Teddy Einstein
Math 4320

HW2 Solutions

Problem 1: 2.22
Find the sign and inverse of the permutation shown in the book (and below).

Proof. Its disjoint cycle decomposition is:

$$(19)(28)(37)(46)$$

which immediately makes it an even permutation because it is a product of an even number of transpositions. One can easily verify that since it is a product of disjoint transpositions, it has order 2, so the above permutation is its own inverse. □

Problem 2: 2.26
Show that an r-cycle is even if and only if r is odd.

Proof. Let $\alpha \in S_n$ with:

$$\alpha = (a_1, \ldots, a_r)$$

Then observe that α is:

$$\alpha = (a_1, a_r) \ldots (a_1 a_3)(a_1 a_2)$$

a product of $r-1$ transpositions. Naturally, $r, r-1$ have opposite parity, so α is even if and only if r is odd. □

Problem 3: 2.29i
Let $\alpha \in S_n$. Show that α is regular (α is the identity or has no fixed point and is a product of disjoint cycles of the same length) if and only if α is a power of an n–cycle.

Proof. First observe that if α is regular, then:

$$\alpha = (a_{11}, \ldots, a_{1t})(a_{21}, \ldots, a_{2t}) \ldots (a_{m1}, \ldots, a_{mt})$$

and each of $1, 2, \ldots, n$ is among the a_{ij} because if k does not appear in any of the cycles it is fixed. Observe then that:

$$(a_{11}, a_{21}, \ldots, a_{m1}, a_{12}, a_{22}, \ldots, a_{m2}, \ldots, a_{1t}, \ldots, a_{mt})^m = \alpha$$

Since every number $1, 2, \ldots, n$ appears among the a_{ij}, the above cycle must be an n cycle. To understand the motivation behind the above formula, try taking a t cycle to the s power and see what happens (perhaps use actual numbers for t,s and try cases where $t|s$ and where t, s are relatively prime).

Suppose on the other hand that α is a power of an n-cycle. Write $\alpha = (r_1, \ldots, r_n)^m$. Without loss of generality, we may assume that $0 \leq m < n$ because $\alpha^n = (1)$. Define r_ℓ for all $\ell \in \mathbb{Z}$ so that for $1 \leq i \leq n$, $r_\ell = r_i$ if and only if $r_\ell \equiv r_i (\text{mod } n)$. Observe that $\alpha^k(r_\ell) = r_{\ell+km}$, since α moves elements m slots down the cycle $(r_1, \ldots, r_n)$. Hence we see that $\alpha^k(r_i) = r_i$ if and only if $n|km$. The smallest n for which $n|km$ is

$$km = \text{lcm}(m,n) = \frac{mn}{\gcd(m,n)} \Rightarrow k = \frac{n}{\gcd(m,n)}$$

Therefore, for all i, $\alpha^k(r_i) = r_i$ whenever $k = \frac{n}{\gcd(m,n)}$ and this is the smallest such k. Set $k' = \frac{n}{\gcd(m,n)}$. Thus by applying α repeatedly to r_i, we generate outputs

$$r_i \mapsto r_{i+m} \mapsto r_{i+2m} \mapsto \ldots \mapsto r_{i+(k'-1)m} \mapsto r_i$$

so we see that the orbits of r_i, r_j are distinct whenever $i \not\equiv j (\text{mod } n)$. Since permutations are by definition bijections on $\{1, \ldots, n\}$, then $\{1, 2, \ldots, n\}$ can be partitioned into disjoint orbits[1] $O_1, \ldots, O_r$ each containing exactly k' elements. Hence α is a product of r disjoint $k'-$cycles where each cycle consists of the k' elements in O_i. If α has a fixed point, then $k' = 1$, so α fixes every element of $\{1, 2, \ldots, n\}$ in which case α is the identity. Therefore, α is regular, as claimed. □

Problem 4:
How many elements of S_6 have the same cycle structure as $(135)(246)$.

Solution: Any permutation in S_6 with 2 disjoint 3-cycles can be constructed as follows: We may insist that the first cycle contains 1. There are $\binom{5}{2} = 10$ ways to choose the remaining entries of the cycle. Observe that given any 3 numbers, there are exactly 2 ways to make a 3 cycle out of them.[2] Hence there are 20 possible arrangements for the 3 cycle which contains 1. The other 3-cycle's entries are determined by the first, so given the first cycle, there are two possible arrangements for the second. Hence there are 40 such permutations in S_6.

Problem 5:
Show that given a permutation $\sigma \in S_\ell$, the minimal number of simple transpositions needed to express σ as a product thereof is equal to the number of inversions of σ.

Lemma 0.1. *Let σ be a permutation and $\tau \equiv (i, i+1)$ a simple transposition. If σ has n inversions, then $\sigma\tau$ has $n-1$ inversions if $(i, i+1)$ is an inversion of σ and $n+1$ inversions otherwise.*

[1]The orbit of x under α is defined to be $\{y : y = \alpha^k(x), k \in \mathbb{Z}\}$. In other words, the orbit of x is the set of all points that can be reached from x by applying α to x. Note that orbits are indeed disjoint because if $x = \alpha^k(y)$, then $\alpha^{-k}(x) = y$ so x is in the orbit of y if and only if y is in the orbit of x. In fact, you can check for yourself that $x \sim y$ if and only if x and y are in the same orbit is an equivalence relation.

[2]By convention, we can make the smallest number appear first in the cycle, there are two choices for the second entry and the final entry is fixed.

Proof. First we claim if (j,k) is an inversion of σ,τ with $j<k$ and $j,k\neq i,i+1$, then (j,k) is an inversion of τ. Since τ fixes j,k, we see that $\sigma\tau(k)=\sigma(k)$ and $\sigma\tau(j)=\sigma(j)$, so $\sigma\tau(j)=\sigma(j)>\sigma(k)=\sigma\tau(k)$ since (j,k) is an inversion of σ. Hence (j,k) remains an inversion of $\sigma\tau$.

Next we claim that if (i,j), $j\neq i+1$, is an inversion of σ, then $(i+1,j)$ is an inversion of $\sigma\tau$. Suppose first that $i<j$. Then $i+1<j$ since $i<j$ and $j\neq i+1$. We have that $\sigma\tau(i+1)=\sigma(i)>\sigma(j)=\sigma\tau(j)$. So we have an inversion. On the other hand if $i>j$, we still have $i+1>j$, so $\sigma\tau(i+1)=\sigma(i)>\sigma(j)=\sigma\tau(j)$, and $(i+1,j)$ is an inversion.

By essentially the same argument, if $(i+1,j)$ is an inversion of σ, then (i,j) is an inversion of $\sigma\tau$.

Now, if $(i,i+1)$ is an inversion, then $\sigma\tau(i+1)=\sigma(i)>\sigma(i+1)=\sigma\tau(i)$, so $(i,i+1)$ is no longer an inversion. On the other hand, if $(i,i+1)$ is not an inversion of σ, then $\sigma\tau(i+1)=\sigma(i)>\sigma(i+1)=\sigma\tau(i)$, so that $(i,i+1)$ now becomes an inversion.

If we observe that $\sigma\tau\tau=\sigma$, applying the above twice, we see that the only inversion that $\sigma\tau$ can possibly have which is not in $1-1$ correspondence with an inversion of σ is $(i,i+1)$. Similarly, $\sigma\tau$ can have exactly 1 inversion which is not in $1-1$ correspondence. Furthermore, the result shows that $\sigma\tau$ has an extra inversion when $(i,i+1)$ is not an inversion of σ and $\sigma\tau$ has 1 fewer inversion ($(i,i+1)$ is removed). □

and now the main problem:

Proof. Proof proceeds by induction on n where n is the number of inversions of σ. Suppose σ has no consecutive $(i,i+1)$ such that (i,j) is an inversion of σ. Then $\sigma(i+1)>\sigma(i)$ for all i so that in general,[3] $\sigma(i)>\sigma(j)$ whenever $i>j$. Suppose $\sigma(i)>i$ for some i. Then we see that $\sigma(i)\geq i+1$, so $\sigma(i+2)\geq i+2$ and by repeating this process $n-i$ times, $\sigma(n)\geq n+1$ which is impossible. Thus $\sigma(i)\leq i$, so $\sigma(1)=1$ which means that $\sigma(2)=2$ and so on so that $\sigma(i)=i$ for all i. Consequently, σ is the identity and hence has no inversions.

If σ has 0 inversions, then by the above, σ is the identity and the statement holds trivially. Now suppose the result holds for $n-1$, that is any permutation which has $n-1$ or fewer inversions, can be expressed as a product of $n-1$ simple transpositions and this is the minimal number of simple transpositions needed. Given a permutation $\sigma\in S_\ell$ with n inversions with $n\geq 1$, then σ has at least one consecutive pair $(i,i+1)$ which is an inversion of σ (or else the argument for the base case shows that σ is the identity). Let $\tau=(i,i+1)\in S_\ell$. By the preceding lemma, $\sigma\tau$ has exactly $n-1$ inversions, so $\sigma\tau$ is a product of $n-1$ simple transpositions. Thus we have that $(\sigma\tau)\tau=\sigma$ is a product of n simple transpositions.

Now we need to prove minimality. Suppose toward a contradiction that $\sigma=\tau_k\dots\tau_2\tau_1$ where $k<n$ and the τ_i are simple transpositions. Let $\tau_1=(ab)$. If (a,b) is an inversion of σ, then $\sigma\tau_1$ has $n-1$ inversions by the above lemma, but $\sigma\tau_1=\tau_k\dots\tau_2$, a product of $k-1<n-1$ simple transpositions

[3] Apply a simple induction argument.

which contradicts the inductive hypothesis. On the other hand, if (a, b) is not an inversion of σ, then $\sigma\tau_1$ has $n+1$ inversions. Since the preceding lemma shows that multiplying on the right by a simple transposition changes the number of inversions by at most 1 in any direction, we see that $\sigma\tau_1\tau_2\ldots\tau_k$ must have at least $n+1-(k-1) = (n-k)+2 > 0$ inversions. However, $\sigma\tau_1\tau_2\ldots\tau_k = \tau_k\ldots\tau_2\tau_1\tau_1\tau_2\ldots\tau_k = (1)$ which has zero inversions, so we have a contradiction. Therefore, it follows by induction that σ can be expressed as a product of n simple transpositions and cannot be expressed as a product of fewer than n simple transpositions. □

Postscript: (How to actually come up with the solution)

Inversions can be visualized nicely as follows. Arrange two rows of n vertices labelling them 1 through n from left to right in order. If σ maps 1 to k, draw an edge from 1 in the top row to k in the bottom row. Continue similarly for all elements in the top row i.e. if $i \mapsto j$, draw an edge from i in the top row to j in the bottom row. Convince yourself that the number of crossings corresponds to the number of inversions of σ. Observe that multiplying by a simple transposition $(i, i+1)$ on the right corresponds to switching the vertices $i, i+1$ in the top row (i.e. the edges connected to i and $i+1$ in the top row are swapped). This will either induce or undo a crossing between the edges crossing $i, i+1$ while the fact that they are consecutive will lead to these edges swapping their crossings as well. This is the fundamental idea behind the lemma which leads to the solution.

Problem 6: 2.39i

How many elements of order 2 are there in S_5, S_6.

Solution: By proposition 2.55, the order of any permutation is the least common multiple of the cycles in a disjoint cycle decomposition. In order for the least common multiple of a collection of positive integers to be 2, the only choices are $1, 2$. Since a 1−cycle is the identity, every permutation of order 2 can be written as a product of disjoint 2 cycles.

Count as follows:

Permutations which move 1: There are 4 choices for elements to be paired with 1 in the transposition. Thus leaving $\binom{3}{2} = 3$ choices for a second transposition plus 1 for the possiblity that we just have a transposition, yielding 16 choices.

Permutations fixing 1 but moving 2. There are 3 choices for elements to be paired with 2 in a transposition. Thus leaving $\binom{2}{2} = 1$ choices for a second transposition plus 1 for the possiblity that we just have a transposition, yielding 6 choices.

Permutations fixing $1, 2$ but moving 3. Easily this is just $\{(34), (35)\}$. Finally, we have (45). Thus we have a total of 25 such permutations.

Now for S_6: permutations moving 1: There are 5 choices to pair with 1. For a product of 3 disjoint transpositions, we have $\binom{4}{2}$ choices for one transposition and then the other is fixed; however, this method generates duplicates, so we need to divide by 2 to get $5 \cdot \frac{1}{2} \cdot \binom{4}{2} = 15$ possiblities. Additionally,

there are $5 \cdot (\binom{4}{2} + 1) = 35$ choices for products of two transpositions and single transpositions which move 1. This makes a total of 50 such permutations which move 1.

Now count permutations fixing 1 but moving 2. These must be products of 1 or 2 transpositions. There are 4 items which can be paired with 2 and $\binom{3}{2} + 1$ possibilities for the second transposition plus 1 for the identity. Hence we get 16 possiblities of this type.

For permutations fixing $1, 2$ but moving 3, we have 3 possible pairings for 3, a fixed choice of second transposition or the identity, giving 6 total possibilities.

The remaining ones are easy to count: we only have $(45), (46), (56)$. Giving an additional 3 total. Adding up all the cases, we obtain 75.

Problem 7: 2.42

Let $G = GL(2, \mathbb{Q})$ and let

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$

Show that while A, B have finite order $4, 6$ respectively, their product does not. In particular, if G is not a finite group, a subgroup generated by elements of finite order may in fact have infinite order.

Proof. It is straightforward to check that $A^4 = B^6 = I_2$. Observe that:

$$AB = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$$

A standard induction argument (which you should have produced) shows that:

$$(AB)^n = AB = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$$

so that $\langle A, B \rangle \leq G$ does not have finite order. □

Problem 8:

Let G be a group. Assume that G is generated by x, y, z such that $x^4 = y^4 = z^4 = e$, $xy = z$, $yz = x$, $zx = y$ and $x^2 = y^2 = z^2$.

Proof. We first claim that every element of G can be represented in the form $x^m y^n$ where $0 \leq m, n \leq 3$. Given a word α in x, y, z, we can immediately eliminate z by applying the relation $z = xy$. Let β be the word α with the substitution $z = xy$ applied Now observe that since $z = xy$ and $yz = x$, substituting the first equation into the second, we obtain $yxy = x$ so that $yx = xy^{-1} = xy^3$. If β is not of the form $x^m y^n$ with $m, n \in \mathbb{Z}$, then β has the form $x^m y \ldots$, and there are k instances of x following the first y. By applying the relation $yx = xy^3$ the first x following the first y can be moved left of the first y in finitely many steps yielding a word with $k-1$ instances of x following the first y. Applying the above process inductively yields a word γ of the form x^m, y^n with $m, n \in \mathbb{Z}$. We may

further assume that $0 \leq m, n \leq 3$ because if r_m, r_n are the remainders[4] mod 4 for m, n respectively, then

$$x^m = x^{r_m} \qquad y^n = y^{r_n}$$

because $x^4 = y^4 = e$. Thus every element of G can be represented as $x^m y^n$ where $0 \leq m, n \leq 3$ (note these may not and in fact, cannot be distinct).

Hence G is finite with at most 16 distinct elements. By using the fact $x^2 = y^2$ however, we see that the following elements are the same:

$$x^2 = y^2 \qquad x^2y^2 = e \qquad x^3y = xy^3 \qquad xy^2 = x^3 \qquad y^3 = x^2y$$

$$x = x^{-3} = x^{-1}y^{-2} = x^3y^2 \qquad x^2y^3 = x^4y = y \qquad x^3y^3 = xx^2y^2y = xy$$

We have 8 relations linking distinct elements, so there can be at most 8 elements in G.

This is an admittedly ugly (but elementary) solution. A cleaner solution can be derived as follows. Let $H = \langle x \rangle$ and $K = \langle y \rangle$. Since every element of G has the form $x^m y^n$, then we see that $HK = G$. The following formula is well known (and not that hard to derive):

$$|G| = |HK| = \frac{|H||K|}{|H \cap K|}$$

Since $|H||K| \leq 4 \cdot 4$ and we know that $|H \cap K| \geq 2$, since $e, x^2 = y^2 \in H \cap K$, then the above formula shows that $|G| \leq 8$. □

[4] i.e. $m = 4q + r_m$ where $q \in \mathbb{Z}$ and $0 \leq r_m \leq 3$.