WORKSHEET ON SYMMETRIC GROUPS, MATH 504, FALL 2018

DUE FRIDAY, NOVEMBER 2
EXTENDED TO MONDAY, NOV 5, BY POPULAR DEMAND AND CONVINCING ARGUMENTS

1. Generators of S_n

Definition 1.1. The symmetric group on n elements, denoted S_n is a group of self-bijections (or permutations) of the set $X = \{1, 2, \ldots, n\}$. For the purposes of this worksheet, we multiply permutations from left to right. You could multiply from right to left as well - this will not change any of the main results but you'll need to adjust some of the formulas. Either way is fine as long as you (and I:)) are consistent.

Notation. Let $\sigma \in S_n$. Hence, $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is a bijection. The commonly used notation for the corresponding permutation is the following:

$$\begin{pmatrix} 1 & 2 & \ldots & \mathrm{n} \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Definition 1.2. A permutation $\sigma \in S_n$ is called a *cycle* if there exists a subset $\{x_1, \ldots, x_k\} \subset \{1, 2, \ldots, n\}$ such that $\sigma(x_i) = x_{i+1}$ and $\sigma(y) = y$ for any $y \neq x_i$. The standard notation for such a permutation is

$$(x_1, x_2, \ldots, x_k).$$

Two cycles $(x_1, x_2, \ldots, x_k)$ and $(y_1, y_2, \ldots, y_\ell)$ are called *disjoint* if the sets $\{x_1, x_2, \ldots, x_k\}$ and $\{y_1, y_2, \ldots, y_\ell\}$ do not intersect.

Example 1.3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} = (234)$

Symmetric group has various sets of generators. For example:

Proposition 1.4. *(=$\boxed{\text{Problem 0}}$.) The symmetric group S_n can be generated by two elements: a cycle of length 2 and a cycle of length n.*

Proposition 1.5. *(=$\boxed{\text{Problem 1}}$.) Any permutation $\sigma \in S_n$ can be written as a composition of disjoint cycles.*

Remark 1.6. Such decomposition is unique up to the order of the factors.

Example 1.7. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix} = (15)(234)$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = (12)(3)(45) = (12)(45)$

A cycle of length 1, such as (3) in the example above, just indicates that the corresponding element is fixed under the permutation. These are often skipped when permutation is written as a product of cycles.

We now describe the conjugacy classes of S_n (= the orbits under the action by conjugation of S_n on itself).

Theorem 1.8. *(=* $\boxed{\textit{Problem 2}}$*.) Let $\sigma, \tau \in S_n$. Then σ and τ are conjugate if and only if their decompositions into disjoint cycles can be put into one-to-one correspondence such that the corresponding cycles are of the same length.*

In particular, the conjugacy class of a single cycle consists of all cycles of the same length.

Remark 1.9. The group S_n is non-commutative for $n \geq 3$. Nonetheless, disjoint cycles always commute.

Definition 1.10. A transposition is a cycle of length 2.

Proposition 1.11. *(=* $\boxed{\textit{Problem 3}}$*.) The symmetric group S_n is generated by transpositions.*

2. Alternating group

Note that the symmetric group S_n acts on polynomials on n variables. Namely, we define

$$(\sigma f)(x_1, \ldots, x_n) = f(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$$

In short, $\sigma f = f \circ \sigma^{-1}$. For example, for $n = 3$, $\sigma = (12)$ a cycle of length 2,

$$\sigma(x_1^2 x_2 x_3^5) = x_2^2 x_1 x_3^5 = x_1 x_2^2 x_3^5.$$

For $\sigma = (123)$,

$$\sigma(x_1^2 x_2 x_3^5) = x_3^2 x_1 x_2^5 = x_1 x_2^5 x_3^2.$$

Let

$$f(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j).$$

Question. Do you know for which matrix $f(x_1, \ldots, x_n)$ is a determinant?

Note that for any $\sigma \in S_n$, we have $\sigma f = \pm f$. Define a map

$$\mathrm{Sgn} : S_n \to \mathbb{Z}/2\mathbb{Z}$$

via $\mathrm{Sgn}(\sigma) = -1$ if $\sigma f = -f$ and $\mathrm{Sgn}(\sigma) = 1$ otherwise.

Proposition 2.1. *(=* $\boxed{\textit{Problem 4}}$*.)* Sgn *is a group homomorphism.*

Definition 2.2. A permutation $\sigma \in S_n$ is called *even* if $\mathrm{Sgn}(\sigma) = 1$. Otherwise, it is called *odd*.

Corollary 2.3. *The subset of all even permutations is a normal subgroup of S_n.*

Definition 2.4. The subgroup of even permutations is called an *alternating group A_n*.

As we shall see in the following theorem, the sign of a permutation can be determined from its decomposition into transpositions.

Theorem 2.5. *(=* $\boxed{\textit{Problem 5}}$*.) (1) If $\tau \in S_n$ is a transposition, then* $\mathrm{Sgn}(\tau) = -1$
(2) A permutation σ is even if and only if it can be written as a product of even number of transpositions.

We now determine generators of A_n.

Theorem 2.6. *(=* $\boxed{\textit{Problem 6}}$*.) The group A_n is generated by 3-cycles of the form $(12i)$, $3 \leq i \leq n$.*

3. Derived series for S_n

Theorem 3.1. *(= $\boxed{\textit{Problem 7}}$) The symmetric group S_n is solvable for $n = 2, 3, 4$.*

Write down the explicit derived series in the proof.

Theorem 3.2. *(= $\boxed{\textit{Problem 8}}$)*

(1) $[S_n, S_n] = A_n$
(2) *For $n \geq 5$, $[A_n, A_n] = A_n$*

The following lemma might be useful (prove it if you use it):

Lemma 3.3. *Let i, j, k, ℓ, m be distinct integers. Then*

(1) $(ij)(k\ell) = [(ijk), (ij\ell)]$,
(2) $(ijk) = [(ik), (ij)]$,
(3) $(ijk) = [(ik\ell), (ijm)]$.

Theorem 3.4. *For $n \geq 5$, the group A_n is simple.*

4. Sylow subgroups of S_{p^n}

In this section you'll give an alternative proof of the first Sylow theorem. So you are NOT allowed to assume any of them!
Let $\nu(n)$ denote the maximal power of p dividing $(p^n)!$; that is, $p^{\nu(n)} | (p^n)!$ but $p^{\nu(n)+1} \not| (p^n)!$.

Lemma 4.1. $\nu(n) = 1 + p + \ldots + p^{n-1}$.

Proposition 4.2. *(= $\boxed{\textit{Problem 9}}$) The symmetric group S_{p^n} has a Sylow p-subgroup.*

Proof. Hint: proof by induction. For the induction step $n-1 \mapsto n$, subdivide S_{p^n} into p equal parts. Consider the permutation σ of order p defined explicitly as a product of p^{n-1} disjoint cycles as follows:

$$\sigma = (1, p^{n-1}{+}1, \ldots, (p{-}1)p^{n-1}{+}1) \ldots (j, p^{n-1}{+}j, \ldots, (p{-}1)p^{n-1}{+}j) \ldots (p^{n-1}, 2p^{n-1}, \ldots, (p{-}1)p^{n-1}, p^n)$$

Now using a Sylow p-subgroup of $S_{p^{n-1}}$ and the permutation σ, construct a Sylow p-subgroup for S_{p^n}. □

Definition 4.3. Let G be a group, and H, K be subgroups of G. For an element $x \in G$, the set

$$HxK := \{hxk \,|\, h \in H, k \in K\}$$

is called a *double coset* of H, K in G.

The next three statements constitute $\boxed{\text{Problem 10}}$.

Lemma 4.4. *Suppose H, K are finite subgroups of G. Then for any $x \in G$,*

$$|HxK| = \frac{|H||K|}{|H \cap xKx^{-1}|}.$$

Proposition 4.5. *Let $H < G$ be finite groups, and suppose that G has a Sylow subgroup Q. Then H has a Sylow subgroup P. Moreover, $P = H \cap xQx^{-1}$ for some $x \in G$.*

Proof. Hint: Consider double cosets HxQ, and let p^n be the maximal power of p dividing $|H|$ (so that the expected order of P is p^n). Using the formula for the size of double cosets in the Lemma above and the fact that G is a union of non disjoint double cosets, show (by contradiction) that at least one intersection $H \cap xQx^{-1}$ must have the maximal possible size p^n. □

Now, the first Sylow theorem is an easy consequence of what you already proved.

Theorem 4.6. *Any finite group whose order is divisible by p has a Sylow p-subgroup.*

5. Old Homework problem

This part is optional but if you haven't completed Problem 2.2 in Homework 3, you could do a simplified version of the proof of one of the theorems in the previous section here and claim credit for the old homework.

Problem 5.1. *(=*$\boxed{\textit{Problem 4.2 of HW 3}}$*) Describe explicitly the Sylow 2-subgroup of* S_{2^n}.