Week 3, Due Mon 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 and τ and 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 of S_{52} generated by all 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 $(1, 2)(51, 52)$.

   (a) Prove that the elements of the form $(n, 53-n)$ generate the a subgroup H isomorphic $(\mathbf{Z}/2\mathbf{Z})^{26}$ inside S_{52}.

   (b) Show that there is a homomorphism from G to the group S_{26}, such that:

      i. The homomorphism is surjective.

      ii. The kernel is precisely the subgroup 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 $g \in G$ and $h \in G$ 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. Say that a subgroup H of G is cyclic if it is of the form $H = \langle g \rangle := \langle g, g^{-1} \rangle$ for some element $g \in G$.

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

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

   (c) Prove that if G is any group, there is a bijection from the set of homomorphisms from $\mathbf{Z}$ to G and elements of G, given by $\phi : \mathbf{Z} \to G$ goes to $\phi(1)$. (2.3 (19)).

   (d) Exhibit a proper subgroup of $\mathbf{Q}$ which is not cyclic (2.4 (15)).

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