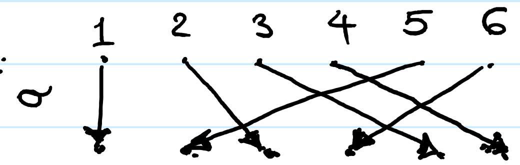
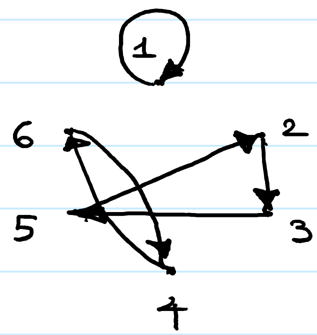
Lecture 11: The symmetric group

Sunday, October 22, 2017 8:05 PM

One of the extremely important groups is the symmetric group S_n. Viewing S_n as symmetries of the set $\{1,\dots,n\}$ gives us an action $S_n \curvearrowright \{1,2,\dots,n\}$. So, for any permutation $\sigma \in S_n$, the cyclic group $\langle\sigma\rangle \curvearrowright \{1,2,\dots,n\}$; and we can look at its orbits, which give us a partition of $\{1,2,\dots,n\}$. In a single orbit, σ acts "cyclically"; that means if we make a directed graph with vertices $1,2,\dots,n$ and directed edges $(i,\sigma(i))$; then we get disjoint directed cycles.

<u>Ex.</u>





mathematical symbol to code this
$(1)(2\ 3\ 5)(4\ 6)$
or simply
$(2\ 3\ 5)(4\ 6)$

<u>Def.</u> A permutation $\tau \in S_n$ is called <u>cycle</u> if $\exists\, c_1,\dots,c_k$ s.t. $\tau = (c_1 \cdots c_k)$; that means $\tau(c_i) = c_{i+1}$ if $i<k$, and $\tau(c_k) = c_1$, and $\tau(x) = x$ if $x \in \{1,\dots,n\} \setminus \{c_1,\dots,c_k\}$.

Lecture 11: Support and fixed points; disjointness

Sunday, October 22, 2017 9:05 PM

<u>Def.</u> • For $\sigma \in S_n$, let $\mathrm{Fix}(\sigma) := \{ i \in \{1, \ldots, n\} \mid \sigma(i) = i \}$

and $\mathrm{supp}(\sigma) := \{1, \ldots, n\} \setminus \mathrm{Fix}(\sigma)$.

• We say $\sigma_1, \sigma_2 \in S_n$ are disjoint if $\mathrm{supp}(\sigma_1) \cap \mathrm{supp}(\sigma_2) = \emptyset$.

Notice that $\mathrm{Fix}(\sigma)$ is $\langle \sigma \rangle$-invariant; and so should be its complement; this means $\mathrm{supp}(\sigma)$ is $\langle \sigma \rangle$-invariant.

<u>Lemma</u>. Suppose $\sigma, \tau \in S_n$ are disjoint. Then $\sigma\tau = \tau\sigma$.

<u>Pf.</u> $\forall\, i \in \{1, \ldots, n\}$,

<u>Case 1.</u> $\tau(i) \neq i$.

Then $i \in \mathrm{Supp}(\tau) \Rightarrow \tau(i) \in \mathrm{Supp}(\tau)$. And so $i, \tau(i) \notin \mathrm{supp}(\sigma)$; this implies $\sigma(i) = i$ and $\sigma(\tau(i)) = \tau(i)$. Therefore

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

<u>Case 2.</u> $\sigma(i) \neq i$ and $\tau(i) = i$.

(by a similar argument, we get $\sigma(\tau(i)) = \tau(\sigma(i))$.

<u>Case 3.</u> $\sigma(i) = \tau(i) = i$.

Then $\sigma(\tau(i)) = i = \tau(\sigma(i))$.

So in any we get $(\sigma\tau)(i) = (\tau\sigma)(i)$. Hence $\sigma\tau = \tau\sigma$. ∎

<u>Lemma</u>. Suppose $\tau_i \in S_n$ and τ_i's are pairwise disjoint. Then for any i, $(\tau_1 \tau_2 \cdots \tau_m)\big|_{\mathrm{Supp}\,\tau_i} = \tau_i\big|_{\mathrm{Supp}(\tau_i)}$. In particular

$\mathrm{Supp}(\tau_1 \cdots \tau_m) = \bigcup_{i=1}^{m} \mathrm{Supp}(\tau_i)$.

Lecture 11: Support of product of disjoint permutations

Monday, October 23, 2017 11:16 AM

Pf. Since $\mathrm{Supp}(\tau_i)$'s are disjoint, $\forall i$ we have

$$\mathrm{supp}(\tau_i) \subseteq \bigcup_{j\neq i} \mathrm{Fix}\, \tau_j .$$

As $\tau_i(\mathrm{Supp}(\tau_i)) = \mathrm{Supp}\,\tau_i$, for any $x \in \mathrm{Supp}(\tau_i)$ we have

$\tau_i(\tau_{i+1}\cdots\tau_m(x)) = \tau_i(x) \in \mathrm{Supp}(\tau_i)$; and so

$$(\tau_1\tau_2\cdots\tau_m)(x) = \tau_i(x).$$

Since $x \in \mathrm{Supp}\,\tau_i$, $\tau_i(x) \neq x$. Therefore $(\tau_1\cdots\tau_m)(x) = \tau_i(x) \neq x$.

$\Rightarrow \bigcup \mathrm{Supp}\,\tau_i \subseteq \mathrm{supp}(\tau_1\cdots\tau_m)$.

If $x \notin \bigcup \mathrm{supp}\,\tau_i$, then $x \in \bigcap \mathrm{Fix}\,\tau_i$. So $(\tau_1\cdots\tau_m)(x) = x$; and the claim follows. ∎

Corollary. Suppose $\tau_1,\dots,\tau_m \in S_n$ are disjoint, $X \subseteq \{1,2,\dots,n\}$ and $|X| \geq 2$.

Then X is an orbit of $\langle \tau_1\cdots\tau_m\rangle \Leftrightarrow X$ is an orbit of $\langle \tau_i \rangle$ for some i.

Pf. $(\Rightarrow)$ Let $x \in X$. Since $|X| \geq 2$ and X is the $\langle \tau_1\cdots\tau_m\rangle$-orbit which contains x, we have $x \in \mathrm{Supp}(\tau_1\cdots\tau_m)$. By the previous lemma $\exists!\, i$ such that $x \in \mathrm{Supp}\,\tau_i$. Since $\tau_1\cdots\tau_m\big|_{\mathrm{Supp}\,\tau_i} = \tau_i\big|_{\mathrm{Supp}\,\tau_i}$ and $x \in \mathrm{Supp}\,\tau_i$, we deduce that the $\langle \tau_1\cdots\tau_m\rangle$-orbit X which

Lecture 11: Orbits of product of disjoint permutations

Monday, October 23, 2017 11:55 AM

contains $x \in \mathrm{Supp}\, \tau_i$ is a subset of X. Therefore by the previous lemma, $(\tau_1 \cdots \tau_m)\big|_X = \tau_i\big|_X$. Hence inductively $(\tau_1 \cdots \tau_m)^j(x) = \tau_i^j(x)$ for any $j \in \mathbb{Z}^+$; this implies X is the $\langle \tau_i \rangle$-orbit of x.

$(\Leftarrow)$ Suppose X is an orbit of τ_i, and $x \in X$. Then, as $|X| \geq 2$, $x \in \mathrm{Supp}\, \tau_i$; and so $(\tau_1 \cdots \tau_m)(x) = \tau_i(x)$; and this is true for any $x \in X$; this means $\tau_1 \cdots \tau_m\big|_X = \tau_i\big|_X$ $\circledast$. As X is $\langle \tau_i \rangle$-invariant, it is also $\langle \tau_1 \cdots \tau_m \rangle$-invariant. So using $\circledast$ inductively we have $(\tau_1 \cdots \tau_m)^j(x) = \tau_i^j(x)$; this implies the $\langle \tau_1 \cdots \tau_m \rangle$-orbit of x is the same as $\langle \tau_i \rangle$-orbit X of x. $\blacksquare$

<u>Lemma</u>. Let $\sigma = (i_1\ i_2 \cdots i_k) \in S_n$. Suppose $k > 1$, $X \subseteq \{1, \ldots, n\}$, and $|X| \geq 2$. Then X is a $\langle \sigma \rangle$-orbit if and only if $X = \{i_1, \ldots, i_k\}$.

<u>Pf.</u> $(\Rightarrow)$. $x \in X \Rightarrow |\langle \sigma \rangle \cdot x| = |X| \geq 2 \Rightarrow x \in \mathrm{Supp}\, \sigma \Rightarrow x \in \{i_1, \ldots, i_k\}$

$\Rightarrow x = i_t$ for some $t \Rightarrow X = \langle \sigma \rangle \cdot i_t = \{i_1, \ldots, i_k\}$.

$(\Leftarrow)$ is clear. $\blacksquare$

Lecture 11: Uniqueness of cycle decomposition

Monday, October 23, 2017 12:11 PM

<u>Lemma</u> (Uniqueness) Suppose $\tau_1, \ldots, \tau_m$ are disjoint cycles and $\sigma_1, \ldots, \sigma_k$ are disjoint cycles. Suppose $|\operatorname{supp} \tau_i| \geq 2$ and $|\operatorname{supp} \sigma_i| \geq 2$ (they are non-trivial.). Then

$\tau_1 \cdot \cdots \cdot \tau_m = \sigma_1 \cdot \cdots \cdot \sigma_k$ implies $m = k$ and

$$\tau_1 = \sigma_{i_1}, \ldots, \tau_m = \sigma_{i_m}$$

where $(i_1, \ldots, i_m)$ is a permutation of $1, \ldots, m$.

<u>Pf.</u> We proceed by induction on m; with an understanding that $m=0$ means the LHS is the identity element.

<u>Base of induction.</u> If $k \neq 0$, then $\operatorname{supp}(\sigma_1 \cdots \sigma_k) = \bigcup \operatorname{supp} \sigma_i \neq \emptyset$

by a lemma which is proved earlier

<u>Induction step.</u> Since τ_1 is a non-trivial cycle, $\operatorname{supp} \tau_1$ is a $\langle \tau_1 \rangle$-orbit of size ≥ 2. Hence by a lemma $\operatorname{supp} \tau_1$ is a $\langle \tau_1 \cdots \tau_m \rangle$-orbit of size ≥ 2. Therefore $\operatorname{supp} \tau_1$ is a $\langle \sigma_1 \cdots \sigma_k \rangle$-orbit of size ≥ 2. Thus by a lemma $\exists\, i_1$ s.t. $\operatorname{Supp} \tau_1$ is a $\langle \sigma_{i_1} \rangle$-orbit of size ≥ 2. As σ_{i_1} is a cycle, by a lemma, $\operatorname{supp} \tau_1 = \operatorname{Supp} \sigma_{i_1}$. We also know

Lecture 11: Uniqueness of cycle decomposition

Monday, October 23, 2017 12:24 PM

$$\tau_1\big|_{\mathrm{Supp}\,\tau_1} = (\tau_1\cdots\tau_m)\big|_{\mathrm{Supp}\,\tau_1}$$
$$= (\sigma_1\cdots\sigma_k)\big|_{\mathrm{Supp}\,\tau_1}$$
$$= (\sigma_1\cdots\sigma_k)\big|_{\mathrm{supp}\,\sigma_{i_1}}$$
$$= \sigma_{i_1}\big|_{\mathrm{supp}\,\sigma_{i_1}} \quad ; \text{ this implies } \tau_1 = \sigma_{i_1}.$$

Now the claim follows using the induction hypothesis. ■

<u>Lemma</u> (Existence) For any $\sigma \in S_n \setminus \{I\}$, there are disjoint cycles $\tau_1, \dots, \tau_m$ such that $\sigma = \tau_1 \cdot \dots \cdot \tau_m$.

<u>Pf.</u> Suppose $\langle\sigma\rangle \backslash \{1,2,\dots,n\} = \{X_1,\dots,X_k\}$. And after reordering assume $|X_1|,\dots,|X_m| \geq 2$ and $|X_{m+1}| = \dots = |X_k| = 1$.

For $1 \leq i \leq m$, let $\tau_i \in S_n$ be $\tau_i\big|_{X_i} = \sigma\big|_{X_i}$ and
$$\tau_i\big|_{X_i^c} = I\big|_{X_i^c}.$$

<u>Claim 1.</u> τ_i is a cycle.

<u>Pf.</u> • $\tau_i(X_i) = \sigma(X_i) = X_i \Rightarrow \tau_i$ is surjective $\Rightarrow \tau_i \in S_n$.

• $X_i = \langle\sigma\rangle \cdot x = \{x, \sigma(x), \dots, \sigma^{\ell}(x)\} = \{x, \tau_i(x), \dots, \tau_i^{\ell}(x)\}$
and $x = \sigma^{\ell+1}(x)$ and $\tau^{\ell+1}(x) = x$

So $\tau_i = (x \;\sigma(x) \cdots \sigma^{\ell}(x))$. ■

Lecture 11: Existence of cycle decomposition

Monday, October 23, 2017 12:41 PM

Claim 2. $\sigma = \tau_1 \tau_2 \cdots \tau_m$.

Pf. $\forall x \in \{1, \ldots, n\}$, $\exists!\, i_x$ s.t. $x \in X_{i_x}$. If $i_x \geq m+1$, then $\sigma(x) = x$ and $\tau_i(x) = x$, for any $1 \leq i \leq m$.

And so $\sigma(x) = x = (\tau_1 \cdots \tau_m)(x)$.

If $i_x \leq m$, then $x \in \operatorname{Supp} \tau_{i_x}$; and so

$$(\tau_1 \cdots \tau_m)(x) = \tau_{i_x}(x) = \sigma(x)$$

$$\boxed{\tau_{i_x}\big|_{\operatorname{Supp} \tau_{i_x}} = \sigma\big|_{\operatorname{Supp} \tau_{i_x}}}$$

And the claim follows.

By Claim 1 and Claim 2, $\tau_1 \cdots \tau_m$ is a cycle decomposition of σ. ■

Proposition. $\forall \sigma \in S_n \setminus \{1\}$ can be written as a product of disjoint cycles; and this decomposition is unique up to reordering its factors. This decomposition is called the cycle decomposition of σ.