MATH 4041 HW 9

David Chen, dc3451

November 9, 2020

1

First, we want to show that any cycle $(a_1, a_2, \ldots, a_n) = \prod_{i=1}^{n-1}(a_i, a_{i+1})$. Induct on n; the case of $n = 2$ is easy, since it just reduces to $(a_1, a_2) = \prod_{i=1}^{2-1}(a_i, a_{i+1}) = (a_1, a_2)$ directly.

If we have the identity for n, then $\sigma = (a_1, a_2, \ldots, a_{n+1})$ defined by $\sigma(a_{n+1}) = a_1$, and for $i < n+1$, $\sigma(a_i) = \sigma(a_{i+1})$ and fixes every element not in $a_1, \ldots, a_{n+1}$; however, we can check that $\tau = (a_1, a_2, \ldots, a_n)(a_n, a_{n+1})$ maps the same elements to the same outputs: for $i < n$, the first permutation fixes a_i, and the second sends $a_i \mapsto a_{i+1}$. We can directly check that (a_n, a_{n+1}) takes $a_{n+1} \mapsto a_n$, and $(a_1, \ldots, a_n)$ takes $a_n \mapsto a_1$, so $\tau(a_{n+1}) = a_1$, and since (a_n, a_{n+1}) takes $a_n \mapsto a_{n+1}$ which is fixed by $(a_1, a_2, \ldots, a_n)$, we have that $\tau(a_n) = a_{n+1}$. Any element not in $a_1, \ldots, a_{n+1}$ is fixed by both $(a_1, \ldots, a_n)$ and (a_n, a_{n+1}) and is thus fixed by τ. Thus, $\tau = \sigma$ since they coincide on every input, and

$$(a_1, \ldots, a_{n+1}) = (a_1, \ldots, a_n)(a_n, a_{n+1}) = \left(\prod_{i=1}^{n-1}(a_i, a_{i+1})\right)(a_n, a_{n+1}) = \prod_{i=1}^{n}(a_i, a_{i+1})$$

so by induction this holds for a cycle of any length.

This gives us that a cycle of length n has sign $(-1)^{n-1}$.

a

We can use the algorithm given in the proof from class to see that this permutation reduces to $(1, 5, 8)(2, 3, 7, 6)$, so the sign is $(-1)^2(-1)^3 = -1$ so this permutation is odd.

b

The sign is $(-1)^3(-1)^2 = -1$ so this permutation is odd.

c

It's a square, so it has to be even.

The sign is $(-1)^5(-1)^5 = 1$, so it is even, which was what we expected.

d

The sign is $(-1)^5(-1)^5(-1)^5 = -1$, so it is odd.

e

The sign is $(-1)^3(-1)^3 = 1$, so it is even.

2

i

Consider the permutation $(a_1, a_2)(a_3, a_4)$. Pick any two disjoint pairs a_1, a_2 and a_3, a_4. There are $\binom{n}{2} = n(n-1)/2$ ways to pick the first pair, and $\binom{n-2}{2} = (n-2)(n-3)/2$ ways to pick the second. Then, since we want to discard the order between the pairs, we divide by 2, since we have currently counted both the selection of both $(a_1, a_2)(a_3, a_4)$ and $(a_3, a_4)(a_1, a_2)$ and disjoint pairs commute.

This comes out to a total of

$$\frac{\binom{n}{2}\binom{n-2}{2}}{2} = \frac{n(n-1)(n-2)(n-3)}{8}$$

ii

Consider a $k-$cycle $(a_1, a_2, \ldots, a_k)$. There are $n!/(n-k)!$ to pick the $a_1, a_2, \ldots, a_k$ distinctly from $\{1, 2, \ldots n\}$. However, this might not define a distinct permutation, since we have that $(a_1, a_2, \ldots, a_k) = (a_2, a_3, \ldots, a_k, a_1)$. In particular, for any set $\{a_1, \ldots, a_k\}$, there are k identical rotations of $(a_1, a_2, \ldots, a_k)$ which give rise to the same permutation. Then, we divide by k to compensate, giving us a total of $\frac{n!}{(n-k)!k}$.

iii

Write any $\sigma \in A_5$ as $\sigma = \prod_i^n \sigma_i$, where σ_j is a cycle of length $k_j \geq 2$ disjoint from the other σ_i. The sign of σ is then $\prod_{i=1}^n (-1)^{k_i - 1} = (-1)^{\sum_{i=1}^n k_i - n}$ as shown in the first problem of the HW (given that the sign is multiplicative).

We have that since $\sum_{i=1}^n k_i \geq \sum_{i=1}^n 2 = 2n$, that n is at most 2 (since $\sum_{i=1}^n k_n \geq 3n = 6 > 5$). Note that this condition $\sum_{i=1}^n k_1 \leq 5$ is given explicitly in the HW, but arises immediately from counting the number of distinct elements in the support of the product of σ, since each cycle moves another distinct k_j elements.

Suppose that $n = 1$. Then, σ is a cycle, and has sign $k_1 - 1$ as shown in the first problem of the HW. We have the following cases, since the cycle needs to be of odd length greater than 1.

- $k_1 = 3$. Then, there are $\frac{5!}{2!3} = 20$ $3-$cycles as shown in part ii.
- $k_1 = 5$. Then, there are $\frac{5!}{0!5} = 24$ $5-$cycles as shown in part ii.

Then, if $n = 2$, the sign of σ is $(-1)^{k_1+k_2-2} = (-1)^{k_1+k_2}$, so $k_1 + k_2 = 2$ or $k_1 + k_2 = 4$. Clearly the first is impossible if we want that $k_1, k_2 \geq 2$, so $k_1 + k_2 = 4$ and $k_1 = k_2 = 2$. From part i, there are exactly $\frac{5\cdot4\cdot3\cdot2}{8} = 15$ such products of distinct $2-$cycles.

The last one we haven't counted is the identity, bringing our total to $1 + 15 + 24 + 20 = 60$, as desired.

3

Note that H is the subgroup of S_4 which contains elements that are the product of distinct 2-cycles and the identity, but its easier to directly compute that it is a subgroup.

H is clearly a subset of S_4 and since elements are either the identity for the product of two 2-cycles, the sign of which is $(-1)^{-1}(-1)^{-1} = 1$, all the elements are even as well, so it is a subset of A_4.

H clearly contains the identity. We can do some direct computation (note that disjoint cycles commute) to see that it is closed and contains inverses.

$$
\begin{aligned}
(1,2)(3,4)\cdot(1,2)(3,4) &= (1,2)(3,4)\cdot(4,3)(2,1)\\
&= (1,2)((3,4)(4,3))(2,1)\\
&= (1,2)(2,1) = 1\\
(1,3)(2,4)\cdot(1,3)(2,4) &= (1,3)(2,4)\cdot(4,2)(3,1)\\
&= (1,3)(3,1) = 1\\
(1,4)(2,3)\cdot(1,4)(2,3) &= (1,4)(2,3)\cdot(3,2)(4,1)\\
&= (1,4)(4,1) = 1\\
(1,2)(3,4)\cdot(1,3)(2,4) &= \begin{pmatrix}1&2&3&4\\3&4&1&2\\4&3&2&1\end{pmatrix} = (1,4)(2,3)\\
(1,3)(2,4)\cdot(1,2)(3,4) &= \begin{pmatrix}1&2&3&4\\2&1&4&3\\4&3&2&1\end{pmatrix} = (1,4)(2,3)\\
(1,2)(3,4)\cdot(1,4)(2,3) &= \begin{pmatrix}1&2&3&4\\4&3&2&1\\3&4&1&2\end{pmatrix} = (1,3)(2,4)\\
(1,4)(2,3)\cdot(1,2)(3,4) &= \begin{pmatrix}1&2&3&4\\2&1&4&3\\3&4&1&2\end{pmatrix} = (1,3)(2,4)\\
(1,3)(2,4)\cdot(1,4)(2,3) &= \begin{pmatrix}1&2&3&4\\4&3&2&1\\2&1&4&3\end{pmatrix} = (1,2)(3,4)\\
(1,4)(2,3)\cdot(1,3)(2,4) &= \begin{pmatrix}1&2&3&4\\3&4&1&2\\2&1&4&3\end{pmatrix} = (1,2)(3,4)
\end{aligned}
$$

so we can see that each element is its own inverse and is closed under composition, and is thus a subgroup. Further, we can see that it is commutative.

Define the bijection $f : H \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ such that

$$
\begin{aligned}
f(1) &= (0,0)\\
f((1,2)(3,4)) &= (1,0)\\
f((1,3)(2,4)) &= (0,1)\\
f((1,4)(2,3)) &= (1,1)
\end{aligned}
$$

Checking that this is an isomorphism (clearly it is bijective), since H commutes it is enough to check the following:

$$f((1,2)(3,4)\cdot(1,3)(2,4)) = f((1,4)(2,3)) = (1,1) = f((1,2)(3,4)) + f((1,3)(2,4))$$
$$f((1,2)(3,4)\cdot(1,4)(2,3)) = f((1,3)(2,4)) = (0,1) = f((1,2)(3,4)) + f((1,4)(2,3))$$
$$f((1,3)(2,4)\cdot(1,4)(2,3)) = f((1,2)(3,4)) = (1,0) = f((1,3)(2,4)) + f((1,4)(2,3))$$

And as seen above, for any $\tau \in H$,

$$f(\tau^2) = 1 = (1,0) + (1,0) = (1,1) + (1,1) = (0,1) + (0,1) = f(\tau) + f(\tau)$$

4

First, we want to show that if $\sigma = (a_0, a_1, \ldots, a_{k-1})$, then $\sigma^\alpha(a_i) = a_r$ where $i + \alpha = kq + r$, where $q \in \mathbb{Z}$, $0 \le r \le k-1$. This r is unique and always exists from the number theory classes. Clearly this holds for $\alpha = 0$, since $i + 0 = i$, and we already have $0 \le i \le k-1$. Then, if it holds for $\alpha \ge 0$, then $\sigma^{\alpha+1}(a_i) = \sigma^\alpha(\sigma(a_i))$. Now, if $i = k-1$, then $\sigma^\alpha(\sigma(a_{k-1})) = \sigma^\alpha(a_0) = a_r$ where $r = \alpha - kq$ for some integer q. Then, this is exactly what we wanted, since $k-1+(\alpha+1) = \alpha+k = r+kq+k = r+k(q+1)$. Further, if $i < k-1$, then we have by the inductive hypothesis that $\sigma^\alpha(\sigma(a_i)) = \sigma^\alpha(a_{i+1}) = a_r$ where $r = (i+1) + \alpha - kq$, but again we have that $i + (\alpha+1) = i+1+\alpha = r+kq$. In either case, we have that $\sigma^{\alpha+1}(a_i) = a_r$ where $i + (\alpha+1) = r + kq$ for some integer q.

Then for $\alpha < 0$, $\sigma^{-\alpha}(a_i) = a_r$ where $i - \alpha = kq + r$. Then, $\sigma^\alpha(a_r) = a_i$ where $r + \alpha = -kq + i$; but this is exactly the same as the condition in positive case.

This now tells us that $\sigma^k(a_i) = a_i$, since i satisfies that $i + k = kq + r$ with $q = 1, r = i$. Then, $\sigma^k = 1$, and for any $0 < \alpha < k$, $\sigma^\alpha(a_0) = a_\alpha \ne a_0$, since $0 + \alpha = kq + r$ with $q = 0, r = \alpha$. Thus, the order of σ is k.

Err, just realized that the problem has a, not α as the exponent. Oops!

Then, take $\alpha, \beta \in \mathbb{Z}$, $\gcd(\alpha, k) = 1$. We have then that $\alpha x + ky = \beta$ has integral solutions x, y, so $\sigma^\beta = \sigma^{\alpha x + ky} = (\sigma^\alpha)^x(\sigma^k)^y = (\sigma^\alpha)^x$, so $\langle\sigma^\alpha\rangle \supseteq \langle\sigma\rangle$. Clearly since $(\sigma^\alpha)^x = \sigma^{\alpha x}$, $\langle\sigma^\alpha\rangle \subseteq \langle\sigma\rangle$, so $\langle\sigma^\alpha\rangle = \langle\sigma\rangle$.

We now want that $O_\sigma(i) \subseteq O_{\sigma^\alpha}(i)$. To see this, we have that for any element $\sigma^\beta(i) \in O_\sigma(i)$, $\sigma^\beta = (\sigma^\alpha)^x$ for some integral x, and so $(\sigma^\alpha)^x(i) \in O_{\sigma^\alpha}(i)$ also satisfies $(\sigma^\alpha)^x(i) = \sigma^\beta(i) \in O_\sigma(i)$, so $O_\sigma(i) \subseteq O_{\sigma^\alpha}(i)$ and $O_{\sigma^\alpha}(i) \subseteq O_\sigma(i)$, so the orbits of σ^α are the same as the orbits of σ.

However, from class, the orbits of σ, a cycle, are $O_1, O_2, \ldots, O_N$ where $|O_i| = 1$ for $i \ge 2$, and $|O_1| = k$. By a theorem from class, we have that since σ^α has the same orbits, $\sigma^\alpha = \rho$ where ρ is a k-cycle with support O_1.

5

We have that for any k such that $2 \leq k \leq n$, $(1, k-1)(k-1, k)(1, k-1) = ((1, k-1)(k-1), (1, k-1)(k)) = (1, k)$ by the "beautiful" formula given in class. The middle term in the equality has that $(1, k-1)(k-1)$ and $(1, k-1)(k)$ are function application.

We can induct on k to see that any subgroup containing $\{(1,2), (2,3), \ldots, (n-1, n)\}$ also contains $(1, k)$ for $k \leq n$. In particular, this holds for $k = 1$ since $(1, 1) = 1$, which is the subgroup by definition. We can check the base case $k = 2$, since $(1, 2)$ is explicitly in the subgroup. Then, if $(1, k-1)$ (where $k \leq n$) is in the subgroup, we know that $(k-1, k)$ is contained in the subgroup by assumption, so $(1, k-1)(k-1, k)(1, k-1) = (1, k)$ is in the subgroup by closure.

Then, consider any transposition (i, j) for $i, j \leq n$. We have that $(1, i)$, $(1, j)$ are both in any subgroup containing $\{(1,2), (2,3), \ldots, (n-1, n)\}$, and so $(1, i)(1, j) = (i, 1)(1, j) = (i, j)$ by the identity shown in the first HW problem. This shows by closure that (i, j) is in the subgroup as well, so any subgroup containing $\{(1,2), (2,3), \ldots, (n-1, n)\}$ must contain any transposition, and since any permutation is the product of transpositions, the subgroup by closure must be the entire group S_n.

Unnumbered Question (?)

We have that every transposition is its own inverse since if $\sigma = (a, b)(a, b), \sigma(a) = (a, b)(b) = a$ and $\sigma(b) = (a, b)(a) = b$, so $\tau_i^2 = 1$ for any i.

Further, if $j \neq i \pm 1$, then we have two cases. First, if $j = i$, then $\tau_i \tau_j = \tau_i^2 = 1$. Otherwise, $j \neq i, i+1$ and $j + 1 \neq i, i+1$. Then, τ_i, τ_j are disjoint, and thus commute.

The braid relation is then immediate from the "beautiful" formula:

$$
\begin{aligned}
\tau_i \tau_{i+1} \tau_i &= (i, i+1)(i+1, i+2)(i, i+1) \\
&= ((i, i+1)(i+1), (i, i+1)(i+2)) \\
&= (i, i+2) \\
\tau_{i+1} \tau_i \tau_{i+1} &= (i+1, i+2)(i, i+1)(i+1, i+2) \\
&= ((i+1, i+2)(i), (i+1, i+2)(i+1)) \\
&= (i, i+2)
\end{aligned}
$$

6

We have that $\sigma^k(1) = k+1$ for $1 \leq k \leq n-1$ and $\sigma^k(2) = k+2$ for $1 \leq k \leq n-2$ from the formula shown in the proof of 4. Then, $\sigma^k \tau \sigma^k = (k, k+1)$. This then gives that by closure, $\{(1,2),(2,3),(3,4),\dots,(n-1,n)\} = \{\sigma^0\tau\sigma^{-0}, \sigma^1\tau\sigma^{-1}, \sigma^2\tau\sigma^{-2}, \dots, \sigma^{n-2}\tau\sigma^{-(n-2)}\}$ is contained in any subgroup containing $(1,2)$ and $(1,2,\dots,n)$. Then, by an earlier problem, we have that any subgroup containing $(1,2)$ and $(1,2,\dots,n)$ is the entirety of S_n.

7

Any alternating group element can be written as the product of an even amount of transpositions by the definition of the alternating group. In particular, let any $\sigma \in A_n$ be $\sigma = \prod_{i=1}^{2k}(a_i, b_i)$; reindexing, $\prod_{i=1}^{2k}(a_i, b_i) = \prod_{i=1}^{k}(a_{2i-1}, b_{2i-1})(a_{2i}, b_{2i})$. Then, we can clearly see that any element σ is the product of the product of two 2-cycles $(a_{2i-1}, b_{2i-1})(a_{2i}, b_{2i})$.

Consider $(i,j)(i,l)$ where $i \neq j$, $i \neq l$. If $j = l$, then this becomes $(i,j)(i,j) = 1$ since transposes are their own inverses, and if $j \neq l$, then by the identity shown in 1, $(i,j)(i,l) = (j,i)(i,l) = (j,i,l)$. Then, the product of nondisjoint two 2-cycles is 3-cycle.

Then, $\sigma = (i,j,k)(k,i,l)$ clearly fixes any element not equal to one of i,j,k,l. Then, directly computing,

$$\begin{aligned}
\sigma(i) &= (i,j,k)(l) = l \\
\sigma(j) &= (i,j,k)(j) = k \\
\sigma(k) &= (i,j,k)(i) = j \\
\sigma(l) &= (i,j,k)(k) = i
\end{aligned}$$

and

$$\begin{aligned}
((j,k)(l,i))(i) &= l \\
((j,k)(l,i))(j) &= k \\
((j,k)(l,i))(k) &= j \\
((j,k)(l,i))(l) &= i
\end{aligned}$$

and $(j,k)(l,i)$ also fix any element not i,j,k,l, so $\sigma = (j,k)(l,i)$. Then, any product of two 2-cycles is either a product of two 3-cycles if the 2-cycles are disjoint ($(i,j)(j,k) = (i,j,k)(k,i,l)$ for $i \neq j \neq k \neq l$) or is a 3-cycle (or the identity) if they are not disjoint ($(i,j)(i,l) = 1$ or (j,i,l)). Thus, for $n \geq 3$, we have that 3-cycles generate all products of two 2-cycles, which in turn generate A_n.