b,c in S.
Parentheses aren't necessary to determine "order of computation".
An associative magma is called a semigroup.

**Definition 2.** If $*$ is a binary operation on S we call e an identity element if $a * e = e * a = a$ for all $a \in S$.

**Proposition 2.** If e is an identity of $(S, *)$ then it is the unique identity element.

*Proof.* Suppose for a contradiction that $S, *$ have two distinct identity elements ($e_1 \neq e_2$). Call them $e_1, e_2$. Since $e_1$ is an identity $e_1 * e_2 = e_2$. But since $e_2$ is an identity $e_1 * e_2 = e_1$, but then $e_1 = e_2$ which is a contradiction. $\square$

**Definition 3.** A semigroup with an identity element is called a monoid.

**Example 4.** $\mathbb{Z}_{\geq 0} = \mathbb{N} = \{0, 1, 2, 3, ...\}$ and the operation $+$ is a monoid.

**Definition 4.** If $(S, *)$ is a set with binary operation and an identity element e we call the inverse of an element a $a^{-1}$ if $a * a^{-1} = a^{-1} * a = e$.

**Definition 5.** If $(S, *)$ is a monoid where every element has an inverse then we call it a group. Equivalently a group is a set S together with a binary operation that is
1) Closed
2) Associative
3) Has an identity element
4) Every element has an inverse

If $(S, *)$ is a magma where the equation $a * x = b$ has a unique solution $x$ for any $a$ and $b$ in $S$. Then we call $(S, *)$ a quasigroup.

A quasigroup with an identity is called a loop.

A group is an associative loop.