Linear Algebra 1: Lecture 5

Irena Penev

Winter 2022/2023

Notation: We denote by $\mathbb{N}$ the set of all positive integers, and we denote by $\mathbb{N}_0$ the set of all non-negative integers.

1 Monoids

A *monoid* is an ordered pair $(S, \circ)$, where S is a set and $\circ$ is a binary operation on S (.e. $\circ : S \times S \to S$) satisfying the following two properties:

1. the operation $\circ$ is associative, i.e. for all $a, b, c \in S$, we have that
$$a \circ (b \circ c) = (a \circ b) \circ c;$$
2. there exists some $e \in S$, called the *identity element* of $(S, \circ)$, such that for all $a \in S$, we have that
$$e \circ a = a \quad \text{and} \quad a \circ e = a.$$

Proposition 1.1. *Let $(S, \circ)$ be a monoid. Then the identity element of $(S, \circ)$ is unique.*

Proof. Suppose that e_1, e_2 are identity elements of $(S, \circ)$.[1] Then
$$e_1 \overset{(*)}{=} e_1 \circ e_2 \overset{(**)}{=} e_2$$
where (*) follows from the fact that e_2 is the identity element of the monoid $(S, \circ)$, and (**) follows from the fact that e_1 is the identity element of the monoid $(S, \circ)$. So, the identity element of the monoid $(S, \circ)$ is unique. □

Example 1.2. *Here are some examples of monoids:*

[1] This means that the following hold:
- for all $a \in S$, we have that $e_1 \circ a = a$ and $a \circ e_1 = a$;
- for all $a \in S$, we have that $e_2 \circ a = a$ and $a \circ e_2 = a$.

1. $(\mathbb{N}_0, +)$;
2. $(\mathbb{Z}, +)$;
3. $(\mathbb{Q}, +)$;
4. $(\mathbb{R}, +)$;
5. $(\mathbb{C}, +)$.

In all the examples above, 0 *is the identity element.*

Note, however, that $(\mathbb{N}, +)$ is **not** a monoid (where $\mathbb{N}$ is the set of all positive integers), since it does not have an identity element.

Example 1.3. *Here are some examples of monoids ("$\cdot$" denotes multiplication):*

1. $(\mathbb{N}_0, \cdot)$;
2. $(\mathbb{N}, \cdot)$;
3. $(\mathbb{Z}, \cdot)$;
4. $(\mathbb{Q}, \cdot)$;
5. $(\mathbb{R}, \cdot)$;
6. $(\mathbb{C}, \cdot)$.

In all the examples above, 1 *is the identity element.*

Example 1.4. *Here are some examples of monoids ("$\cdot$" denotes multiplication):*

1. $(\mathbb{N}, \cdot)$;
2. $(\mathbb{Z} \setminus \{0\}, \cdot)$;
3. $(\mathbb{Q} \setminus \{0\}, \cdot)$;
4. $(\mathbb{R} \setminus \{0\}, \cdot)$;
5. $(\mathbb{C} \setminus \{0\}, \cdot)$.

In all the examples above, 1 *is the identity element.*

2 Groups

A *group* is an ordered pair $(G, \circ)$, where G is a set and $\circ$ is a binary operation on G (i.e. $\circ : G \times G \to G$) satisfying the following three properties:

1. the operation $\circ$ is associative, i.e. for all $a, b, c \in G$, we have that
$$a \circ (b \circ c) = (a \circ b) \circ c;$$
2. there exists some $e \in G$, called the *identity element* of $(G, \circ)$, such that for all $a \in G$, we have that
$$e \circ a = a \quad \text{and} \quad a \circ e = a;$$
3. for all $a \in G$, there exists some $a' \in G$, called the *inverse* of a, such that
$$a \circ a' = e \quad \text{and} \quad a' \circ a = e.$$

An *abelian group* is a group $(G, \circ)$ that satisfies the following additional condition:

4. the operation $\circ$ is commutative, i.e. for all $a, b \in G$, we have that

$$a \circ b \quad = \quad b \circ a.$$

Remark: Note that the first two axioms (axioms 1. and 2.) from the definition of a group are precisely the monoid axioms. So, every group is a monoid. By Proposition 1.1, it follows that the identity element e of a group is unique. In particular, the third axiom (axiom 3.) makes sense.

Proposition 2.1. *Let $(G, \circ)$ be a group, and let $g \in G$. Then the inverse of g is unique.*

Proof. Let e be the identity element of the group G. Fix $g \in G$. Let g_1 and g_2 be inverses of G.[2] Then

$$\begin{aligned}
g_1 &= g_1 \circ e && \text{because } e \text{ is the identity element of } (G, \circ) \\
&= g_1 \circ (g \circ g_2) && \text{because } g_2 \text{ is an inverse of } g \\
&= (g_1 \circ g) \circ g_2 && \text{because } \circ \text{ is associative} \\
&= e \circ g_2 && \text{because } g_1 \text{ is an inverse of } g \\
&= g_2 && \text{because } e \text{ is the identity element of } (G, \circ).
\end{aligned}$$

We have now shown that $g_1 = g_2$. So, the inverse of g is unique. □

Notation: Typically, the (unique) inverse of an element g of a group $(G, \circ)$ is denoted by g^{-1}. However, when the group operation is denoted by $+$ (note: this is only done if the group is abelian), then the inverse of an element g is denoted by $-g$.

Example 2.2. *All the following are abelian groups:*

1. $(\mathbb{Z}, +)$;
2. $(\mathbb{Q}, +)$;
3. $(\mathbb{R}, +)$;
4. $(\mathbb{C}, +)$.

In each of the above cases, the identity element is 0*, and the inverse of a group element g is $-g$.*[3]

Note that the monoid $(\mathbb{N}_0, +)$ is **not** a group because elements other than 0 do not have inverses, and so the third axiom is not satisfied.

Example 2.3. *All the following are abelian groups:*

[2] This means that both of the following hold:

- $g \circ g_1 = e$ and $g_1 \circ g = e$;
- $g \circ g_2 = e$ and $g_2 \circ g = e$.

[3] For example, in the group $(\mathbb{R}, +)$, the inverse of $\sqrt{13}$ is $-\sqrt{13}$.

1. $(\mathbb{Q} \setminus \{0\}, \cdot)$*;* *2.* $(\mathbb{R} \setminus \{0\}, \cdot)$*;* *3.* $(\mathbb{C} \setminus \{0\}, \cdot)$*;*

In each of the above cases, the identity element is 1*, and the inverse of a group element* g *is* $g^{-1} = \frac{1}{g}$*.*[4]

Note that the monoids $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, and $(\mathbb{C}, \cdot)$ are **not** groups because, in each of those cases, 0 does not have the inverse element. Note also that $(\mathbb{Z} \setminus \{0\}, \cdot)$ is **not** a group because elements other than 1 and -1 do not have inverses.

It might now seem that all groups are abelian. However, this is not the case, as we shall see in section 3, when we study the "symmetric group."

Let us now prove some elementary properties of groups.

Proposition 2.4. *Let* $(G, \circ)$ *be a group with identity element* e*. Then all the following hold (here, the inverse of a group element* g *is denoted by* g^{-1}*):*

(a) for all $a, b, c \in G$*, if* $a \circ b = a \circ c$*, then* $b = c$*;*

(b) for all $a, b, c \in G$*, if* $b \circ a = c \circ a$*, then* $b = c$*;*

(c) for all $a, b \in G$*, there exists a unique* $x \in G$ *such that* $a \circ x = b$*;*

(d) for all $a, b \in G$*, there exists a unique* $x \in G$ *such that* $x \circ a = b$*;*

(e) for all $a \in G$*,* $(a^{-1})^{-1} = a$*;*[5]

(f) for all $a, b \in G$*,* $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$*.*

Proof. We first prove (a). Fix $a, b, c \in G$, and assume that $a \circ b = a \circ c$. Then

$$
\begin{aligned}
b &= e \circ b && \text{because } e \text{ is the identity element of } (G, \circ) \\
&= (a^{-1} \circ a) \circ b && \text{because } a^{-1} \circ a = e \\
&= a^{-1} \circ (a \circ b) && \text{because } \circ \text{ is associative} \\
&= a^{-1} \circ (a \circ c) && \text{because } a \circ b = a \circ c \\
&= (a^{-1} \circ a) \circ c && \text{because } \circ \text{ is associative} \\
&= e \circ c && \text{because } a^{-1} \circ a = e \\
&= c && \text{because } e \text{ is the identity element of } (G, \circ).
\end{aligned}
$$

This proves (a). The proof of (b) is similar.

[4]For example, in the group $(\mathbb{R}, \cdot)$, the inverse of $\sqrt{13}$ is $\frac{1}{\sqrt{13}}$.

[5]So, the inverse of the inverse of a is equal to a.

Next, we prove (c). Fix $a, b \in G$. We must show that there exists a unique $x \in G$ such that $a \circ x = b$. For existence, we set $x := a^{-1} \circ b$, and we observe that

$$\begin{aligned} a \circ x &= a \circ (a^{-1} \circ b) && \text{because } x = a^{-1} \circ b \\ &= (a \circ a^{-1}) \circ b && \text{because } \circ \text{ is associative} \\ &= e \circ b && \text{because } a \circ a^{-1} = e \\ &= b && \text{becuase } e \text{ is the identity element of } (G, \circ). \end{aligned}$$

Uniqueness follows from (a). This proves (c). The proof of (d) is similar.

We now prove (e). Fix $a \in G$. It suffices to show that $a^{-1} \circ (a^{-1})^{-1} = a^{-1} \circ a$, for then (a) will guarantee that $(a^{-1})^{-1} = a$, which is what we need. Since $(a^{-1})^{-1}$ is the inverse of a^{-1}, we know that $a^{-1} \circ (a^{-1})^{-1} = e$. On the other hand, since a^{-1} is the inverse of a, we have that $a^{-1} \circ a = e$. Thus, $a^{-1} \circ (a^{-1})^{-1} = a^{-1} \circ a$. As explained above, this implies that $(a^{-1})^{-1} = a$. This proves (e).

It remains to prove (f). Fix $a, b \in G$. We observe that

$$\begin{aligned} (a \circ b) \circ (b^{-1} \circ a^{-1}) &= a \circ (b \circ b^{-1}) \circ a && \text{because } \circ \text{ is associative} \\ &= a \circ e \circ a^{-1} && \text{because } b \circ b^{-1} = e \\ &= a \circ a^{-1} && \text{because } e \text{ is the identity element of } (G, \circ) \\ &= e && \text{because } a \circ a^{-1} = e, \end{aligned}$$

and similarly,

$$\begin{aligned} (b^{-1} \circ a^{-1}) \circ (a \circ b) &= b^{-1} \circ (a^{-1} \circ a) \circ b && \text{because } \circ \text{ is associative} \\ &= b^{-1} \circ e \circ b && \text{because } a^{-1} \circ a = e \\ &= b^{-1} \circ b && \text{because } e \text{ is the identity element of } (G, \circ) \\ &= e && \text{because } b^{-1} \circ b = e. \end{aligned}$$

We have now shown that $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$ and $(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$. It follows that $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$. This proves (f). □

2.1 Subgroups

A *subgroup* of a group $(G, \circ)$ is a group $(H, \diamond)$ such that $H \subseteq G$ and for all $a, b \in H$, we have that $a \diamond b = a \circ b$. If $(H, \diamond)$ is a subgroup of $(G, \circ)$, we write $(H, \diamond) \leq (G, \circ)$.

Example 2.5. *Every group $(G, \circ)$ has at least two (trivial) subgroups: $(G, \circ)$ and $(\{e\}, \circ)$, where e is the identity element of G.*

Example 2.6. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

3 Permutations and the symmetric group

A *permutation* of a set X is any bijection from X to itself. The set of all permutations of X is denoted by $\mathrm{Sym}(X)$. As usual, Id_X is the identity function on X, i.e. $Id_X : X \to X$ is given by $Id_X(x) = x$ for all $x \in X$.

Note that for any set X, $(\mathrm{Sym}(X), \circ)$ is a group, called the *symmetric group on X* (here, $\circ$ is the composition of functions). Clearly, $\circ$ is associative; indeed, for any $\pi, \sigma, \tau \in \mathrm{Sym}(X)$, we have that $\pi \circ (\sigma \circ \tau) = (\pi \circ \sigma) \circ \tau$, because for all $x \in X$, we have

$$\begin{aligned}
\Big(\pi \circ (\sigma \circ \tau)\Big)(x) &= \pi\Big(\sigma \circ \tau)(x)\Big) \\
&= \pi\Big(\sigma(\tau(x))\Big) \\
&= (\pi \circ \sigma)(\tau(x)) \\
&= \Big((\pi \circ \sigma) \circ \tau\Big)(x).
\end{aligned}$$

The identity element of the group is the identity function Id_X on X. The inverse element of any $\pi \in \mathrm{Sym}(X)$ is the inverse permutation π^{-1} (since permutations are bijections, they have inverse functions).

If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian. However, if X has at least three elements, then X is **not** abelian, as we now show. Suppose $|X| \geq 3$, and let a, b, c be pairwise distinct elements of X. Let $\sigma, \tau : X \to X$ be defined as follows:[6]

- $\sigma(a) = b$, $\sigma(b) = a$, and $\sigma(x) = x$ for all $x \in X \setminus \{a, b\}$;
- $\tau(a) = c$, $\tau(c) = a$, and $\tau(x) = x$ for all $x \in X \setminus \{a, c\}$.

Clearly, $\sigma, \tau \in \mathrm{Sym}(X)$. But now

[6]The permutation σ swaps ("transposes") a and b, while leaving all other elements of X fixed. Similarly, the permutation τ swaps ("transposes") a and c, while leaving all other elements of X fixed. For more on transpositions, see subsection 3.3.

- $(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(c) = c$;
- $(\tau \circ \sigma)(a) = \tau(\sigma(a)) = \tau(b) = b$.

Since $b \neq c$, we have that $(\sigma \circ \tau)(a) \neq (\tau \circ \sigma)(a)$. So, $\sigma \circ \tau \neq \tau \circ \sigma$.

We particularly often consider $\mathrm{Sym}(X)$ for the case when $X = \{1, \ldots, n\}$ for some positive integer n. The set $\mathrm{Sym}(\{1, \ldots, n\})$ is also denoted by $\mathrm{Sym}(n)$, Sym_n, or S_n. The group $(S_n, \circ)$ is called the *symmetric group of degree* n. Note that $|S_n| = n!$.

A permutation $\pi \in S_n$ can be represented in the following way:

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}.$$

So, in the top row, we have numbers $1, 2, \ldots, n$, and in the bottom row, we have those same numbers in some order (determined by the permutation π). For example, the permutation $\pi : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ in S_4 given by $\pi(1) = 3$, $\pi(2) = 2$, $\pi(3) = 4$, and $\pi(4) = 1$ can be represented as follows:

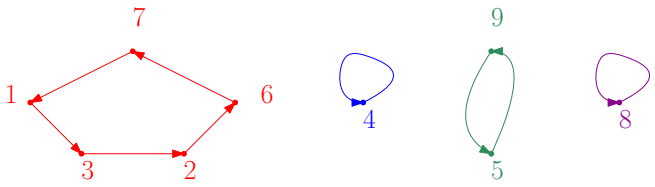
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

3.1 Cycle notation

Suppose we are given the following permutation in S_9.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 2 & 4 & 9 & 7 & 1 & 8 & 5 \end{pmatrix}.$$

We can represent this permutation geometrically, as shown below (the cycles are color coded for easier reference).



We can "encode" the picture that we obtained as a "product of disjoint cycles":

$$\pi = (13267)(4)(59)(8).$$

The above is also referred to as a "disjoint cycle decomposition" of the permutation π. Disjoint cycle decomposition is unique up to cyclic permutation of the elements within each cycle, and the changing of order of different cycles. For example, we also have

$$\pi = (95)(26713)(8)(4).$$

However, the first disjoint cycle decomposition[7] is canonical/standard because it satisfies the following two properties:

- within each cycle, the smallest number appears first;
- the first elements of the cycles from the disjoint cycle decomposition form an increasing sequence.[8]

Usually, the canonical representation is preferred, but occasionally, it may be more practical to use a non-canonical one. When the n from S_n is clear from context, one-element cycles may be omitted. So, if we know that we are working in S_9, then we may omit the one-element cycles (4) and (8) from the representation above, and write simply

$$\pi \quad = \quad (13267)(59).$$

In this case, the cycles (4) and (8) are understood from context. However, we can only do this when n has been specified beforehand! Otherwise, cycles of length one must be included.

Notation: When there is danger of confusion, we put commas between elements within cycles. For instance, if we are working in S_{12}, then (123) is ambiguous. To avoid ambiguity, we write $(1, 2, 3)$ or $(12, 3)$, as appropriate. However, if we are working in S_n, where n is a single-digit number, then there is no danger of confusion, and so we normally avoid parentheses.

Let us consider some more examples.

Example 3.1. *Find the disjoint cycle decompositions of the following permutations.*

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}$

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$

Solution. We have:

(a) $\pi_1 = (125)(34)$;

(b) $\pi_2 = (134)(2)(56)$;

(c) $\pi_3 = (12543)$.

Note that in (b), we could also have written $\pi \in S_6$, $\pi = (134)(56)$. □

[7] That is, the disjoint cycle decomposition $\pi = (13267)(4)(59)(8)$.

[8] Indeed, $1 < 4 < 5 < 8$.

It is also easy to go the other way around: from the disjoint cycle decomposition to the table representation, i.e. representation of the form

$$\pi \quad = \quad \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}.$$

For instance, we see that

$$(143)(26)(5) \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}$$

and

$$(154362) \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 3 & 4 & 2 \end{pmatrix}.$$

Clearly, the composition of two or more permutations in S_n is another permutation in S_n. For instance, in S_5, we have the following (with permutations color coded for easier reference):

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

As usual with function decomposition, we apply permutations from right to left with respect to $\circ$. So, in the case above, we first apply the blue permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$, and then we apply the red permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$. So, for instance, 1 first gets mapped to 2 via the blue permutation, and then 2 gets mapped to 3 via the red permutation. So, the composition above maps 1 to 3.

We can similarly compose permutations given by cycle permutations. For instance,

$$(1)(23)(45) \circ (124)(35) \quad = \quad (134)(25).$$

Again we apply permutations from right to left with respect to $\circ$. So, in the case above, we first apply the blue permutation $(124)(35)$, and then we apply the red permutation $(1)(23)(45)$. However, within each permutation (separated by $\circ$'s from the other permutations), we read from the left to right. For instance, in the blue permutation $(124)(35)$, 1 gets mapped to 2, 2 gets mapped to 4, and 4 gets mapped to 1.

Again, when the n from S_n is clear from context, we may omit one-element cycles. For instance, in S_5, we have

$$(154) \circ (245)(13) \circ (25) \quad = \quad (135).$$

Here, certain one-element cycles are understood from context. For instance, $(154) = (154)(2)(3)$, $(25) = (1)(25)(3)(4)$, and $(135) = (135)(2)(4)$. So, the above expression can be rewritten as

$$(154)(2)(3) \circ (245)(13) \circ (1)(25)(3)(4) \quad = \quad (135)(2)(4).$$

We note that we can obtain the inverse of a permutation π in S_n by starting with a disjoint cycle permutation of π, and then reversing the order of elements in all cycles, i.e. turning each cycle of the form $(a_1 a_2 \dots a_k)$ into $(a_k \dots a_2 a_1)$. For example, in S_7:

- if $\pi_1 = (143)(2576)$, then $\pi_1^{-1} = (341)(6752) = (134)(2675)$;
- if $\pi_2 = (15)(2)(3476)$, then $\pi_2^{-1} = (51)(2)(6743) = (15)(2)(3674)$.

Notation: The identity permutation in S_n is often denoted simply by 1. So, in this context, we have that

$$1 \quad = \quad (1)(2)\dots(n).$$

3.2 The sign of a permutation

Given a positive integer n and a permutation $\pi \in S_n$, the *sign* of π, denoted by $\mathrm{sgn}(\pi)$, is given by

$$\mathrm{sgn}(\pi) \quad = \quad (-1)^{n-k},$$

where k is the number of cycles in the disjoint cycle decomposition of π **including the one-element cycles**. For instance, for $\pi_1 = (1367)(2)(45)$ in S_7, we have

$$\mathrm{sgn}(\pi_1) \quad = \quad (-1)^{7-3} \quad = \quad 1,$$

whereas for $\pi_2 = (12)(345)(6)(7)$ in S_7, we have

$$\mathrm{sgn}(\pi_2) \quad = \quad (-1)^{7-4} \quad = \quad -1.$$

Equivalently, for $\pi \in S_n$, we have that

$$\mathrm{sgn}(\pi) \quad = \quad (-1)^{n'-k'},$$

where k' is the number of cycles in some disjoint cycles in some disjoint cycle decomposition of π (possibly with some one-element cycles omitted), and n' is the number of elements in those k' cycles. The two definitions are equivalent because if d is the number of omitted one-element cycles in some disjoint cycle decomposition of π , then $n = n' + d$, and if we write the complete disjoint cycle representation of π involving all one-element cycles, then we get $k = k' + d$ cycles. So, $n - k = n' - k'$, and consequently, $(-1)^{n-k} = (-1)^{n'-k'}$. For instance, for $\pi_3 = (123)(45)$ in S_7, we have

$$\mathrm{sgn}(\pi_3) \quad = \quad (-1)^{5-2} = -1.$$

Note that the one-element cycles (6) and (7) are implicitly understood for π_3, that is, $\pi_3 = (123)(45)(6)(7)$. And indeed, we have

$$\mathrm{sgn}(\pi_3) \quad = \quad (-1)^{7-4} = -1,$$

as before.

Permutations whose sign is $+1$ are called *even*, and permutations whose sign is -1 are called *odd*.

Note that the sign of the identity permutation is $+1$, and so the identity permutation 1 is even.

Proposition 3.2. *Let $n \geq 2$ be an integer, and let π be a permutation in S_n. Then $sgn(\pi^{-1}) = sgn(\pi)$.*

Proof. This follows from the fact that π and π^{-1} have the same number of cycles in their disjoint cycle representations. □

3.3 Transpositions

Slightly informally, a transposition is a permutation that swaps two elements and fixes all the remaining ones. More formally, given an integer $n \geq 2$, a *transposition* in S_n is a permutation $\pi \in S_n$ such that there exist distinct $i, j \in \{1, \ldots, n\}$ such that $\pi(i) = j$, $\pi(j) = i$, and $\pi(\ell) = \ell$ for all $\ell \in \{1, \ldots, n\} \setminus \{i, j\}$. Such a transposition is denoted by (ij) (here, $n - 2$ one-element cycles are implicitly understood). For instance, the following permutation in S_5 is a transposition:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} \quad = \quad (25)$$

is a transposition. Note that this transposition could also have been written in the form $(1)(25)(3)(4)$. More commonly, one-element cycles are omitted.

Note that the sign of any transposition is -1, and so transpositions are odd.

As we shall see, for $n \geq 2$, any permutation can be written as a composition of transpositions. For instance, in S_7, we have

$$(134)(2657) \quad = \quad (13) \circ (34) \circ (26) \circ (65) \circ (57)$$

This works in general, as the following proposition shows.

Proposition 3.3. *Let $n \geq 2$ be an integer. Then any permutation in S_n can be written as a composition of transpositions.*

Proof. The identity permutation in S_n can be written in the form $(12) \circ (12)$. Let us now suppose that π is some permutation in S_n other than the identity. Then π can be written as the product of one or more disjoint cycles of length at least two (one-element cycles are omitted in our expression, but are understood from context). Let us say we have k cycles of length at least two, as follows (to help the reader, the cycles are color coded):

$$\pi \quad = \quad (a_1^1 a_2^1 \ldots a_{\ell_1}^1) \ldots (a_1^k a_2^k \ldots a_{\ell_k}^k),$$

where the a_i^j's are pairwise distinct, and $\ell_1, \ldots, \ell_k \geq 2$. But then we have

$$\pi \;=\; (a_1^1 a_2^1) \circ (a_2^1 a_3^1) \circ \cdots \circ (a_{\ell_1 - 1}^1 a_{\ell_1}^1) \circ \cdots \circ (a_1^k a_2^k) \circ (a_2^k a_3^k) \circ \cdots \circ (a_{\ell_k - 1}^k a_{\ell_k}^k),$$

and so π is the composition of transpositions. □

Example 3.4. *Express each of the following permutations in S_6 as the composition of transpositions.*

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 3 & 4 & 6 \end{pmatrix}$;

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$;

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix}$.

Solution. To help the reader, we color code the cycles that we obtain, as well as the transpositions that correspond to them.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 3 & 4 & 6 \end{pmatrix} = (2543) = (25) \circ (54) \circ (43)$;

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix} = (12)(456) = (12) \circ (45) \circ (56)$;

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix} = (135)(264) = (13) \circ (35) \circ (26) \circ (64)$.

□

We note that the same permutation can be expressed as the composition of transpositions in more than one way. For instance, in S_5, we have:

- $(12345) = (12) \circ (23) \circ (34) \circ (45)$
- $(12345) = (15) \circ (14) \circ (13) \circ (12)$.

However, as we shall see, for any given permutation π in S_n, where $n \geq 2$, in all representations of π as compositions of transpositions, the number of transpositions is of the same parity (i.e. it is either always odd or always even). We prove this in Proposition 3.6. However, to prove Proposition 3.6, we need the following technical proposition, which states that composing a permutation with a transposition changes the sign of the permutation.

Proposition 3.5. *Let $n \geq 2$ be an integer, let $\pi \in S_n$, and let $i, j \in \{1, \ldots, n\}$ be distinct. Then $sgn\Big((ij) \circ \pi\Big) = -sgn(\pi)$.*

Proof. We consider the disjoint cycle decomposition of π (with one-element cycles included). There are two cases to consider: when i and j are in the same cycle, and when they are in different cycles.

Case 1: i and j are in the same cycle of the disjoint cycle decomposition of π. After possibly swapping the order of our disjoint cycles, and cyclically permuting the elements of the cycle that contains i and j, we may assume that our disjoint cycle decomposition of π is given by

$$\pi \quad = \quad (i\ a_1 \dots a_p\ j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r).$$

Note: Here, i and j are both in the red cycle. The remaining cycles (the ones that do not contain i and j) are colored blue.[9]

In the permutation $(ij) \circ \pi$, the red cycle essentially gets "split up" into two, while the blue cycles remain unaffected, as follows:

$$\begin{aligned}(ij) \circ \pi \quad &= \quad (ij) \circ (i\ a_1 \dots a_p\ j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r) \\ &= \quad (i\ a_1 \dots a_p)(j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r)\end{aligned}$$

But now the disjoint cycle decomposition of $(ij) \circ \pi$ has one cycle more than the disjoint cycle decomposition of π, and it follows that $\operatorname{sgn}\Big((ij) \circ \pi\Big) = -\operatorname{sgn}(\pi)$,[10] which is what we needed to show.

Case 2: i and j are in different cycles of the disjoint cycle decomposition of π. After possibly swapping the order of our disjoint cycles, and cyclically permuting the elements of the cycle that contains i and j, we may assume that our disjoint cycle decomposition of π is given by

$$\pi \quad = \quad (i\ a_1 \dots a_p)(j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r)$$

Note: Here, i and j are in the two red cycles. The remaining cycles (the ones that do not contain i and j are colored blue.[11]

In the permutation $(ij) \circ \pi$, the two red cycles essentially get "merged" into one, while the blue cycles remain unaffected, as follows:

$$(ij) \circ \pi \quad = \quad (i\ a_1 \dots a_p\ j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r).$$

[9] It is possible that $r = 0$, so that π consists only of the red cycle. It is also possible that $p = 0$ (in this case, the red cycle is $(i\ j\ b_1 \dots b_q)$), or that $q = 0$ (in this case, the red cycle is $(i\ a_1 \dots a_p\ j)$). If $p = q = 0$, then the red cycle is simply (ij).

[10] Indeed, the disjoint cycle decomposition of π has $r + 1$ cycles, and the disjoint cycle decomposition of $(ij) \circ \pi$ has $r + 2$ cycles. So,

$$\operatorname{sgn}\Big((ij) \circ \pi\Big) \quad = \quad (-1)^{n-(r+2)} \quad = \quad (-1)^{n-(r+1)-1} \quad = \quad -(-1)^{n-(r+1)} \quad = \quad -\operatorname{sgn}(\pi).$$

[11] It is possible that $p = 0$, $q = 0$, or $r = 0$. Similar remarks apply as in Case 1.

But now the disjoint cycle decomposition of $(ij) \circ \pi$ has one cycle less than the disjoint cycle decomposition of π, and it follows that $\operatorname{sgn}\Big((ij) \circ \pi\Big) = -\operatorname{sgn}(\pi)$,[12] which is what we needed to show. □

Proposition 3.6. *Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then*

(1) $sgn(\pi) = (-1)^r$;

(2) π is an even permutation if and only if r is even;

(3) π is an odd permutation if and only if r is odd.

Proof. Clearly, (2) and (3) follow from (1). Statement (1) follows from Proposition 3.5 by an easy induction on r. Let us give the details. We prove the following statement: "for every positive integer r and permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\operatorname{sgn}(\pi) = (-1)^r$."

Base case: $r = 1$. Note that if π is the composition of one transposition (i.e. π itself is a transposition), then $\operatorname{sgn}(\pi) = (-1)^{2-1} = (-1)^r$.

Induction step: Fix a positive integer r, and assume that for any permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\operatorname{sgn}(\pi) = (-1)^r$. Now, fix a permutation $\pi \in S_n$ in S_n such that π can be expressed as the composition of $r+1$ transpositions, say $\pi = (a_0 a_0') \circ (a_1 a_1') \circ \cdots \circ (a_r a_r')$. Then by the induction hypothesis, $\pi' := (a_1 a_1') \circ \cdots \circ (a_r a_r')$ satisfies $\operatorname{sgn}(\pi') = (-1)^r$. But since $\pi = (a_0 a_0') \circ \pi'$, Proposition 3.5 guarantees that $\operatorname{sgn}(\pi) = -\operatorname{sgn}(\pi')$. So, $\operatorname{sgn}(\pi) = -\operatorname{sgn}(\pi') = -(-1)^r = (-1)^{r+1}$.

This completes the induction. □

Proposition 3.7. *Let $n \geq 2$ be an integer, and let $\sigma, \tau \in S_n$. Then $sgn(\sigma \circ \tau) = sgn(\sigma) sgn(\tau)$.*

Proof. This easily follows from Propositions 3.3 and 3.6. Let us give the details. By Proposition 3.3, we can express σ and τ as compositions of transpositions, say

- $\sigma = (s_1 s_1') \circ (s_2 s_2') \circ \cdots \circ (s_k s_k')$;
- $\tau = (t_1 t_1') \circ (t_2 t_2') \circ \cdots \circ (t_\ell t_\ell')$.

By Proposition 3.6, we have that $\operatorname{sgn}(\sigma) = (-1)^k$ and $\operatorname{sgn}(\tau) = (-1)^\ell$. On the other hand, $\sigma \circ \tau = (s_1 s_1') \circ (s_2 s_2') \circ \cdots \circ (s_k s_k') \circ (t_1 t_1') \circ (t_2 t_2') \circ \cdots \circ (t_\ell t_\ell')$, and so again by Proposition 3.6, we have that $\operatorname{sgn}(\sigma \circ \tau) = (-1)^{k+\ell}$. So, $\operatorname{sgn}(\sigma \circ \tau) = (-1)^{k+\ell} = (-1)^k (-1)^\ell = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$. □

[12] Indeed, the disjoint cycle decomposition of π has $r+2$ cycles, and the disjoint cycle decomposition of $(ij) \circ \pi$ has $r+1$ cycles. So,

$$\operatorname{sgn}\Big((ij) \circ \pi\Big) = (-1)^{n-(r+1)} = (-1)^{n-(r+2)+1} = -(-1)^{n-(r+2)} = -\operatorname{sgn}(\pi).$$

3.4 The alternating group A_n

For an integer $n \geq 2$, let A_n be the set of all even permutations in S_n. Let us show that $(A_n, \circ)$ is a subgroup of $(S_n, \circ)$, where $\circ$ is the composition of functions. Since $A_n \subseteq S_n$, it suffices to show that $(A_n, \circ)$ is a group. First of all, by Proposition 3.7, the composition of two even permutations is even; so, $\circ$ is indeed a binary operation on A_n. Obviously, $\circ$ is associative. Next, the identity function on $\{1, \ldots, n\}$ is even, and therefore, it belongs to A_n; moreover, the identity function on $\{1, \ldots, n\}$ is the identity element of A_n. Finally, by Proposition 3.2, the inverse of an even permutation in S_n is even. So, every element of A_n has an inverse in A_n. Thus, $(A_n, \circ)$ is indeed a group, and therefore, it is a subgroup of $(S_n, \circ)$.

The group $(A_n, \circ)$ is called the *alternating group of degree n*.

We remark that the set of odd permutations in S_n, call it O_n,[13] does **not** form a subgroup of S_n. This is, first of all, because the composition of two odd permutations is even (by Proposition 3.7), and so $\circ$ is not a binary operation on O_n. Alternatively, we note that the identity permutation in S_n is even and therefore does not belong to O_n.

[13] O_n is **not** standard notation for the set of odd permutations in S_n; in fact, no standard notation exists for this set. However, A_n is the standard notation for the set of even permutations in S_n.