Homework 3 solutions.

Problem 6.1. Write out a multiplication table for S_3.

Answer.

$\cdot$	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(132)	(123)	(23)	(13)
(13)	(13)	(123)	e	(132)	(12)	(23)
(23)	(23)	(132)	(123)	e	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	e
(132)	(132)	(23)	(12)	(123)	e	(123)

□

Problem 6.2. Express each of the following elements of S_8 as a product of disjoint cyclic permutations, and as a product of transpositions. Which, if any, of these permutations belong to A_8?

Answer.

- $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 4 & 1 & 8 & 2 & 3 & 5 \end{bmatrix}$:
  As a product of disjoint cycles, this is (1734)(26)(58). As a product of transpositions, this is (14)(13)(17)(26)(58). Since there are an odd number of transpositions, this permutations doesn't belong to A_8.
- (4568)(1245):
  As a product of disjoint cycles, this is (125)(468). As a product of transpositions, this is (15)(12)(48)(46). There are an even number of transpositions, so this permutation does belong to A_8.
- (624)(253)(876)(45):
  As a product of disjoint cycles, this is (25687)(34). As a product of transpositions, this is (27)(28)(26)(25)(34). There are an odd number of transpositions, so this permutations does not belong to A_8.

□

Problem 6.3. Show that the elements of S_9 which send the numbers 2,5,7 among themselves form a subgroup of S_9. What is the order of this subgroup?

Proof. We showed in the last homework that if H is a finite subset of a group G then H is a subgroup iff it is closed under multiplication. Let H be the subset of S_9 that sends the numbers 2,5,7 among themselves. Since S_9 is a finite group, H is a finite subset. So we just need to show it is closed under multiplication.

Let $\alpha, \beta \in H$. Let $n \in \{2, 5, 7\}$. Then $\alpha(n) \in \{2, 5, 7\}$. Since β send the set $\{2, 5, 7\}$ to itself, $\beta(\alpha(n)) \in \{2, 5, 7\}$ as well. So $\beta \cdot \alpha$ sends the elements of the set $\{2, 5, 7\}$ among themselves. Thus, $\beta \cdot \alpha \in H$, so H is closed under group multiplication. Therefore, H is a subgroup.

Now we find the order of H. Let $\alpha \in H$. Note that α must consist of two disjoint transpositions: one which permutes the elements of $\{2, 5, 7\}$ and one which permutes the remaining numbers between 1 and 9. So we will first count the number of ways to permute the numbers 2,5,7 and then the number of ways to permute the rest of the numbers between 1 and 9.

There are 3! ways to permute elements of the set $\{2, 5, 7\}$. That's because an element $\alpha \in H$ has 3 choices of where to send 2, then 2 remaining choices of where to send 5, and finally one choice of where to send 7. Likewise, since there are six elements between 1 and 9 that are not 2, 5 or 7, there are 6! ways to permute them.

Any way of permuting 2, 5 and 7 can be paired with any way of permuting the rest of the numbers between 1 and 9 to give an element of H. And any element of H is a way of permuting 2, 5 and 7 combined with a way of permuting the rest of the numbers between 1 and 9. So there are $3! \cdot 6! = 6 \cdot 720 = 4320$ elements of H. □

Problem 6.4. Find a subgroup of S_4 which contains six elements. How many subgroups of order six are there in S_4?

Answer. The group $S_3 = \{e, (12), (23), (13), (123), (132)\}$ is a subgroup of S_4 and it has order 6.

There are 4 subgroups of order 6. □

Problem 6.5. Compute $\alpha P(x_1, x_2, x_3, x_4)$ when $\alpha_1 = (143)$ and when $\alpha_2 = (23)(412)$.

Answer. Since $\alpha_1 = (143)$ is even, we should get $\alpha_1 P = P$ and since $\alpha_2 = (23)(412)$ is odd, we should get $\alpha_2 P = -P$. But we can check this by calculating.

We start with

$$P(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

Since $\alpha_1(1) = 4, \alpha_1(2) = 2, \alpha_1(3) = 1$ and $\alpha_1(4) = 3$ we substitute every 1 by a 4 and so on to get

$$\begin{aligned}\alpha_1 P(x_1, x_2, x_3, x_4) &= (x_4 - x_2)(x_4 - x_1)(x_4 - x_3)(x_2 - x_1)(x_2 - x_3)(x_1 - x_3) \\ &= -(x_2 - x_4) \cdot -(x_1 - x_4) \cdot -(x_3 - x_4) \cdot -(x_1 - x_2) \cdot (x_2 - x_3) \cdot (x_1 - x_3) \\ &= P(x_1, x_2, x_3, x_4)\end{aligned}$$

where the last line is true because there are an even number of - signes.

Next we do the same thing with α_2. We have that $\alpha_2(1) = 3$, $\alpha_2(2) = 4$, $\alpha_2(3) = 2$ and $\alpha_2(4) = 1$.

$$\begin{aligned}\alpha_2 P(x_1, x_2, x_3, x_4) &= (x_3 - x_4)(x_3 - x_2)(x_3 - x_1)(x_4 - x_2)(x_4 - x_1)(x_2 - x_1) \\ &= (x_3 - x_4) \cdot -(x_2 - x_3) \cdot -(x_1 - x_3) \cdot -(x_2 - x_4) \cdot -(x_1 - x_4) \cdot -(x_1 - x_2) \\ &= -P(x_1, x_2, x_3, x_4)\end{aligned}$$

where the last line is true because there are an odd number of minus signs. □

Problem 6.6. If H is a subgroup of S_n and if H is not contained in A_n, prove that precisely one-half of the elements of H are even permutations.

Proof. Let H be a subgroup of S_n. If H is not contained in A_n, it must contain some odd permutation α. Then for any β in H $\alpha\beta$ is also in H. Since α is odd, it can be written as the product of an odd number of transpositions. If β is even it can be written as an even number of transpositions. That means $\alpha\beta$ can be written as an odd number of transpositions. So if β is even, then $\alpha\beta$ is odd.

We can write H as the union of sets of the form $\{\beta, \alpha\beta\}$ where β is even. That is,

$$H = \bigcup_{\beta \in H,\ \beta \text{ even}} \{\beta, \alpha\beta\}$$

To see this, note that clearly all the even elements of H are in this union. And if γ is an odd element of H, then $\alpha^{-1}\gamma$ is even (because α^{-1} is odd since α is odd). So the pair $\{\alpha^{-1}\gamma, \gamma\}$ is in the union since $\alpha\alpha^{-1}\gamma = \gamma$, so γ is in the union. Therefore all the odd and even elements of H are in the above union, so we get all of H.

Given distinct β and β', the sets $\{\beta, \alpha\beta\}$ and $\{\beta', \alpha\beta'\}$ are disjoint. To see this, note that if $\beta \neq \beta'$, then $\alpha\beta \neq \alpha\beta'$. So if two sets $\{\beta, \alpha\beta\}$ and $\{\beta', \alpha\beta'\}$ were not disjoint then we must have that either $\beta = \alpha\beta'$ or $\beta' = \alpha\beta$. But β and β' are assumed to be even permutations, so we know that $\alpha\beta$ and $\alpha\beta'$ are odd. So those equalities cannot be true. Therefore, any two such sets are or disjoint.

Since we can write H as the disjoint union of sets where one element is even and the other element is odd, H must have the same number of odd elements as even elements. Therefore precisely one-half of the elements of H are even permutations.

□

Problem 6.7. Show that if n is at least 4 every element of S_n can be written as a product of two permutations, each of which has order 2. (Experiment first with cyclic permutations).

Proof. Note that a product of disjoint transpositions has order 2.

Let's do an example first. Take a cyclic permutation $(a_1 a_2 a_3 a_4 a_5 a_6)$. This sends a_1 to a_2 and so on in a circle.

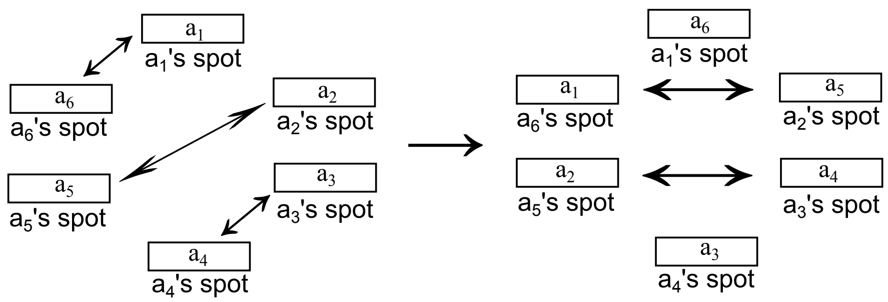

FIGURE 1. First do $(a_1\ a_6)(a_2\ a_5)(a_3\ a_4)$ and then do $(a_2\ a_6)(a_3\ a_5)$

In the above picture, we start with each a_i in its spot. We need to move each a_i one spot clockwise. So first we do transpositions $(a_1\ a_6)(a_2\ a_5)(a_3\ a_4)$ giving us the configuration shown in the right hand diagram. That is, a_6 is in a_1's spot and so on. Then we do transpositions $(a_2\ a_6)(a_3\ a_5)$ which put a_1 in a_2's spot, and generally puts a_i in a_{i+1}'s spot, which is what we needed.

Now we generalize this to any cyclic permutation. Let $\alpha = (a_1\ a_2 \ldots a_n)$ be a cyclic permutation. We will show that we can write α as the product of α_1 and α_2 where α_1 and α_2 are two permutations of order 2. Furthermore, α_1 and α_2 will each be products of disjoint transpositions where the only numbers that appear in these transpositions are the $a_1 \ldots a_n$ that appear in α.

So let $\alpha_1 = (a_1\ a_n)(a_2\ a_{n-1})\cdots(a_i\ a_{n-i+1})\cdots(a_N\ a_{n-N+1})$ where N is the biggest integer smaller than $\frac{n}{2}$ (so it's just $n/2$ if n is even.) Let $\alpha_2 = (a_2\ a_n)$ $(a_3\ a_{n-1})\ \cdots\ (a_{i+1}\ a_{n-i+1})\ \cdots\ (a_{N+1}\ a_{n-N+1})$. Note that α_1 and α_2 are each products of disjoint transpositions, so they have order 2.

Then we claim that $\alpha_2\alpha_1 = \alpha$. Since α_1 and α_2 are products of disjoint transpositions, what they do to any one a_i is determined just by the transposition containing that a_i. So for $i \leq N$, the transposition $(a_i\ a_{n-i+1})$ in α_1 sends a_i to a_{n-i+1} and then the transposition $(a_{i+1}\ a_{n-i+1})$ in α_2 sends a_{n-i+1} to a_{i+1}. So $\alpha_2\alpha_1$ sends a_i to a_{i+1} if $i \leq N$. If $i > N$ set $j = n - i + 1$. Note that $j \leq N$ since $i > N$ because N is at most $n/2$. We then have that $i = n - j + 1$. So the transposition $(a_j\ a_{n-j+1})$ is in α_1 and it sends $a_i = a_{n-j+1}$ to a_j and the transposition $(a_{j-1+1}\ a_{n-(j-1)+1}) = (a_j\ a_{n-j+2})$ in α_2 sends a_j to a_{n-j+2}. But since $j = i-n+1$, $n - j + 2 = i + 1$. Thus $\alpha_2\alpha_1$ sends a_i to a_{i+1} when $i > N$ as well. So $\alpha_2\alpha_1$ is indeed α.

Now let β be any permutation. Write β as the product of disjoint permutations β_i, so that $\beta = \beta_1 \cdots \beta_k$. Then each β_i can be written as the product of two transpositions $\alpha_{i,1}$ and $\alpha_{i,2}$ each of order 2 where $\alpha_{i,1}$ and $\alpha_{i,2}$ only permute the numbers that appear in β_i. Since the β_i are disjoint, if $j \neq i$, then $\alpha_{i,1}$ and $\alpha_{i,2}$ are disjoint from $\alpha_{j,1}$ and $\alpha_{j,2}$. So $\alpha_{i,1}$ commutes with $\alpha_{j,1}$and $\alpha_{i,2}$ for all $j \neq i$. Thus we can write

$$\begin{aligned}\beta &= \beta_1 \cdots \beta_k \\ &= \alpha_{1,2}\alpha_{1,1} \cdots \alpha_{k,2}\alpha_{k,1}\end{aligned}$$

Since $\alpha_{i,2}$ is to the left of $\alpha_{i,1}$ we can move $\alpha_{i,1}$ as far to the right as we want. So we can move all the $\alpha_{i,1}$'s to the right of all the $\alpha_{i,2}$'s. So,

$$\beta = \alpha 1, 2 \cdots \alpha_{k,2} \cdot \alpha 1, 1 \cdots \alpha_{k,1}$$

Define $\alpha_1 = \alpha 1, 1 \cdots \alpha_{k,1}$ and $\alpha_2 = \alpha 1, 2 \cdots \alpha_{k,2}$. Note that since the $\alpha i, 2'$'s are all disjoint and have order 2, and the $\alpha_{i,1}$'s are all disjoint and have order 2, both α_1 and α_2 have order 2. We have showen that $\beta = \alpha_2\alpha_1$ so β is the product of two permutations of order 2. $\square$

Problem 6.8. If $\alpha, \beta \in S_n$, check that $\alpha\beta\alpha^{-1}\beta^{-1}$ always lies in A_n and that $\alpha\beta\alpha^{-1}$ belongs to A_n whenever β is an even permutation. Work out these elements when $n = 4, \alpha = (2143)$ and $\beta = (423)$.

Proof. Since transpositions generate S_n write α as the product of n transpositions. Then α^{-1} can be written as a product of the transpositions of α taken in the opposite order. So if β can be written as the product of m transpositions, β^{-1} can also be written as the product of m transpositions. Then by composing the corresponding products of transpositions, we can write $\alpha\beta\alpha^{-1}\beta^{-1}$ as the product of $n+m+n+m = 2(n+m)$ transpositions. This is an even number of transpositions regardless of what n and m are. So $\alpha\beta\alpha^{-1}\beta^{-1} \in A_n$.

Suppose $\alpha\beta\alpha^{-1}$ belongs to A_n. If α can be written as a product of n transpositions and β can be written as a product of m transpositions, then $\alpha\beta\alpha^{-1}$ can be written as a product of $2n+m$ transpositions. Since $\alpha\beta\alpha^{-1}$ belongs to A_n, $2n+m$ is even. And since $2n$ is even, m must be even as well. Thus β can be written as an even number of transpositions, so $\beta \in A_n$.

Now let $n = 4, \alpha = (2143)$ and $\beta = (423)$. To do the method described above, we would write $\alpha = (23)(24)(21)$ and $\beta = (43)(42)$. Then $\alpha^{-1} = (21)(24)(23)$ and $\beta^{-1} = (42)(43)$. So $\alpha\beta\alpha^{-1}\beta^{-1} = (23)(24)(21) \cdot (43)(42) \cdot (21)(24)(23) \cdot (42)(43)$.

Since α and β are cyclic permutations, however, $\alpha\beta\alpha^{-1}\beta^{-1}$ is a bit easier to compute. We have $\alpha^{-1} = (3412)$ and $\beta^{-1} = (324)$. So $\alpha\beta\alpha^{-1}\beta^{-1} = (2143)(423)(3412)(324) = (124)$ which is in A_4 and $\alpha\beta\alpha^{-1} = (2143)(423)(3412) = (123)$ which is also even since β is. □

Problem 6.9. When n is odd show that (123) and $(1, 2, \ldots, n)$ together generate A_n. When n is even show that (123) and $(2, 3, \ldots, n)$ together generate A_n.

Proof. We will work with A_n for $n \geq 4$ since A_3 is generated by (123), so there is nothing to show.

Note that Theorem 6.5 actually showed that A_n is generated by 3-cycles of the form $(1ab)$.

Remark. Three cycles of the form $(1\ a\ a+1)$ generate A_n.

Proof. Note that $(1\ a+1\ a+2)(1\ a\ a+1) = (1\ a\ a+2)$. We can generalize this. That is, if $b > a$ then

$$(1ab) = (1\ b-1\ b)(1\ b-2\ b-1)\cdots(1\ a+1\ a+2)(1\ a\ a+1)$$

If $b < a$ then $(1ab) = (1ba)^2$ where $(1ba)$ can be written as a product of elements of the form $(1\ k\ k+1)$ as shown above. Since 3-cycles of the form $(1\ k\ k+1)$ are in A_n, and they can be multiplied to get any 3-cycle of the form $(1ab)$, we have that 3-cycles of the form $(1\ k\ k+1)$ generate A_n. □

Remark. A_n is generated by elements of the form $(a, a+1, a+2)$.

Proof. Note that $(234)(123)(234)^{-1} = (134)$ (and since $n \geq 4$ these elements are in A_n). Again, we can generalize this. That is, for any $b > 1$, we have $(1\ b\ b+1) = (b-1\ b\ b+1)(b-2\ b-1\ b)\cdots(234)(123)(234)^{-1}\cdots(b-2\ b-1\ b)^{-1}(b-1\ b\ b+1)^{-1}$.

Again, since 3-cycles of the form $(k\ k+1\ k+2)$ are in A_n, and they can be multiplied to get any 3-cycle of the form $(1\ b\ b+1)$, we have that 3-cycles of the form $(k\ k+1\ k+2)$ generate A_n. □

Let n be odd. Let H be the subgroup generated by (123) and $(1, 2, \ldots, n)$. Clearly $(123) \in A_n$. Since n is odd, $(1, 2, \ldots, n) \in A_n$. So H is a subgroup of A_n. We need to show that any element of A_n is in H.

Note that $(12\ldots n)(abc)(12\ldots n)^{-1} = (a+1\ b+1\ c+1)$ where we take $a-1, b-1$ and $c-1$ mod n, so if for example $a = 1$ then $a - 1 = n$. This is because if we start with some number $d-1$, then $(12\ldots n) \cdot (d-1) = d$. If d is not one of a, b, c then $(abc)(d) = d$. Then $(12\ldots, n)^{-1}(d) = d - 1$. So the permutation $(12\ldots n)^{-1}(abc)(12\ldots n)$ leaves $d-1$ fixed whenever d is not a, b or c. And one can check that it send $a-1$ to $b-1$ and so on.

Applying this to the generators of H, $(12\ldots n)(123)(12\ldots n)^{-1} = (234)$. In fact for any number a, $(12\ldots n)^{a-1}(123)(12\ldots n)^{-(a-1)} = (a\ a+1\ a+2)$, where again subtraction is mod n. Thus all 3-cycles of the form $(a\ a+1\ a+2)$ are in H. Since these 3-cycles generate A_n, we have that $H = A_n$.

Now let n be even. In this case, (123) and $(23\ldots n) \in A_n$. We now need to show that every element of $H =< (123), (23\ldots n) >$ is in A_n. Note that $(23\ldots n)(123)(23\ldots n)^{-1} = (134)$. In general, $(23\ldots n)^{a-2}(123)(23\ldots n)^{-(a-2)} =$

$(1\ a\ a+1)$. We have shown that elements of the form $(1\ a\ a+1)$ generate A_n so again $H = A_n$. □

Problem 6.11. Find the order of each permutation listed in Exercise 6.2.

Answer. The order of a permutation is the lcm of the lengths of the disjoint cycles. So the order of $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 4 & 1 & 8 & 2 & 3 & 5 \end{bmatrix} = (1734)(26)(58)$ is 4. The order of $(4568)(1245) = (125)(468)$ is 3. And the order of $(624)(253)(876)(45) = (25687)(34)$ is 10. □

Problem 7.1. Check that the numbers 1,2,4,5,7,8 form a subgroup under multiplication modulo 9 and show that this group is isomorphic to $\mathbb{Z}_6$.

Proof. Let G be the set $\{1, 2, 4, 5, 7, 8\}$ under multiplication mod 9. The set is closed under multiplication since this set has all the numbers between 1 and 9 that share no common factors with 9. So products of elements in this set will also have no common fact with 9, and this property is preserved when we take products mod 9. 1 is the identity in this set. The numbers 2 and 5 are inverses, the numbers 4 and 7 are inverses and the number 8 is its own inverse. So this set has inverses. It's associative because multiplication mod 9 is associative. Therefore, G is a group.

We define the following map $f : G \to \mathbb{Z}_6$. Let $f(1) = 0$ because we need to send the identity of G to the identity of $\mathbb{Z}_6$. Since 2 generates G, deciding where to send 2 determines where the other elements go because we need f to be a homomorphism. Let $f(2) = 1$. Then since $2 \times_9 2 = 4$ we have $f(4) = f(2) + f(2) = 2$. Again, $4 \times_9 2 = 8$ means $f(8) = f(4) + f(2) = 3$. Next $f(7) = f(8 \times_9 2) = f(8) + f(2) = 4$ and $f(5) = f(2 \times_9 7) = f(2) + f(8) = 5$.

Since f sends distinct elements of G to distinct elements of $\mathbb{Z}_6$, it is one to one. Since every element of $\mathbb{Z}_6$ has some element of G sent to it, f is onto. So f is a bijection. The above definitions ensure that f satisfies $f(x \times_9 y) = f(x) + f(y)$ so it is a homomorphism. Thus f is an isomorphism. □