3 Subgroups and Group Functions

10/17: 1. Let $\sigma \in S_n$ be an n-cycle, and let $\tau \in S_n$ be a 2-cycle. Show by constructing a counterexample that there exists a choice σ, τ, n such that $\langle \sigma, \tau \rangle \neq S_n$. Bonus Question: Determine for which n such an example exists.

Proof. As a particular counterexample, we may pick

$$\boxed{n = 4 \qquad \sigma = (1,2,3,4) \qquad \tau = (2,4)}$$

Notice that $\langle \sigma, \tau \rangle \cong D_4$ with $\sigma \sim r$ and $\tau \sim s$; this observation will motivate the remainder of our proof. We withhold a proof that $\langle (1,2,3,4), (2,4) \rangle \neq S_4$ in favor of proving the more general fact that for any

$$\boxed{n \geq 4}$$

we may use the n-cycle $\sigma = (1, 2, \ldots, n)$ and the 2-cycle $\tau = (2, n)$ to generate a subgroup of S_n of order $2n$. This fact will imply the desired result, as explained below. Let's begin.

We will first show that $\sigma^i \tau = \tau \sigma^{-i}$ for $i = 1, \ldots, n-1$. For the base case $n = 1$, we have by direct computation that

$$\sigma\tau = (1,2)(3,4,\ldots,n) = \tau\sigma^{-1}$$

Now suppose inductively that we have proven the claim for i. Then

$$\sigma^{i+1}\tau = \sigma(\sigma^i\tau) = \sigma(\tau\sigma^{-i}) = (\sigma\tau)\sigma^{-i} = (\tau\sigma^{-1})\sigma^{-i} = \tau\sigma^{-(i+1)}$$

as desired.

We will now prove that

$$\langle \sigma, \tau \rangle = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1}\}$$

via a bidirectional inclusion proof. This will imply our desired result by inspection. The right-to-left case follows directly from the definition of generators. For the left-to-right case, let $x \in \langle \sigma, \tau \rangle$ be arbitrary. Then x is equal to a finite product of σ's and τ's, i.e., $x = \tau^i \sigma^j \tau^k \sigma^\ell \cdots$. With respect to i, k, and other exponents of the τ's: If these numbers are not congruent to 1 mod 2, then that term (e.g., $\tau^i, \tau^k, \ldots$) is equal to the identity (because $|\tau| = 2$). Thus, we may rewrite $x = \tau\sigma^i\tau\sigma^j \cdots$. Invoking the above rule, we can combine that τ's further:

$$x = \tau\tau\sigma^{-i}\sigma^j \cdots = \sigma^{j-i} \cdots$$

It should not be hard to see that τ only appears in the fully condensed decomposition of x iff τ appears an odd number of times in the expanded decomposition. In other words, τ appears at most once (and when it does show up, we can make it appear on the leftmost side of the equation). Moreover, the other term will be composed entirely of σ raised to some power, which we can take mod n since $|\sigma| = n$. Thus, $x = \tau^k \sigma^i$ for some $k = 0, 1$ and $0 \leq i \leq n-1$. Therefore,

$$x \in \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1}\}$$

so we have the desired set equality. As stated above, it follows by inspection that $|\langle \sigma, \tau \rangle| = 2n$, as desired.

To have $\langle \sigma, \tau \rangle \neq S_n$, we want $2n < n!$ (recall that $|S_n| = n!$). This inequality is satisfied for $n \geq 4$, proving our result. Note that we can confirm by casework that there are no two elements $\sigma, \tau \in S_n$ for $n = 1, 2, 3$ satisfying the desired conditions:

S_1: We cannot pick a 2-cycle in S_1.

S_2: The only 2-cycle in S_2 generates the entire set.

S_3: S_3 is generated by $\langle (1,2), (2,3) \rangle$. Any 2- and 3-cycles we pick will generate these two transpositions. □

2. Shuffling Redux. Let G be the subgroup generated by the union of the following elements.

   - $(n, 53-n)$ for all n;
   - The element $(1, 2, \ldots, 26)(52, 51, \ldots, 27)$ of order 26;
   - The element $(1, 2)(51, 52)$.

   With this definition in mind, respond to the following.

   (a) Let $H = \langle (n, 53-n) \mid n \in [52] \rangle$. Prove that $H \cong (\mathbb{Z}/2\mathbb{Z})^{26}$ inside S_{52}.

   Proof. Let $a = (a_1, \ldots, a_{26})$ be a 26-tuple, every entry of which is either 1 or 0. Define $\psi : (\mathbb{Z}/2\mathbb{Z})^{26} \to H$ by

   $$\psi(a) = \bigcirc_{i=1}^{26} (i, 53-i)^{a_i}$$

   To prove that ψ is a homomorphism, it will suffice to show that $\psi(a +_2 b) = \psi(a)\psi(b)$. But we have that

   $$\begin{aligned} \psi(a +_2 b) &= \bigcirc_{i=1}^{26} (i, 53-i)^{a_i +_2 b_i} \\ &= \bigcirc_{i=1}^{26} (i, 53-i)^{a_i} \circ (i, 53-i)^{b_i} \\ &= \left[\bigcirc_{i=1}^{26} (i, 53-i)^{a_i}\right] \circ \left[\bigcirc_{i=1}^{26} (i, 53-i)^{b_i}\right] \\ &= \psi(a)\psi(b) \end{aligned}$$

   where we get from the first to the second line via: If $a_i + b_i \leq 1$, regular exponent rules hold; if $a_i, b_i = 1$, then $a_i +_2 b_i = 0$ and $(i, 53-i)^{a_i +_2 b_i} = e$ just the same as $(i, 53-i)^1 \circ (i, 53-i)^1 = (i, 53-i)^2 = e$. We get from the second to the third line since disjoint cycles commute.
   We verify bijectivity by noting that since the generators of H are disjoint 2-cycles, every element of H can be written in the form

   $$\bigcirc_{i=1}^{26} (i, 53-i)^{a_i}$$

   with every $a_i \in \{0, 1\}$. Thus, ψ^{-1} can be defined by sending each a_i to the i^{th} slot in the 26-tuple a. It will naturally follow that $\psi \circ \psi^{-1} = I = \psi^{-1} \circ \psi$, proving bijectivity. □

   (b) Show that there is a homomorphism $\phi : G \to S_{26}$ such that...

   i. ϕ is surjective;
   ii. $\ker \phi = H$.

   (It follows from this that G has order $2^{26} \cdot 26! = 2706443181710666438004021657600000$0.)

   Proof. Define $w : [52] \to [26]$ by

   $$w(i) = \begin{cases} i & i \in [26] \\ 53 - i & i \in [27:52] \end{cases}$$

   Define $\phi : G \to S_{26}$ by

   $$\phi(g) = w \circ g|_{[26]}$$

   We now prove two lemmas.

   Lemma 1: Any $f \in G$ obeys the functional rule $f(n) + f(53-n) = 53$. This follows from the facts that all generators of G obey said functional rule, f is a composition of the generators of G, and compositions of functions that obey said functional rule obey said function rule (as per HW1, Q1).
   Lemma 2: $w(i) = w(53-i)$. We divide into two cases ($i \in [26]$ and $i \in [27:52]$). If $i \in [26]$, then $53 - i \in [27:52]$, so $w(i) = i = 53 - (53-i) = w(53-i)$. If $i \in [27:52]$, then $53 - i \in [26]$, so $w(i) = 53 - i = w(53-i)$.

   To prove that ϕ actually maps elements of G to S_{26} as defined, it will suffice to show that for any $g \in G$, $\phi(g) : [26] \to [26]$ is a bijection.

Let $g \in G$ and $i \in [26]$ be arbitrary. We divide into two cases ($g(i) \in [26]$ and $g(i) \in [27:52]$). If $g(i) \in [26]$, then $w(g(i)) = g(i) \in [26]$. If $g(i) \in [27:52]$, then $w(g(i)) = 53 - g(i) \in [26]$. Therefore, $\phi(g) : [26] \to [26]$.

Now suppose $w(g(i)) = w(g(j))$. If either $g(i), g(j) \in [27:52]$, invoke Lemmas 1-2 to rewrite $w(g(x)) = w(53 - g(x)) = w(g(53 - x))$. Since g, itself, has mirror symmetry, what we are essentially doing here is guaranteeing that both $i, j \in [26]$ or $i, j \in [27:52]$; there may be distinct $i, j \in [52]$ such that $w(g(i)) = w(g(j))$ (namely, $i, 53 - i$), but we are going to show that there is only one $i, j \in [26]$ such that $w(g(i)) = w(g(j))$. Continuing, based on our rewrite, we may assume that $g(i), g(j) \in [26]$. Now let

$$w(i) = \begin{cases} w_1(i) & i \in [26] \\ w_2(i) & i \in [27:52] \end{cases}$$

where w_1, w_2 are naturally bijections. Since $g(i), g(j) \in [26]$, we have

$$\begin{aligned} w(g(i)) &= w(g(j)) \\ w_1(g(i)) &= w_1(g(j)) \\ g(i) &= g(j) \\ i &= j \end{aligned}$$

where the last line follows since $g \in S_{52}$ is a bijection by definition. Note that if $i, j \in [27:52]$, we may take $53 - i = 53 - j$ to be the unique desired element of $[26]$.

Lastly, let $j \in [26]$. It follows from the above that either $g^{-1}(w_1^{-1}(j))$ or $g^{-1}(w_2^{-1}(j))$ is an element of $[26]$, as desired.

To prove that ϕ is a homomorphism, it will suffice to show that $\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)$ for all $\sigma, \tau \in G$. Let $\sigma, \tau \in G$ be arbitrary. Now notice that

$$\phi(\sigma\tau) = w \circ (\sigma\tau)|_{[26]} = w(\sigma(\tau)) \qquad \phi(\sigma)\phi(\tau) = (w \circ \sigma|_{[26]}) \circ (w \circ \tau|_{[26]}) = w(\sigma(w(\tau)))$$

Thus, if we let $i \in [26]$ be arbitrary, it will suffice to show that $w(\sigma(\tau(i))) = w(\sigma(w(\tau(i))))$ to prove that ϕ is a homomorphism. We divide into two cases ($\tau(i) \in [26]$ and $\tau(i) \in [27:52]$). If $\tau(i) \in [26]$, then $w(\tau(i)) = \tau(i)$, implying the desired result. If $\tau(i) \in [27:52]$, then

$$\begin{aligned} w(\sigma(w(\tau(i)))) &= w(\sigma(53 - \tau(i))) && \text{Definition of } w \\ &= w(53 - \sigma(\tau(i))) && \text{Lemma 1} \\ &= w(\sigma(\tau(i))) && \text{Lemma 2} \end{aligned}$$

as desired.

To prove that ϕ is surjective, it will suffice to show that for all $\sigma \in S_{26}$, there exists $g \in G$ such that $\phi(g) = \sigma$. Note that this argument will be distinct (but closely related to) our earlier argument that $\phi(g)$ is surjective. Take

$$\begin{aligned} g(i) &= \begin{cases} w_1^{-1}(\sigma(w(i))) & i \in [26] \\ w_2^{-1}(\sigma(w(i))) & i \in [27:52] \end{cases} \\ &= \begin{cases} \sigma(i) & i \in [26] \\ 53 - \sigma(53 - i) & i \in [27:52] \end{cases} \end{aligned}$$

Now we must prove that $g \in G$. Recall from class that $S_{26} = \langle (1,2), (1,2,\ldots,26) \rangle$, and note that $(1,2)(52,51)$ and $(1,2,\ldots,26)(52,51,\ldots,27)$ are generators of G. It follows that $(1,2)(52,51)$ and $(1,2,\ldots,26)(52,51,\ldots,27)$ generate all elements of G that permute the elements of $[26]$, and do the same permutation symmetrically to $[27:52]$. This combined with the observations that $g : [26] \to [26]$, $g : [27:52] \to [27:52]$, and g has obeys the mirror symmetry equation

$f(n) + f(53 - n) = 53$ (as is evident from its definition) proves that g is generated by these two generators, and is thus an element of G.

To prove that $\ker \phi = H$, it will suffice to show that $\phi(h) = e \in S_{26}$ for all $h \in H$. Let $h \in H$ be arbitrary. Then since h is the product of disjoint 2-cycles which are all mirror symmetric, we know that for every $i \in [26]$, h either sends $i \mapsto i$ or $i \mapsto 53 - i$. If $h : i \mapsto i$, then $w \circ h : i \mapsto i$. If $h : i \mapsto 53 - i$, then $w(h(i)) = w(53 - i) = 53 - (53 - i) = i$. Either way, $w \circ h$ is the identity on $[26]$, so $\phi(h) = e \in S_{26}$, as desired. □

(c) Prove that the group generated by the two riffle shuffles is a subgroup of G. (In fact, they are equal.)

Proof. To prove this, it will suffice to show that $A, B \in G$ because then, all products of them are naturally a subset of all products of the generators of G. Both A, B obey mirror symmetry; thus, $\phi(A), \phi(B) \in S_{26}$ because of the way ϕ is defined in part (b). It follows since ϕ is surjective that we can find, using the algorithm in part (b), elements $A', B' \in G$ such that $\phi(X') = \phi(X)$ and $X'|_{[26]} \in S_{26}$. Moreover, since A, B obey mirror symmetry, we can find $h, h' \in H$ such that $hA|_{[26]}, h'B_{[26]} \in S_{26}$. But this implies that $hA = A'$ and $hB = B'$, i.e., that $A = h^{-1}A' \in G$ and likewise for B, as desired. □

3. Let G be a finite group, and let $g, h \in G$ both have order 2. Determine the possible orders of gh.

Proof. We will prove that

$$\boxed{|gh| \text{ can be any natural number.}}$$

We divide into three cases ($|gh| = 1$, $|gh| = 2$, and $|gh| > 2$).

Suppose we want $|gh| = 1$. Consider S_2. Let $g = (1, 2)$ and $h = g^{-1} = (1, 2)$. Then clearly $|g| = |h| = 2$, but $|gh| = |e| = 1$.

Suppose we want $|gh| = 2$. Let G be some abelian group containing distinct elements of order 2 (for example, take $G = (\mathbb{Z}/2\mathbb{Z})^2$). Let g be one such element and h another. Then $(gh)^2 = ghgh = g^2h^2 = ee = e$, so $|gh| = 2$, as desired.

Suppose we want $|gh| = n$ for some $n > 2$. Consider the dihedral group D_{2n}. Let $g = rs$ and $h = s$. Then $g^2 = rsrs = rssr^{-1} = e$ and $h^2 = s^2 = e$, so $|g| = 2$ and $|h| = 2$. Moreover, $gh = rss = r$, so $|gh| = n$, as desired. □

4. Suppose that the map $\phi : G \to G$ given by $\phi(x) = x^2$ is a homomorphism. Prove that G is abelian.

Proof. To prove that G is abelian, it will suffice to show that $xy = yx$ for all $x, y \in G$. Let $x, y \in G$ be arbitrary. Then

$$xxyy = x^2y^2 = \phi(x)\phi(y) = \phi(xy) = (xy)^2 = xyxy$$

so by consecutive applications of the cancellation lemma, we have the desired result. □

5. Call a subgroup $H \subset G$ **cyclic** if $H = \langle g \rangle = \langle g, g^{-1} \rangle$ for some $g \in G$.

(a) Prove that any cyclic subgroup $H \subset G$ is abelian.

Proof. Let H be cyclic. Then $H = \langle h \rangle$. Let $x, y \in H$ be arbitrary. Then $x = h^i$ and $y = h^j$. It follows that

$$xy = h^ih^j = h^{i+j} = h^{j+i} = h^jh^i = yx$$

as desired. □

(b) Prove that any cyclic subgroup $H \subset G$ is either isomorphic to $\mathbb{Z}$ or to $\mathbb{Z}/n\mathbb{Z}$, and that the latter happens exactly when h has finite order n.

Proof. We divide into two cases (G is infinite and G is finite).
Let $G = \langle g \rangle$ be infinite. Then

$$G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, g^3, \dots\}$$

Now suppose for the sake of contradiction that $g^a = g^b$ for some distinct $a, b \in \mathbb{Z}$. Then $g^{a-b} = e$, so $|G| \leq a - b$, a contradiction. Therefore, $G = \{G^{\mathbb{Z}}\}$. In particular, we may define $\phi : \mathbb{Z} \to G$ by $k \mapsto g^k$. This map has the property that $a + b \mapsto g^a g^b$, i.e., $\phi(a)\phi(b) = \phi(ab)$.
Let $G = \langle g \rangle$ be finite. Then

$$G = \{e, g, g^2, \dots, g^{n-1}\}$$

Now suppose for the sake of contradiction that $g^a = g^b$ for some distinct $0 \leq a, b < n$ with $a > b$ WLOG. Then $g^{a-b} = e$, so $|G| \leq a - b < n$, a contradiction. Therefore, we may once again define $\phi : \mathbb{Z}/n\mathbb{Z} \to G$ as above. Note that $a + b \mapsto g^{(a+b) \mod n}$. This is still a homomorphism, though. □

(c) Let G be any group. Prove that there is a bijection between the set of homomorphisms $\{\phi : \mathbb{Z} \to G\}$ and G given by

$$\phi \mapsto \phi(1)$$

(Exercise 2.3.19 of Dummit and Foote (2004).)

Proof. To prove that the given map is bijective, it will suffice to show that it is injective and surjective.
Suppose $\phi(1) = \psi(1)$. Then if $n \in \mathbb{Z}$ is arbitrary,

$$\phi(n) = \phi(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\phi(1) \cdots \phi(1)}_{n \text{ times}} = \underbrace{\psi(1) \cdots \psi(1)}_{n \text{ times}} = \psi(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \psi(n)$$

so $\phi = \psi$, as desired.
Now let $g \in G$ be arbitrary. Define $\phi : Z \to G$ by

$$\phi(n) = g^n$$

Then $\phi(1) = g$, as desired, and ϕ is a homomorphism since

$$\phi(n + m) = g^{n+m} = g^n g^m = \phi(n)\phi(m)$$

as desired. □

(d) Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic. (Exercise 2.4.15 of Dummit and Foote (2004).)

Proof. Consider

$$\boxed{H = \left\langle 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \dots \right\rangle}$$

with addition as the group operation. H is a proper subgroup since every element of H will necessarily have 2^k in the denominator for some $k \in \mathbb{N}_0$. Moreover, H is not cyclic: Suppose for the sake of contradiction that $H = \langle g \rangle$. Then $g = n/2^k$ for some n, k. But then $1/2^{k+1}$, for instance, is unaccounted for. □

(e) Let G be a finite group. Prove that G is equal to the union of its proper subgroups if and only if it is not cyclic.

Proof. Suppose first that G is equal to the union of its proper subgroups. Each proper subgroup is generated by some proper subset of the generators of G. For there to be a nontrivial proper subset of the set of generators, the set of generators must have cardinality greater than or equal to 2. In particular, if the cardinality of this set is not 1, then G cannot be cyclic, as desired.
Now suppose that G is not cyclic. Then $\langle g \rangle$ is a proper subgroup of G for all $g \in G$; clearly, G is equal to the union of all of these subgroups. □

6. Let p be prime, and let $G = \mathrm{GL}_2(\mathbb{F}_p)$ be the group of invertible 2×2 matrices modulo p. Prove that $|G| = (p^2 - 1)(p^2 - p)$. (See §1.4 of Dummit and Foote (2004).)

Proof. First off, note that in general, we can assume the facts of the determinant that we know over $\mathbb{R}^n, \mathbb{C}^n$ hold true independent of field.

Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be a 2×2 matrix modulo p. Then $a, b, c, d \in \{0, 1, \ldots, p-1\}$. We know that A is invertible iff

$$\det(A) = ad - bc \neq 0$$

and iff the two columns $(a, c)^T, (b, d)^T$ are linearly independent.

Let's begin by counting the possible values of $(a, c)^T$. a can take on p values and c can take on p values, but in the specific case that $a = 0$, we do not want to choose $c = 0$ as well (because then $\det(A) = 0$). Thus, there are $p^2 - 1$ choices of $(a, c)^T$.

Now let's count the possible values of $(b, d)^T$ corresponding to each $(a, c)^T$. Let $(a, c)^T$ be arbitrary. WLOG assume that $a \neq 0$. We want $(b, d)^T$ to be linearly independent, but since linear independence is a requirement of both variables, we can let b be any of the p values and fix our constraint on d. We will do this. Suppose we have chosen $b \in \{0, \ldots, p-1\}$. Then $bc \in \mathbb{Z}/p\mathbb{Z}$. Moreover, since p is prime, every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ is a generator of the group of order p. Thus, there exists exactly one $d \in \{0, \ldots, p-1\}$ such that $ad = bc$, i.e., $ad - bc = 0$. Therefore, for any choice of b, there are $p - 1$ choice for d that preserve linear independence.

It follows that the total order of the group is

$$|G| = (p^2 - 1)p(p - 1) = (p^2 - 1)(p^2 - p)$$

as desired. □