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.

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}.

   (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 $2^{26} \cdot 26! = 27064431817106664380040216576000000$.)

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

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

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

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.

   (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.

   (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).)

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

   (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.

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).)