# MATH 541: MARCH 21ST AND 23RD NOTES

ANTOINE MARTIN AND TIM SWAST

## 1. March 21st Notes: Defining Sign Homomorphism

**Definition 1.1.** *Let $G, H$ be groups. A function $\varphi : G \to H$ is called a* homomorphism *if it satisfies*

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2), \forall g_1, g_2 \in G$$

Let $S_n$ denote the group of automorphisms, $Aut(\{1, 2, ..., n\})$. We are going to define a homomorphism $sgn : S_n \to \{\pm 1\}$ which is onto. It will be explained later that $sgn$ is the unique function which holds these properties.

### 1.1. Sign for $n = 2$.

Consider the polynomial,

$$D(x_1, x_2) = x_2 - x_1.$$

Let $\sigma \in S_2$. Then one can apply $\sigma$ on the function $D$

$$^{\sigma}D = D(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)})$$

Then,

$$D(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}) = \begin{cases} x_2 - x_1 = D & \text{if } \sigma = id \\ x_1 - x_2 = -D & \text{if } \sigma = (1\ 2) \text{ transpose 1 and 2} \end{cases}$$

We define $sgn(\sigma)$ to be $\pm 1$ such that

$$^{\sigma}D = sgn(\sigma) D$$

**Claim 1.2.** *$sgn$ is a homomorphism (for $n = 2$).*

*Proof.* We wish to verify that $sgn(\sigma_1 \circ \sigma_2) = sgn(\sigma_1) \cdot sgn(\sigma_2)$ for all $\sigma_1, \sigma_2 \in S_2$.

Since there are only two elements of $S_2$, we can verify this by checking.

First, build a multiplication table for $S_2$. Let $\sigma$ indicate the transposition $\left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$.

| | $id$ | $\sigma$ |
|---|---|---|
| $id$ | $id$ | $\sigma$ |
| $\sigma$ | $\sigma$ | $id$ |

Since $sgn(id) = 1$, the only interesting case to test is $sgn(\sigma \circ \sigma) \stackrel{?}{=} sgn(\sigma) \cdot sgn(\sigma)$.

$$\begin{aligned} sgn(\sigma \circ \sigma) &= sgn(id) \\ &= 1 \\ sgn(\sigma) \cdot sgn(\sigma) &= -1 \cdot -1 \\ &= 1 \end{aligned}$$

∎

1.2. **Sign for $n = 3$.** In order to get a better intuition for the general case, consider the sign function over the set $S_3$.

For $n = 3$, the polynomial $D$ is defined in the following way,

$$D(x_1, x_2, x_3) = (x_3 - x_2) \cdot (x_3 - x_1) \cdot (x_2 - x_1).$$

Note, that this is the product of all pairs $x_j - x_k$ where $j > k$.

Let $\sigma \in S_3 = Aut(\{1, 2, 3\})$, then

$${}^{\sigma}D = (x_{\sigma^{-1}(3)} - x_{\sigma^{-1}(2)}) \cdot (x_{\sigma^{-1}(3)} - x_{\sigma^{-1}(1)}) \cdot (x_{\sigma^{-1}(2)} - x_{\sigma^{-1}(1)}).$$

**Claim 1.3.** *${}^{\sigma}D = sgn(\sigma) \cdot D$ where $sgn(\sigma) = \pm 1$.*

*Proof.* We will show that $sgn(\sigma) = (-1)^k$, where

$$k = \#\{i < j | \sigma^{-1}(i) > \sigma^{-1}(j)\}.$$

As an example, if

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

then indeed, $sgn(\sigma) = -1 = (-1)^1$ because

$$\begin{aligned} {}^{\sigma}D &= (x_{\sigma^{-1}(3)} - x_{\sigma^{-1}(2)}) \cdot (x_{\sigma^{-1}(3)} - x_{\sigma^{-1}(1)}) \cdot (x_{\sigma^{-1}(2)} - x_{\sigma^{-1}(1)}) \\ &= (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = -D. \end{aligned}$$

In the general case, for any $\sigma$ consider it acting on a pair of values,

$$\sigma : (x_j - x_i), i < j \mapsto (x_{\sigma^{-1}(j)} - x_{\sigma^{-1}(i)}).$$

Note that the domain of this function is exactly all such pairs that appear in the polynomial $D$. Consider the image of this function. It yields all such pairs which appear in ${}^{\sigma}D$ by definition.

Let the pair $(x_{\sigma^{-1}(j)} - x_{\sigma^{-1}(i)})$ be in the image of the function. Note that $\sigma \in S_n$ is a bijection, then since $i \neq j$, then $\sigma^{-1}(i) \neq \sigma^{-1}(j)$.

If $\sigma^{-1}(i) < \sigma^{-1}(j)$, then $(x_{\sigma^{-1}(j)} - x_{\sigma^{-1}(i)})$ appears in $D$. If $\sigma^{-1}(i) > \sigma^{-1}(j)$, then $-(x_{\sigma^{-1}(j)} - x_{\sigma^{-1}(i)})$ appears in $D$. Therefore, any pair in ${}^{\sigma}D$ appears also in $D$ (by a factor of $-1$).

Also, consider a pair in $D$, $(x_m - x_\ell)$. Note that $\ell < m$. Then, since $\sigma$ is one-to-one and onto, there exists values $i, j$ such that $\sigma^{-1}(j) = m$ and $\sigma^{-1}(i) = \ell$, where $i \neq j$. Thus, either $i < j$ or $j < i$, so any pair in $D$ will then appear in the image of the function and more importantly, in ${}^{\sigma}D$.

Thus, if we set $k$ to be the number of pairs in ${}^{\sigma}D$ such that $i < j$ and $\sigma^{-1}(i) > \sigma^{-1}(j)$, we can write ${}^{\sigma}D = (-1)^k D$. $\square$

As another example, consider

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

Then indeed, $sgn(\sigma) = (-1)^2 = 1$ because

$$\begin{aligned} {}^{\sigma}D &= (x_{\sigma^{-1}(3)} - x_{\sigma^{-1}(2)}) \cdot (x_{\sigma^{-1}(3)} - x_{\sigma^{-1}(1)}) \cdot (x_{\sigma^{-1}(2)} - x_{\sigma^{-1}(1)}) \\ &= (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = (-1)^2 D = D. \end{aligned}$$

$k = 2$, since the following pairs appear in the set $\{i < j | \sigma^{-1}(i) > \sigma^{-1}(j)\}$: $1 < 3 \mapsto \sigma^{-1}(1) > \sigma^{-1}(3) = 3 > 2$ and $1 < 2 \mapsto \sigma^{-1}(1) > \sigma^{-1}(2) = 3 > 1$.

**Claim 1.4.** *$sgn : S_3 \to \{\pm 1\}$ is a homomorphism.*

*Proof (Step 1).* Denote by $\gamma$, the application of $\sigma$ on $P(x)$ a polynomial on $n$ variables by

$$\gamma(\sigma)P(x) \overset{\gamma}{=} P(\sigma^{-1}(x)).$$

Let $\sigma, \tau \in S_n$. We wish to prove that $\gamma(\sigma \circ \tau) = \gamma(\sigma) \circ \gamma(\tau)$. We then have,

$$\begin{aligned}
\gamma(\sigma \circ \tau)P(x) &\overset{\gamma}{=} P((\tau^{-1} \circ \sigma^{-1})(x)) \\
&= P(\tau^{-1}(\sigma^{-1}(x))) \\
&= \underbrace{(\gamma(\tau)P)}_{Q}(\sigma^{-1}(x)) = \gamma(\sigma)Q(x) \\
&= \gamma(\sigma)(\gamma(\tau)P)(x) = (\gamma(\sigma) \circ \gamma(\tau))P(x).
\end{aligned}$$

Therefore,

$$\gamma(\sigma \circ \tau) = \gamma(\sigma) \circ \gamma(\tau).$$

□

*Proof (Step 2).* Obviously, $sgn(id) = 1$.

Let $\sigma, \tau \in S_n$. We wish to show that $sgn(\sigma \circ \tau) = sgn(\sigma) \cdot sgn(\tau)$.

By step 1, Claim **??**, and the definition of $sgn$ as the application on the polynomial $D$,

$$sgn(\sigma \circ \tau) = sgn(\sigma) \cdot sgn(\tau).$$

□

## 2. March 23rd Notes: Uniqueness of Sign Homomorphism

Now, since only definitions for $sgn$ on $S_2$ and $S_3$ have been provided thus far, we will give a general definition for $sgn$.

Define $sgn : S_n \to \{\pm 1\}$ by

$${}^{\sigma}D = sgn(\sigma) \cdot D$$

where

$$D(x_1, \ldots, x_n) = \prod_{n \geq j > i \geq 1} (x_j - x_i)$$

and

$${}^{\sigma}D = D(x_{\sigma^{-1}(1)}, \ldots x_{\sigma^{-1}(n)}) = \prod_{n \geq j > i \geq 1} (x_{\sigma^{-1}(x_j)} - x_{\sigma^{-1}(x_i)}).$$

### 2.1. *sgn* is unique.

**Theorem 2.1.** *There exists a unique onto homomorphism*

$$\varphi : S_n \twoheadrightarrow \{\pm 1\}$$

*Note, that for the purposes of the proof, we will assume the $\varphi(\tau) = -1$ for all transpositions $\tau = (a\ b)$. This assumption is unnecessary and follows from the onto assumption. The proof of this will be shown later.*

*Proof of uniqueness.* The main point is that uniqueness follows from Lemma **??** (page **??**).

Suppose $\varphi$ is an onto homomorphism, where $\varphi : S_n \to \{\pm 1\}$. Also, $\varphi'$ is an onto homomorphism, where $\varphi : S_n \to \{\pm 1\}$.

Take $\sigma \in S_n$. Then by the lemma, $\sigma = \tau_k \circ \ldots \tau_1$. By the assumption of homomorphism,

$$\begin{aligned}
\varphi(\sigma) &= \varphi(\tau_k) \cdot \cdots \cdot \varphi(\tau_1) \\
&= \varphi'(\tau_k) \cdot \cdots \cdot \varphi'(\tau_1) && \text{By the condition that } \varphi(\tau) = \varphi'(\tau) = -1 \\
&= \varphi'(\tau_k \circ \cdots \circ \tau_1) && \text{(homomorphism)} \\
&= \varphi'(\sigma)
\end{aligned}$$

Therefore, $\varphi = \varphi'$.

□

*Proof of existence.* Consider $sgn$. It has been shown that this is a homorphism (Claim **??**). We wish to show that it is also onto.

Consider the transpostion $\tau = (1\ 2) \in S_n = Aut(\{1, 2, \ldots, n\})$. Then the order of $(x_2 - x_1)$ in $D$ switches to $(x_1 - x_2)$ in ${}^{\tau}D$. Since $\tau(i) = i$ for all $i \notin \{1, 2\}$, this is the only pair whose order is affected. Thus, ${}^{\tau}D = -D$. So $sgn(\tau) = -1$.

Therefore, $sgn$ is onto. □

For example, consider the transposition $\tau = (1\ 2) \in S_3$. Then

$$(x_2 - x_1) \to (x_1 - x_2)$$
$$(x_3 - x_1) \to (x_3 - x_2)$$
$$(x_3 - x_2) \to (x_3 - x_1)$$

So, $k = 1$ and $sgn(\tau) = -1$.

### 2.2. **Supporting Lemmas and Definitions.**

**Lemma 2.2.** *For all $\sigma \in S_n$, $\exists$ a decomposition of $\sigma = \tau_\ell \circ \ldots \tau_1$ (where $\tau_i$ are transpositions) for some $\ell$. Also, this $\ell$ has unique* **parity***. i.e. for any two decompositions of lengths $\ell$ and $m$, then $2|(\ell - m)$.*

*Proof (step 1).* Every $\sigma \in S_n$ can be written (uniquely up to change of order) as a product of cycles.

$$\sigma = c_m \circ \cdots \circ c_1$$

The proof of this will be shown later.

**Definition 2.3.** *Let $c \in S_n$. This bijection is called a* **cycle** *if it is of the form*

$$c = (a_1\ a_2\ \ldots\ a_t),\ 1 \le a_i \le n,\ i \in \{1, \ldots, t\}$$

*with $c(a_1) = a_2, c(a_2) = a_3, \ldots c(a_t) = a_1$ and identity ($k \mapsto k$) for all other, $k \in \{1, \ldots, n\}, k \neq a_i, i \in \{1, \ldots, t\}$.*

□

For example, take

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

Then, $\sigma = (1\ 2\ 3) \circ (4\ 5)$.

*Proof (step 2).* Every cycle can be written as a composition of transpositions.

Indeed, consider $c = (a_1\ a_2\ a_3\ \ldots\ a_t)$. Then, $c = (a_1\ a_2) \circ (a_2\ a_3) \circ \cdots \circ (a_{t-1}\ a_t)$.

To verify, consider $a_{i-1}, a_i$, $i < t$. Then following the order of transpositions from right to left, $a_i$ is placed into position $a_{i+1}$, then $a_{i-1}$ is placed into position $a_i$, which is never seen again in the following transpositions. Also, $a_t$ is transposed to $a_{t-1}$, then the next and so on, until it reaches the position $a_1$. □

*Proof (step 3).* Let $\sigma \in S_n$. Consider two decompositions into transpositions of $\sigma$,

$$\tau_1 \circ \cdots \circ \tau_\ell = \sigma = \tau_1' \circ \cdots \circ \tau_m'$$

By the properties of a homomorphism and the fact that $sgn(\tau) = -1$ for any transposition, $\tau$,

$$(-1)^\ell = sgn(\sigma) = (-1)^m$$
$$(-1)^{\ell - m} = 1$$

Therefore, we must have $2|\ell - m$. i.e. The parity of $\ell$ and $m$ are the same. □