SUPPLEMENT ON THE SYMMETRIC GROUP

RUSS WOODROOFE

I presented a couple of aspects of the theory of the symmetric group S_n differently than what is in Isaacs. These notes will sketch this material. You will still want to read your notes and Isaacs Chapter 6.

1. Conjugacy

1.1. **The big idea.** We recall from Linear Algebra that conjugacy in the matrix $GL_n(\mathbb{F})$ corresponds to changing basis in the underlying vector space $\mathbb{F}^n$. That is, if A sends each $\mathbf{e}_i \mapsto \sum_j \alpha_j^{(i)} \mathbf{e}_j$, and B sends $\mathbf{e}_i \mapsto \mathbf{b}_i$ for all i, then

$$(\mathbf{b}_i) \cdot B^{-1}AB = \mathbf{e}_i \cdot AB = (\sum_j \alpha_j^{(i)} \mathbf{e}_j) \cdot B = \sum_j \alpha_j^{(i)} \mathbf{b}_j.$$

Since $GL_n(\mathbb{F})$ is exactly the automorphism group of $\mathbb{F}^n$, it's equivalent to say that conjugation in $\operatorname{Aut} \mathbb{F}^n$ corresponds to change of basis in $\mathbb{F}^n$.

Similarly, S_n is $\operatorname{Sym}[n]$, the symmetries of the set $[n] = \{1, \dots, n\}$. We can think of an element of $\operatorname{Sym}[n]$ as being a "set automorphism" – this just says that sets have no interesting structure, unlike vector spaces with their abelian group structure. You might expect conjugation in S_n to correspond to some sort of change in basis of $[n]$.

1.2. **Mathematical details.**

Lemma 1. *Let $g = (\alpha_1, \dots, \alpha_k)$ be a k-cycle in S_n, and $h \in S_n$ be any element. Then*

$$g^h = (\alpha_1 \cdot h, \alpha_2 \cdot h, \dots \alpha_k \cdot h).$$

Proof. We show that g^h has the same action as $(\alpha_1 \cdot h, \alpha_2 \cdot h, \dots \alpha_k \cdot h)$. Since S_n acts with trivial kernel on $[n]$, the lemma follows.

But if j is any element of $\{1, \dots, n\}$, then

$$(j \cdot h) \cdot h^{-1}gh = j \cdot gh.$$

In particular, g^h sends $\alpha_i \cdot h$ to $\alpha_i \cdot gh = \alpha_{i+1} \cdot h$, and fixes all other elements of $\{1, \dots, n\}$, as desired. □

Lemma 1 corresponds to change of basis, since instead of g acting on $\{1, \dots, n\}$, we see it acting on $\{1 \cdot h, 2 \cdot h, \dots, n \cdot h\}$. In $GL_n(\mathbb{R})$, we had a similar situation: $B^{-1}AB$ acts on $\{e_1 \cdot B, \dots e_n \cdot B\}$ in the same way as A acts on $\{e_1, \dots, e_n\}$.

There is an "if and only if" relation.

Definition 2. The *cycle structure* of a permutation $g \in S_n$ is the unordered list of sizes of lengths of cycles in the cyclic notation for g. (The separator is often written as a plus.)

For example, $(1,2)(3,5)(6,7,8) \in S_8$ has cycle structure $3+2+2+1$. Then:

Theorem 3. *Two elements of S_n are conjugate if and only if they have the same cycle structure.*

Proof. ($\Longrightarrow$): Let $g \in S_n$ have disjoint cycle decomposition $g = \prod_{i=1}^{k} g_i$, and let $h \in S_n$ be any other element. Then Lemma 1 tells us that g_i^h is another cycle, of the same order as g_i. Furthermore, these cycles are disjoint. Thus, the disjoint cycle decomposition of $g^h = \prod_{i=1}^{k} g_i^h$, which has the same cycle structure as g.

($\Longleftarrow$): We need to find an element $x \in S_n$ which sends the cycles of $g \in S_n$ to the cycles of $h \in S_n$. We do this as follows: write out the cycle decomposition of g above that of h, with the cycles in order of decreasing size; and with the fixed points at the end. Map "straight down", as illustrated:

$$\begin{array}{cccccccccccc} (& \alpha_1, & \alpha_2, & \dots, & \alpha_k &) & \cdot(& \dots &) & \cdot(& \dots &) & \text{fixed points} \\ & \downarrow & \downarrow & & \downarrow & & & \downarrow\downarrow & & & \downarrow\downarrow & & \downarrow \\ (& \beta_1, & \beta_2, & \dots, & \beta_k &) & \cdot(& \dots &) & \cdot(& \dots &) & \text{fixed points} \end{array}.$$

So $\alpha_1 \mapsto \beta_1$, etc. This map is invertible (since the corresponding "straight up" map is its inverse), so is a bijection on $[n]$, and so corresponds to an element $x \in S_n$. We have that $g^x = h$ by Lemma 1. $\square$

For example, $(1,2,3)(4,5,6,7)$ and $(3,5,7)(1,4,2,6)$ are conjugate in S_7. An element (not unique) which conjugates the first to the second is the 7-cycle $(1,3,7,6,2,5,4)$.

2. Transpositions

Recall that a *transposition* in S_n is a 2-cycle, i.e., a cycle of the form (i,j).

Lemma 4. *Any element $g \in S_n$ can be written as the product of transpositions.*

Proof. Since g can be written as a disjoint product of cycles, it suffices to write a cycle as a product of decompositions. We check that

$$(\alpha_1, \alpha_2, \dots, \alpha_k) = (\alpha_1, \alpha_2) \cdot (\alpha_1, \alpha_3) \cdot \dots \cdot (\alpha_1, \alpha_k)$$

is such a decomposition. Clearly, the RHS fixes any element not in the orbit of $(\alpha_1, \dots, \alpha_m)$. If we apply the RHS to α_i $(2 \le i \le m-1)$, then the first $i-2$ transpositions fix it, while the $(i-1)$st sends it to α_1, and the ith sends α_1 to α_{i+1}. Similarly for α_1 and α_m. $\square$

Corollary 5. *S_n is generated by its transpositions.*

This is the starting point for the theory of *Coxeter groups*, or *crystallographic groups*. We can look at S_n as acting on $\mathbb{R}^n$ by permuting the basis elements $\{e_1, \ldots, e_n\}$. Each transposition (i, j) corresponds to reflecting $\mathbb{R}^n$ across the hyperplane $\{x_i = x_j\}$, and we get a very geometric approach to understanding S_n.

Unfortunately, Coxeter groups are beyond the scope of this course. If you are interested in knowing more about them, then Humphreys' book "Reflection Groups and Coxeter Groups" may be a good place to start.

3. Normal subgroups in S_n

3.1. **The big idea.** Recall from earlier in class that $GL_n(\mathbb{F})$ has two interesting normal subgroups:

- $Z(GL_n(\mathbb{F}))$ can be seen to consist of all scalar multiples of the identity matrix, hence is nontrivial if $\mathbb{F} \neq \mathbb{Z}_2$. (It is easy to show that any such element is central; the harder part is showing that this is the entire center.)
- $SL_n(\mathbb{F}) = \ker(\det)$, the matrices with determinant 1.

Our first observation is that there is no analogue to the first subgroup in S_n.

Theorem 6. *If $n \geq 3$, then $Z(S_n) = 1$.*

Proof. Let $g \in S_n$ send α to β, and let h be the transposition exchanging β and some γ distinct from α and β. Then g^h sends α to γ by Lemma 1 (and/or its proof). Since g and g^h act differently on α, we have $g^h \neq g$, and g is not central. $\square$

An analogue of the determinant map does exist and give an interesting normal subgroup of S_n. This is the topic of the next section.

4. Even and odd permutations

Definition 7. We define a map

$$\begin{aligned} \operatorname{sign} : S_n &\to \{\pm 1\} \\ g &\mapsto \begin{cases} +1 & \text{if } g \text{ is a product of an even number of transpositions} \\ -1 & \text{if } g \text{ is a product of an odd number of transpositions.} \end{cases} \end{aligned}$$

We say that g is *even* if $\operatorname{sign} g = 1$ (so that g is a product of an even number of transpositions), and that g is *odd* if $\operatorname{sign} g = -1$.

The problem with this definition, is that it's not clear that sign is well-defined!

Example 8. If we tried to define $\heartsuit(g)$ as ± 1 depending on whether g is an even or odd product of 3-cycles, we would get into trouble. For example

$$(1,2,3) \cdot (3,4,5) = (1,2,4,5,3) = (1,2,3) \cdot (2,3,4) \cdot (2,5,3)$$

is both an even and odd product of 3-cycles! So $\heartsuit(g)$ is not well-defined.

Remark 9. Assuming that sign is well-defined, it is a homomorphism. For the product of two odd permutations is an even permutation, and in this case $\operatorname{sign} gh = +1 = \operatorname{sign} g \cdot \operatorname{sign} h$. Similarly for even permutations, or an even and an odd.

Remark 10. This is the same sign that shows up in the definition of the determinant. In fact, one way to prove Theorem 11 below is to map S_n into $GL_n(\mathbb{R})$, mapping an element g to the associated so-called "permutation matrix" which sends a member $\mathbf{e}_i$ of the standard basis to $\mathbf{e}_{i \cdot g}$. The sign map is then the determinant of the permutation matrix.

This is somewhat circular, since the definition of determinant depends on sign being well-defined! And in any case, the proof of Theorem 11 given below is beautiful.

Theorem 11. *The map* $\operatorname{sign} g$ *is a well-defined homomorphism* $S_n \to \{\pm 1\}$.

Proof. It suffices to construct a homomorphism $\varphi : S_n \to \{\pm 1\}$ such that $\varphi((i,j)) = -1$ for any transposition (i,j). We will do this by actions on directed graphs, in a clever proof due to Cartier:

Take a vertex for every number $1 \ldots n$, and put an arrow (directed edge) between each pair of vertices, as in the following examples:

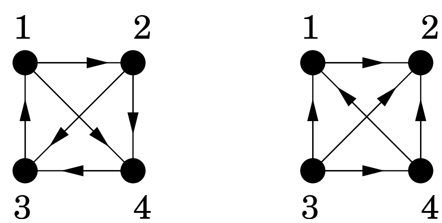

FIGURE 4.1. Two examples of orientations of [4].

Call such an assignment of arrows between each pair an *orientation*. There are many orientations of $[n]$. If o and o' are two orientations, then a pair i, j is a *difference* if o and o' differ on the edge between i and j, i.e., if one has an edge $i \to j$ and the other $j \to i$. To measure the difference between o and o', we define the following function:

$$d(o, o') = (-1)^{\#\text{differences between } o \text{ and } o'}.$$

We make some elementary claims:

Claim 12. $d(o, o) = 1$

Claim 13. $d(o, o') = d(o', o)$

Claim 14. $d(o, o')d(o', o'') = d(o, o'')$

Proof. Let

e be the number of edges where o is different from both o' and o''
e' be the number of edges where o' is different from both o and o''
e'' be the number of edges where o'' is different from both o and o'.

Then

$$d(o,o')d(o',o'') = (-1)^{e+e'}(-1)^{e'+e''} = (-1)^{e+e''+2e'} = (-1)^{e+e''} = d(o,o'')$$

where $(-1)^{2e'} = 1$ since $2e'$ is even. □

Claim 15. The action of S_n on $[n]$ induces an action on $\{\text{orientations of } [n]\}$, and $d(o\cdot g, o'\cdot g) = d(o,o')$.

Proof. The action on $[n]$ sends the edge $i \to j$ to the edge $i\cdot g \to j\cdot g$, for all pairs i,j. Clearly the number of differences remain the same (though they are moved around). More specifically, i,j is a difference between o and o' iff $i\cdot g, j\cdot g$ is a difference between $o\cdot g$ and $o'\cdot g$. □

Fix some orientation o, and let $\varphi(g) = d(o, o\cdot g)$. Intuitively, φ measures the amount that g "moves" the orientation o.

We verify that φ is a homomorphism. First, using Claim 14, we have

$$\varphi(gh) = d(o, o\cdot gh) = d(o, o\cdot h)d(o\cdot h, o\cdot gh).$$

Claim 15 then shows that $d(o\cdot g, o\cdot gh) = d(o, o\cdot h)$. Hence

$$\varphi(gh) = d(o, o\cdot h)d(o, o\cdot g) = \varphi(h)\varphi(g) = \varphi(g)\varphi(h),$$

where the last equality is because $\{\pm 1\}$ is abelian. We have that φ is a homomorphism.

Next, we check that if (i,j) is a transposition, then $\varphi((i,j)) = d(o, o\cdot (i,j)) = -1$. Consider the following diagram:

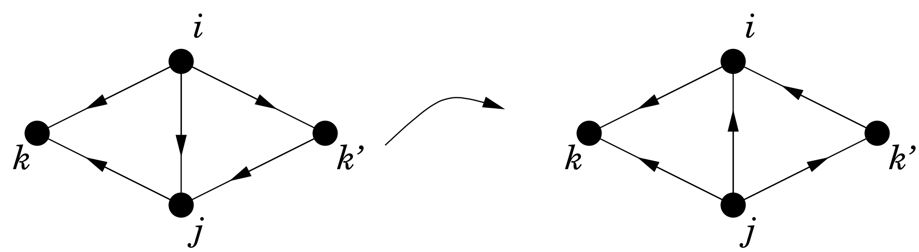

FIGURE 4.2. Transposing i and j.

We see that (i,j) reverses the edge i,j. If the edges k,i and k,j have the same direction, then they do afterwards, and these edges add 0 differences; if the edges k,i and k,j have different directions, then they are reversed by (i,j), and these edges add 2 differences. The claim that $\varphi((i,j)) = -1$ follows since $(-1)^2 = 1$.

We have constructed a concrete, well-defined homomorphism φ which agrees with sign on a generating set, the set of transpositions. Hence φ is equal to sign on any element of S_n. $\square$

The main reason to prove Theorem 11 is its Corollary.

Definition 16. Let $A_n = \{\text{even permutations in } S_n\}$.

Corollary 17. *A_n is a normal subgroup of index 2 in S_n.*

Proof. $A_n = \ker \operatorname{sign}$, hence $A_n \triangleleft S_n$. By the Isomorphism Theorem,

$$[S_n : A_n] = |S_n/A_n| = |\operatorname{Im} \operatorname{sign}| = 2,$$

as desired. $\square$