Math 322, lecture 4, 19/9/2017

Last time: (1) $(\mathbb{Z}/n\mathbb{Z})^\times$

(2) Isomorphism

(3) CRT

Today: The symmetric group

Def: Fix a set X. A permutation of X is a bijection $\sigma: X \to X$.
The set of permutations on X will be denoted S_X, and called the symmetric group (of X)

Recall: If $f: Y \to Z$, $g: X \to Y$, their composition is the function $(f \circ g): X \to Z$ given by $(f \circ g)(x) = f(g(x))$.

Lemma: (1) Composition of functions is associative,

(2) $id_X : X \to X$ defined by $id_X(x) = x$ belongs to S_X, and is an identity for composition.

Pf: (1) $X \xrightarrow{h} Y \xrightarrow{g} Z \xrightarrow{f} W$

then $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$

$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$.

(think of $e^{(\cos x)^2}$)

Examples: $\begin{pmatrix}1\\1\end{pmatrix}$, $\begin{pmatrix}1&2\\2&1\end{pmatrix}$, $\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$ ← values $x \in X$ ← values $\sigma(x) \in X$

only element of $S_{\{1\}}$ — element of $S_{\{1,2\}}$ — element of $S_{\{1,2,3,4\}}$

Examples: $\sigma(x) = -x$ is an element of $S_{\mathbb{R}}$.

Non-examples: $\begin{pmatrix}1&2\\1&1\end{pmatrix}$ $\sigma(1)=1$, $\sigma(2)=1$, $\begin{pmatrix}1&2\\2&3\end{pmatrix}$ not functions from $X \to X$

Lemma: Let $\sigma, \tau : X \to X$.

(1) $\sigma \in S_X$ iff there exists $\bar{\sigma} : X \to X$ s.t. $\sigma \circ \bar{\sigma} = \bar{\sigma} \circ \sigma = id_X$. ($\bar{\sigma}$: compositional inverse)

(2) S_X is closed under composition & compositional inverse.

(3) Suppose $\sigma \in S_X$, and $\sigma\tau = id_X$ or $\tau\sigma = id_X$. Then $\tau = \bar{\sigma}$.
In particular, $\bar{\sigma}$ is unique, will be denoted σ^{-1}!

(4) $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$

then

Pf: (1) If σ is a bijection, for each $j \in X$ there is a unique $i \in X$ s.t. $\sigma(i) = j$. Set $\bar{\sigma}(j) = i$. Then $(\sigma \circ \bar{\sigma})(j) = \sigma(\bar{\sigma}(j)) = \sigma(i) = j$.
$(\bar{\sigma} \circ \sigma)(i) = \bar{\sigma}(\sigma(i)) = \bar{\sigma}(j) = i$, for each i (with $j = \sigma(i)$)

Conversely, if $\sigma \circ \bar{\sigma} = id_X$ then for any x, $\sigma(\bar{\sigma}(x)) = x$ so σ is surjective and if $\bar{\sigma} \circ \sigma = id_X$ and $\sigma(x) = \sigma(y)$ then $x = \bar{\sigma}(\sigma(x)) = \bar{\sigma}(\sigma(y)) = y$, so σ is injective

(2) Say $\bar{\sigma}, \bar{\tau}$ exist. Then $(\sigma\tau) \circ (\bar{\tau}\bar{\sigma}) = \sigma \circ (\tau \circ \bar{\tau}) \circ \bar{\sigma}$
$= \sigma \circ id_X \circ \bar{\sigma} = \sigma \circ \bar{\sigma} = id_X$

and $(\bar{\tau}\bar{\sigma}) \circ (\sigma\tau) = \bar{\tau} \circ (\bar{\sigma} \circ \sigma) \circ \tau = \bar{\tau} \circ id_X \circ \tau = \bar{\tau} \circ \tau = id_X$

Also, $\bar{\sigma}\circ\sigma = id_X$, $\sigma\circ\bar{\sigma} = id_X$, so $\bar{\sigma}$ has a compositional inverse, so

$$\sigma\cdot\tau,\ \bar{\sigma} \in S_X.$$

(3) Say $\sigma\tau = id_X$. Then $\bar{\sigma}(\sigma\tau) = \bar{\sigma}\circ id_X$

so $\bar{\sigma} = \bar{\sigma}\cdot id_X = \bar{\sigma}(\sigma\tau) = (\bar{\sigma}\sigma)\tau = id_Y\circ\tau = \tau$

(assoc law)

Same if $\tau\sigma = id_X$.

(4) Follows from (2) & (3)

(write $\sigma\tau$ for $\sigma\circ\tau$)

Examples: $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

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

In general, $\sigma\tau \neq \tau\sigma$.

Examples $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ can have $\sigma = \sigma^{-1}$!

HW: bijection $X\to Y$ gives isom $S_X \to S_Y$.

For this reason, S_X primarily depends on $|X|$, we write

$$S_n = S_{\{1,2,\dots,n\}}$$

Lemma: $\#S_n = n!$

Pf: n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$, $n-2$ choices for $\sigma(3)$,

... 1 choice for $\sigma(n)$, so $n\cdot(n-1)\cdot(n-2)\cdots 1 = n!$ choices altogether.

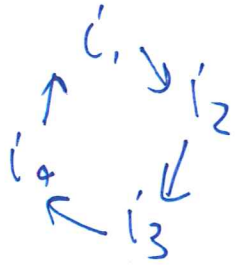
Cycle structure of permutations

Def: For $r \geq 2$, call $\sigma \in S_X$ an *r-cycle* if there are distinct $i_1, i_2, i_3, \ldots, i_r \in X$ s.t.

$$\sigma(i_j) = \begin{cases} i_{j+1} & 1 \leq j < r \\ i_1 & j = r \end{cases}$$

$\sigma(i) = i$ if $i \neq i_j$ for all j.

Cycles



$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 5 & 6 & 7 \end{pmatrix}$$

↑ 4-cycle in S_7.

Def: The *support* of $\sigma \in S_X$ is the set $\operatorname{supp}(\sigma) = \{i \in X \mid \sigma(i) \neq i\}$

Lemma: (1) σ, σ^{-1} have the same support.

(2) if σ, τ have disjoint supports then $\sigma\tau = \tau\sigma$.

Pf: (1) Write $\operatorname{Fix}(\sigma) = \{i \mid \sigma(i) = i\}$. Then $\operatorname{supp}(\sigma) = X \setminus \operatorname{Fix}(\sigma)$ and $\sigma(i) = i$ iff $\sigma^{-1}(\sigma(i)) = \sigma^{-1}(i)$ iff $i = \sigma^{-1}(i)$

so $\operatorname{Fix}(\sigma^{-1}) = \operatorname{Fix}(\sigma)$.

(2) let $A = \operatorname{supp}(\sigma)$, $B = \operatorname{supp}(\tau)$, $C = X \setminus (A \cup B)$

Then $X = A \cup B \cup C$ is a partition.

if $a \in A$, then $a \notin B$ so $(\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(a)$

$(\tau\sigma)(a) = \tau(\sigma(a)) = \sigma(a)$

↑ if $a \in \operatorname{supp}(\sigma)$ then $\sigma(a) \neq a$, $\sigma^{-1}(\sigma(a)) \neq a$

so $\sigma(a) \in \operatorname{supp}(\sigma^{-1}) = \operatorname{supp}(\sigma)$

exchanging A, B, σ, τ get for $b \in B$ that

$$(\tau\sigma)(b) = \tau(b) = (\sigma\tau)(b)$$

Finally if $c \in C$ then $\sigma(c) = c$, $\tau(c) = c$, so

$$(\sigma\tau)(c) = (\tau\sigma)(c) = c.$$

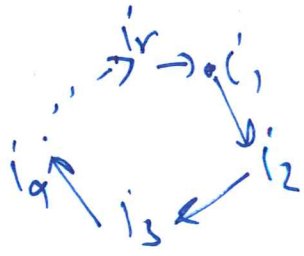
Thm: ("Prime factorization") Every permutation on a finite set is a product of disjoint cycles, uniquely up to the order of the factors.

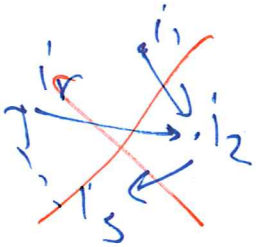
Pf: For existence, let σ be a counterexample with minimal support.

Then $\sigma \neq id_X$ (id_X = empty product)

So there is some $i_1 \in \mathrm{supp}(\sigma)$. Define inductively $i_{j+1} = \sigma(i_j)$

Let r be smallest s.t. $\sigma(i_{r+1}) = \sigma(i_j)$ for some $j \leq r$. (exists: no injective map $\mathbb{Z}_{\geq 1} \to X$). Then $i_1, i_2, \ldots, i_r$ are distinct, and $i_{r+1} = i_1$ (else σ not injective: $\sigma(i_{j-1}) = \sigma(i_r)$)





so $K = (i_1 i_2 \ldots i_r)$ is an r-cycle.

Look at $K^{-1}\sigma$: if $i \notin \mathrm{supp}(\sigma)$ then $\sigma(i) = i$
$K(i) = i$

so $(K^{-1}\sigma)(i) = i$.

Also, $(K^{-1}\sigma)(i_j) = K^{-1}(i_{j+1}) = i_j$

So $\text{supp}(K^{-1}\sigma) = \text{supp}(\sigma) \setminus \{i_1, \ldots, i_r\}$

By hypothesis, $K^{-1}\sigma$ = product of cycles of disjoint support.

(and these supports lie in $\text{supp}(\sigma) \setminus \text{supp}(K)$)

So $\sigma = K \cdot (K^{-1}\sigma)$ is a product of cycles of disjoint supports contradiction

For uniqueness, realize that cycle containing $i_1 \in \text{supp}(\sigma)$ is uniquely defined.

Example: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 2 & 1 & 5 & 7 & 4 \end{pmatrix} = (1\ 6\ 7\ 4)(2\ 3)[(5)]$

↑ sometimes include 1-cycles for fixed points