Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

March 13, 2023

Last time, we have constructed permutations α, β, and γ such that

$$\gamma = \beta \circ \alpha.$$

We have shown

$$\operatorname{sign}(\alpha) = \left(\frac{p}{q}\right) \qquad \text{and} \qquad \operatorname{sign}(\beta) = \left(\frac{q}{p}\right)$$

using Theorem 23.8 ($\operatorname{sign}(g \circ f) = \operatorname{sign}(g) \cdot \operatorname{sign}(f)$).

It remains to

- prove Theorem 23.8, and
- show that $\operatorname{sign}(\gamma) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

Permutation Group

Permutation Group

Definition 24.1

The ***permutation group*** of a set X is the set of permutations of X equipped with the binary operation “composition” and the neutral element id_X. This group is denoted by $\mathrm{Perm}(X)$, $\mathrm{Sym}(X)$, or $\mathfrak{S}(X)$.

It is not difficult to see that any permutation is a composition of cycles. Furthermore, we would like to find a system of ***generators***.

Definition 24.2

A 2-cycle is called a ***transposition***.

Theorem 24.3

Any permutation is an iterated composition of transpositions.

Proof. We only need to show prove this for a cycle, saying $(a_1 a_2 \cdots a_n)$. We may simply write* it as $(12 \cdots n)$.

Then one can verify that $(12 \cdots n) = (12)(23) \cdots (n-1n)$. $\square$

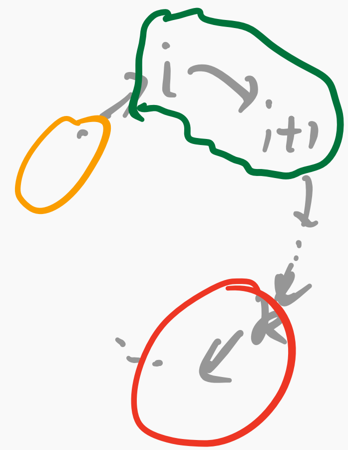
*From now on, we are in the field of abstract algebra. A guideline is: what matters are structures, not elements.

How to verify $(12\cdots n) = (12)(23)\cdots(n-1n)$

We can track an individual $i \in \{1, \cdots, n\}$ under the actions.

First, $(12\cdots n)$ maps i to $i+1$ (Note that we would think $n+1$ as 1.)

When $k > i$, the transposition $(kk+1)$ fixes i. Hence,



$$(i+1i+2)\cdots(n-1n).i = i.$$

Then $(ii+1)$ maps i to $i+1$. So,

$$(ii+1)\cdots(n-1n).i = i+1.$$

The rest transpositions (i.e. $(kk+1)$ with $k < i$) fix $i+1$. Hence,

$$(12)\cdots(n-1n).i = i+1.$$

We thus conclude $(12\cdots n) = (12)(23)\cdots(n-1n)$.

Sign and Transpositions

By the definitions, the sign of a transposition is always -1.

We want to prove the following special case of Theorem 23.8.

Lemma 24.4

Let f be a permutation and τ a transposition of the same set. Then

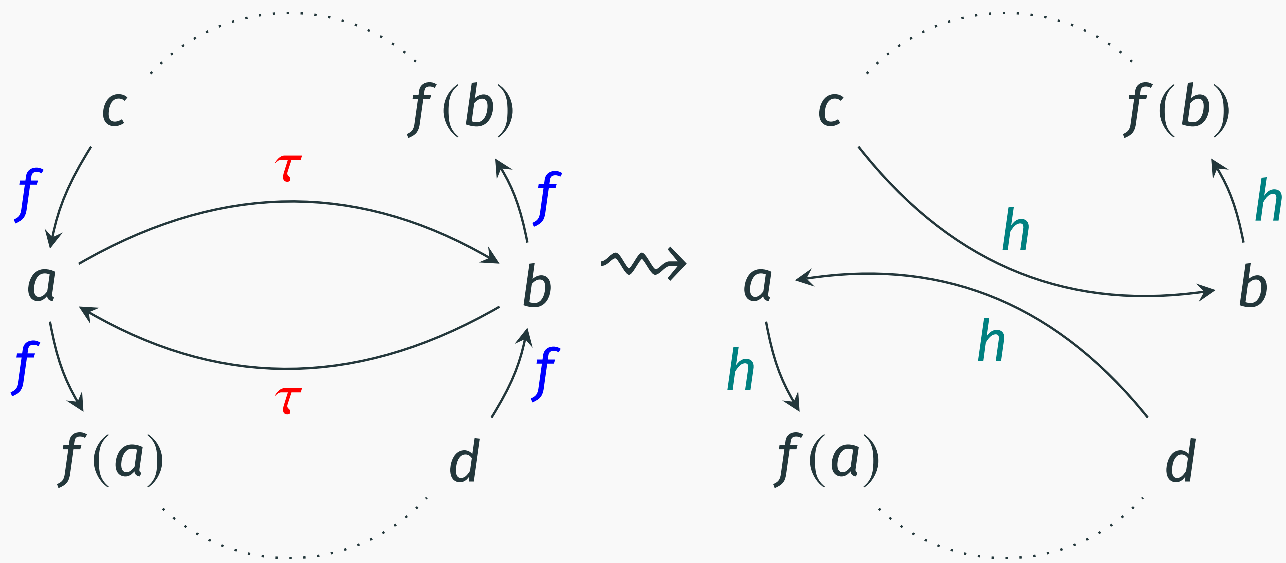
$$\operatorname{sign}(\tau \circ f) = -\operatorname{sign}(f).$$

Proof. Let $h = \tau \circ f$ and suppose $\tau = (ab)$. We separate the proof into two cases:

1. a, b belong to the same cycle of f.
2. a, b belong to two distinct cycles of f.

Sign and Transpositions

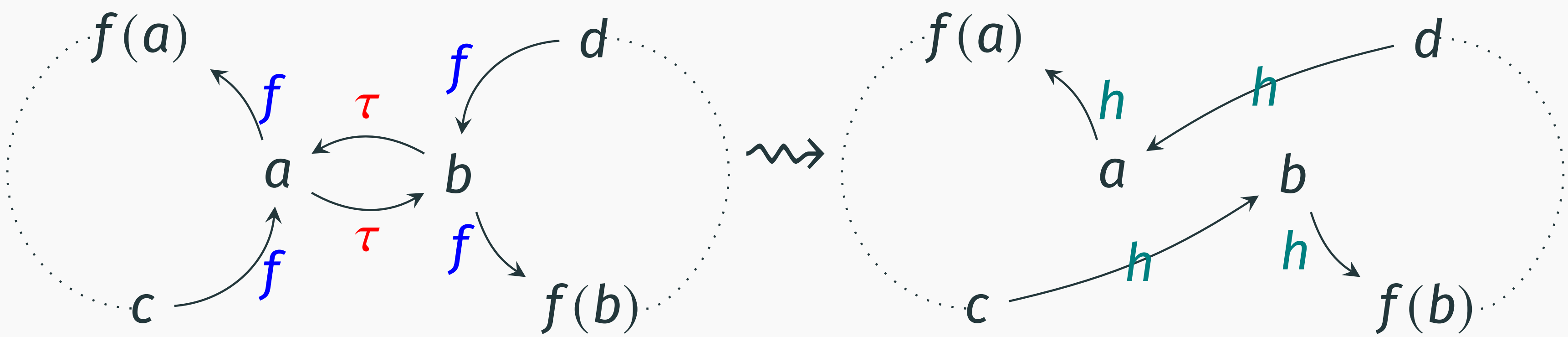
Assume a, b belong to the same cycle of f. Then by composing with τ, this cycle breaks into two.



Moreover, the sum of the length of two new cycles equals the length of original cycle. Hence, $\text{sign}(h) = -\text{sign}(f)$.

$\text{sign} = (-1)^{\text{length}-1}$

Assume a, b belong to two distinct cycles of f. Then by composing with τ, the two cycles merges into one.



Moreover, the length of new cycle equals the sum of the length of two original cycles. Hence, $\operatorname{sign}(h) = -\operatorname{sign}(f)$. $\square$

$(-1)^{\text{Sum of length} - 2}$ v.s. $(-1)^{\text{length} - 1}$

Theorem 24.5 (Second characterization of sign)

Let f be a permutation. If f can be written as the composition of n transpositions, then

$$\operatorname{sign}(f) = (-1)^n.$$

Proof. Let's say $f = \tau_1 \circ \cdots \circ \tau_n$, where τ_i are transpositions. Then by repeatedly applying Lemma 24.4,

$$\begin{aligned}\operatorname{sign}(f) &= -\operatorname{sign}(\tau_2 \circ \cdots \circ \tau_n) \\ &= \cdots \qquad \cdots \\ &= (-1)^n.\end{aligned}$$

□

Sign and Transpositions

Now Theorem 23.8 ($\mathrm{sign}(g \circ f) = \mathrm{sign}(g) \cdot \mathrm{sign}(f)$) is clear: if

$$f = \tau_1 \circ \cdots \circ \tau_n \qquad \text{and} \qquad g = \tau'_1 \circ \cdots \circ \tau'_m,$$

then $g \circ f = \tau'_1 \circ \cdots \circ \tau'_m \circ \tau_1 \circ \cdots \circ \tau_n$. Namely, if we can write f as the composition of n transpositions and g as the composition of m transpositions, then we can write $g \circ f$ as the composition of $m + n$ transpositions. Hence,

$$\mathrm{sign}(g \circ f) = (-1)^{m+n} = (-1)^m (-1)^n = \mathrm{sign}(g) \cdot \mathrm{sign}(f).$$

Sign and inversions

Sign and inversions

From now on, we assume our set X is ***linearly ordered***. You can think this as we fixed a bijection from X to the set $\{1, 2, \cdots, n\}$, where n is the size of X, or even further think X ***is**** $\{1, 2, \cdots, n\}$.

Definition 24.6

Let f be a permutation of X. Then an ***inversion*** of f is a pair (a, b) in X such that

$$a < b \qquad \text{and} \qquad f(a) > f(b).$$

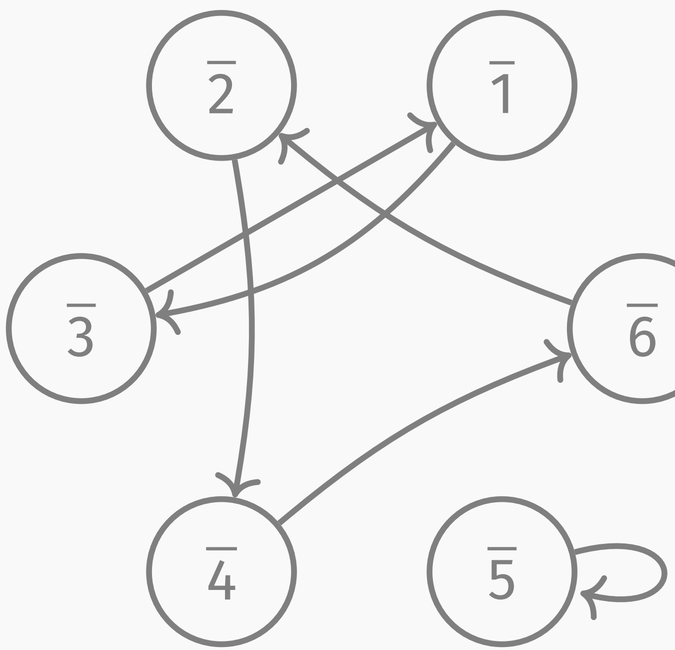
Then $\mathrm{inv}(f)$ is the number of inversions of f.

*Follows the guideline: what matters are structures, not elements.

Sign and inversions

$\text{sign}(f) = (-1)^{\text{inv}(f)}$?

E.g. consider $S = \{1,2,3,4,5,6\}$ and the map f whose dynamic is displayed as left below.



$a<b$

Fill in each $(f(a), f(b))$

a \ b	2	3	4	5	6
1	34	31	36	35	32
2		41	46	45	42
3			16	15	12
4				65	62
5					52

$\text{sign}(f) = -1$

$\text{inv}(f) = 7$

Definition 24.7

A transposition τ is called an ***adjacent transposition*** if it switches two consecutive numbers.

how X is identified with $\{1, 2, \cdots, n\}$

N.B. this notion clearly relies on the linear order.

E.g. On the set $\{1, \cdots, 6\}$, (12) is an adjacent transposition as it switches 1 and 2, while (16) is not.

Lemma 24.8

Let f be a permutation of $\{1, \cdots, n\}$ and $\tau = (aa+1)$. Then

$$\operatorname{inv}(\tau \circ f) - \operatorname{inv}(f) = \begin{cases} 1 & \text{if } f^{-1}(a) < f^{-1}(a+1), \\ -1 & \text{if } f^{-1}(a) > f^{-1}(a+1). \end{cases}$$

Proof. Let (s,t) be a pair such that $1 \leqslant s < t \leqslant n$. We want to see when it is an inversion of f and when it is an inversion of $\tau \circ f$. We will show that τ reverses $(f(s), f(t))$ for exactly one such a pair (s,t). Hence, $\operatorname{inv}(\tau \circ f)$ and $\operatorname{inv}(f)$ are different by 1 and the conclusion then follows.

Sign and inversions

We begin with the case $\{f(s), f(t)\} \neq \{a, a+1\}$. Then τ does not change the order relation between $f(s)$ and $f(t)$. Consequently, (s, t) is an inversion of $\tau \circ f$ if and only if it is an inversion of f.

$$
\begin{tikzcd}
1 \arrow[dd] & & & a \arrow[ddr] & a+1 \arrow[ddl] & & & n \arrow[dd] \\
& \cdots & \cdots & & & \cdots & \cdots & \\
1 & & & a & a+1 & & & n
\end{tikzcd}
$$

Now, we consider the case $\{f(s), f(t)\} = \{a, a+1\}$. Then τ changes the order relation between $f(s)$ and $f(t)$. Hence, (s, t) is an inversion of $\tau \circ f$ if and only if it is NOT an inversion of f. $\square$

Lemma 24.9

Any permutation f of $\{1, \cdots, n\}$ can be written as the composition of $\operatorname{inv}(f)$ adjacent transpositions.

Proof. We prove this by an induction on $\operatorname{inv}(f)$.

If $\operatorname{inv}(f) = 0$, namely f preserves the order, then f has to be id. And id is the imposition of 0 adjacent transpositions.

Now suppose $\operatorname{inv}(f) > 0$. Then $f \neq \operatorname{id}$ and thus there is an a such that

$$f^{-1}(a) > f^{-1}(a+1).$$

By Lemma 24.8, $\operatorname{inv}((aa+1) \circ f) = \operatorname{inv}(f) - 1.$ $<$ inv(f)

By inductive hypothesis, $(aa+1) \circ f$ can be written as the composition of $\mathsf{inv}(f) - 1$ adjacent transpositions. While we have

$$f = (aa+1) \circ \underbrace{(aa+1) \circ f}_{},$$

which can be written as the composition of $\mathsf{inv}(f)$ adjacent transpositions. $\square$

Theorem 24.10 (Third characterization of sign)

Let f be a permutation of a linearly ordered finite set. Then

$$\operatorname{sign}(f) = (-1)^{\operatorname{inv}(f)}.$$

Proof. By the previous lemma, f can be written as the composition of $\operatorname{inv}(f)$ adjacent transpositions. Hence, the second characterization of sign (Theorem 24.5) implies that $\operatorname{sign}(f) = (-1)^{\operatorname{inv}(f)}$. $\square$

Lemma 24.11

$$\mathrm{sign}(\gamma) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Proof. We'll use the 3rd characterization of sign. First recall that $S = \{0, 1, \cdots, pq-1\}$ and on which we have label systems

$$[a, b\rangle := a + bp \qquad \text{and} \qquad \langle a, b] := aq + b.$$

$0 \le a \le p-1 \qquad 0 \le b \le q-1$

It is clear that

$$[a, b\rangle < [a', b'\rangle \iff \text{either } b < b' \text{ or } b = b' \text{ and } a < a',$$
$$\langle a, b] < \langle a', b'] \iff \text{either } a < a' \text{ or } a = a' \text{ and } b < b'.$$

$\langle a,b] > \langle a',b'] \iff a > a'$ or $a = a'$ and $b > b'$

Sign and inversions

The permutation γ maps each $[a, b\rangle$ to $\langle a, b]$. Therefore,

$$\begin{aligned} &([a,b\rangle, [a',b'\rangle) \text{ is an inversion of } \gamma \\ \iff & [a,b\rangle < [a',b'\rangle \text{ and } \langle a,b] > \langle a',b'] \\ \iff & b < b' \text{ and } a > a'. \end{aligned}$$

$\{0, \cdots, q-1\}$ $\{0, \cdots, p-1\}$

The number of such quadruple (a, a', b, b') is

$$\binom{p}{2} \cdot \binom{q}{2} = pq \cdot \frac{p-1}{2} \cdot \frac{q-1}{2} \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2.$$

Therefore, $\mathrm{sign}(\gamma) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$. $\square$