Discrete Mathematics lecture notes 11-1

November 21, 2013

29. The symmetric group is generated by transpositions

When we say a mathematical object is *generated* by some subset, we mean that every element element of the object in question can be in some sense built out of the elements of the subset. For instance, half of the Fundamental Theorem of Arithmetic asserts that the set of primes generate $\mathbb{N}$ multiplicatively: This is just a fancy way of saying that every natural number can be written as a product of primes.[1] The other half of FTA—that the expression of $n \in \mathbb{N}$ as a product of primes is essentially[2] unique—is a strictly stronger notion than generation.[3]

A silly example: If $S := \{p | p \text{ is prime}\} \cup \{6\}$, then every element of $\mathbb{N}$ can be written as a product of elements of S, but not uniquely: $6 = 2 \cdot 3$ is two different expressions of a given natural number in terms of the elements of S. Thus FTA would not be true with S replacing the set of primes, but it is still true that S generates $\mathbb{N}$ multiplicatively.[4]

Last time we showed that the set of cycles generates Σ_n. We also had a sort of uniqueness result: Every $\sigma \in \Sigma_n$ can be written uniquely as a product of disjoint cycles (up to ordering of the cycles and cyclic shifts within the cycles). Note that this is not the same as saying that there is some analogue of the FTA lurking in the background: Saying that σ is a unique product of disjoint cycles does not mean that it is uniquely the product of cycles in general, and there is no way to restrict the types of cycles *a priori*[5] to obtain a set that generates Σ_n uniquely.

Point being: Generation (but not free generation) is the best we can hope for in Σ_n, which have already achieved via the set of all cycles. However, we might be interested in a smaller generating subset, one that's easier to compute with.

Definition 1. A *transposition* is a permutation $\tau \in \Sigma_n$ that swaps two elements and leaves the others fixed. In cycle notation, $\tau = (ab)$ for $a, b \in [n]$ distinct elements.

Proposition 2. *The set of transpositions generates Σ_n.*

Proof. Since every $\sigma \in \Sigma_n$ can be written as a product of cycles, it will suffice to show that every cycle can be written as a product of transpositions.[6] The result follows from the computation:

$$(i_1\ i_2\ i_3\ \dots\ i_{k-1}\ i_k) = (i_1\ i_k)(i_1\ i_{k-1})\dots(i_1\ i_3)(i_1\ i_2).$$

which you should prove by induction on k if it is not clear. □

Remark 3. We are not claiming that the set of transpositions in a minimal generating set. Indeed, if $\tau_i = (i\ i+1)$ for $1 \leq i \leq n-1$, you should convince yourself that $\{\tau_i\}_{i=1}^{n-1}$ forms a generating subset... as does $\{(1\ 2), (1\ 2\ 3\ \dots\ n)\}$. You should check both of these for yourself. The point is not that we're really interested in a minimal generating set, just one that we can easily manipulate.

The expression of $\sigma \in \Sigma_n$ as a product of transpositions is not unique. For instance:

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3) = (2\ 3)(1\ 3) = (2\ 3)(1\ 2)(2\ 3)(1\ 2) = \dots$$

In fact, there are infinitely many expressions of each σ in terms of transpositions, as hinted in the last equality: Not only is the expression of σ as a product of transpositions not unique, but the *number* of transpositions in σ is not well-defined.

[1] Ok, every nonzero natural number, unless we adopt the perspective that 0 is prime. There is some justification for this point of view, but we will not need it here. Note that 1, though not prime itself, is the empty product of primes.

[2] That is, up to reordering.

[3] This uniqueness is usually represented by the more general notion of *freeness*. Thus FTA could be rephrased: The set of nonzero natural numbers, with the operation of multiplication, is *freely generated* by the set of primes.

[4] In general, if A generates an object X, whatever that means, and $A \subseteq B$, then B generates X as well.

[5] That is, before we know which σ we're trying to represent.

[6] This reflects the mantra: If A generates X and B generates A, then B generates X.

However, all is not lost: There is a tiny bit of uniqueness salvageable from the wreckage of generating Σ_n by transpositions.

Theorem 4. *For each $\sigma \in \Sigma_n$, the parity of the number of transpositions needed to express σ is well-defined.*

In other words, if

$$\begin{aligned} \sigma &= \tau_1\tau_2\dots\tau_n \\ &= \tau_1'\tau_2'\dots\tau_m' \end{aligned}$$

with τ_i and τ_j' transpositions, then n is even iff m is even.

We will prove this twice, once using more purely group-theoretic methods, and a second time with combinatorics. In both cases, we begin with a reduction:

Proposition 5. *If* $\mathrm{id} = \tau_1\tau_2\dots\tau_n$ *is an expression of the identity of* Σ_m *as a product of transpositions, then* n *is even.*

Proposition 5 implies Theorem 4. If we suppose that Proposition 5 is true, Theorem 4 follows immediately: From the expression $\sigma = \tau_1\tau_2\dots\tau_n = \tau_1'\tau_2'\dots\tau_m'$, then

$$\begin{aligned} \mathrm{id} = \sigma \circ \sigma^-1 & \\ &= (\tau_1\tau_2\dots\tau_n)(\tau_1'\tau_2'\dots\tau_m')^{-1} \\ &= \tau_1\tau_2\dots\tau_n(\tau_m')^{-1}\dots(\tau_2')^{-1}(\tau_1')^{-1} \\ &= \tau_1\tau_2\dots\tau_n\tau_m'\dots\tau_2'\tau_1', \end{aligned}$$

where the last equality uses the fact that $\tau^{-1} = \tau$ for any transposition. This yields id as a product of $n+m$ transpositions; if we assume Proposition5, this forces $n+m$ to be even, so either both n and m are even or both are odd. □

Proof of Proposition 5. Clearly we cannot write id as a product of a single transposition (as no transposition is the identity), but we can write it as the product of two transpositions (as every transposition is its own inverse). Suppose inductively that whenever we have written id as a product of ℓ transpositions for $\ell < n$, it follows that ℓ is even. If we can show from this assumption that, whenever id is the product of n transpositions, then n is even, strong induction will give us the result.

Suppose that we have an expression of id as a product of transpositions $\mathrm{id} = \tau_1\tau_2\dots\tau_n$. We will show that we can write id as a product of $n-2$ transpositions; by our inductive hypothesis, it will follow that $n-2$ is even, or n itself is even.

Write $\tau_i = (a_i\ b_i)$ for a_i, b_i two distinct elements of $[n]$, and write $a := a_1$ for the first term that appears in the leftmost (i.e., *last*) transposition. I claim that for some $1 < i \leq n$, we must have $a \in \{a_i, b_i\}$. If not, then a is fixed by τ_i, $1 < i \leq n$ and $\tau_1(a) = b_1 \neq a$, showing that the product of transpositions is not the identity. Without loss of generality, assume that $a = a_i$ for $i \in \{k_1, k_2, \dots, k_j\}$ with $1 < k_1 < k_2 < \dots < k_j \leq n$ is a complete list of instances of a in the transpositions after the first. Let's focus our attention on the τ_{k_1}, i.e., the second leftmost transposition containing a.

If $k_1 \neq 2$, then within the expression for id, the expression for id contains the term $\tau_{k_1-1}\tau_{k_1} = (a_{k_1-1}\ b_{k_1-1})(a\ b_{k_1})$. If $b_{k_1-1} \neq b_{k_1}$, then these two transpositions are disjoint,[7] so $(a_{k_1-1}\ b_{k_1-1})(a\ b_{k_1}) = (a\ b_{k_1})(a_{k_1-1}\ b_{k_1-1})$. If $b_{k_1-1} = b_{k_1}$, then

$$(a_{k_1-1}\ b_{k_1})(a\ b_{k_1}) = (a\ a_{k_1-1}\ b_{k_1}) = (a_{k_1-1}\ b_{k_1}\ a) = (a_{k_1-1}\ a)(a_{k_1-1}\ b_{k_1}).$$

In either case, we can rewrite the product expression for σ with the same number of transpositions, but where the second leftmost occurrence of a now is in position $k_1 - 1$. After enough repetitions, we may assume $k_1 = 2$.

[7] Why?

So now our expression begins $(a\ b_1)(a\ b_2)\ldots$. We have two possibilities: Either $b_1 = b_2$, or $b_1 \neq b_2$. In the first instance, $(a\ b_1)(a\ b_1) = \mathrm{id}$, so the first two transpositions cancel. Thus we've arrived at an expression for id in terms of two fewer transpositions than we'd started out with—$n-2$ versus n—which shows that n must be even by the inductive hypothesis.

In the second case that $b_1 \neq b_2$, we have

$$(a\ b_1)(a\ b_2) = (a\ b_2\ b_1) = (b_2\ b_1\ a) = (b_2\ a)(b_2\ b_1).$$

This may not seem like it's getting us much, but note that a does not appear at all in the second transposition. Thus we have eliminated one of the j occurrences of a after the leftmost transposition. Repeat the process of bringing the second leftmost transposition containing a to the second position, either canceling the first two transpositions (and therefore being done by induction) or reducing the number of as by 1. After the jth iteration of this process, there are no more as after the first to cancel, so in fact there must have been a cancelation of the first two transpositions at some point (else we'd end up with an expression for id where a occurs in a unique transposition, which we noted to be impossible at the beginning of this argument). This ends the proof. □