1 Problem of the Week

There are weekly problems assigned which will be discussed in reading groups. A solution will also be given in the reading group. You are not expected to necessarily complete them, but it will be very useful to look through it and have some ideas about how you might go about solving the problem even if you are very unsure.

Weekly Problem 1. Let G be a group with subgroups H, K. Let $HK = \{hk | h \in H, k \in K\}$. Show that if H, K are finite, $\#HK = \frac{\#H\#K}{\#H\cap K}$

Proof. Consider $H \times K$ and define the equivalence relation $(h, k) \sim (h', k')$ if and only if $hk = h'k'$. Notice every element of $H \times K/\sim$ is in one-to-one correspondence with $hk \in HK$. Now each equivalence class has cardinality $H \cap K$ since $hk = h'k'$ implies $(h')^{-1}h = k'k^{-1}$ and thus $hk, h'k' \in H \cap K$. H, K are finite so $H \times K$ has cardinality $\#H\#K$. Hence, $\#HK = \frac{\#H\#K}{\#H\cap K}$. □

Keep in mind that in the "each equivalence class has cardinality $H \cap K$" section, we are viewing the elements (h, k) as ordered pairs rather than the result given by hk.

2 Exercises

These are exercises which will be worked through in the reading group. You are more than welcome to try them beforehand, but you are not expected to. Solutions will be posted after the reading section.

1. Complete the proof for Theorem 4.

   Proof. We show that this map is bijective.

   - For injectivity, assume $Hg^{-1} = H(g')^{-1}$. Then, $g^{-1} = h(g')^{-1}$ so $g = g'h^{-1}$ and thus $gH = g'H$.
   - For surjectivity, this follows from cosets being partitions on G which could be done as in the proof for Lagrange's

   So the result follows. □

   Note that the proof for Lagrange's does not require assuming Theorem 4, but Theorem 4 makes it so that it makes sense to talk about the cardinality of cosets of G rather than having to distinguish between the cardinality of left and right cosets

2. Let G be a group and A, B be non-empty sets in G. Prove that if $\#A + \#B > \#G$ then $AB = G$. Notation: $AB = \{ab | a \in A, b \in B\}$.

Proof. Let G be a finite group and A, B be two non-empty subsets of G. Now assume $\#A + \#B > \#G$. Notice $AB \subseteq G$ so it suffices to show $G \subseteq AB$. Let $g \in G$. Observe that $g = a(a^{-1}g)$ where $a \in A$, so there are $\#A$ ways of writing g in this form and hence $\#A$ possible $a^{-1}g$ corresponding to $\#A$ possible a. There are at most $\#G - \#B$ possible $a^{-1}g$ such that $a^{-1}g \notin B$, but $\#A > \#G - \#B$ so $G - B$ cannot possibly contain all $a^{-1}g$. It follows that there exists $a_0 \in A$ such that $({a_0}^{-1}g) \in B$ so $g = a_0({a_0}^{-1}g) = a'b' \in AB$ so $G \subseteq AB$. Hence, $G = AB$ as required. □

3. Let G be a group with subgroups H, K. Show that if H, K are proper subgroups in G then $G \neq H \cup K$.

   Proof. It suffices to show that if $H \cup K$ is a subgroup, then $H \subseteq K$ or $K \subseteq H$. Clearly if either of H, K is the trivial subgroup then the result follows. Let $h \neq e \in H, k \neq e \in K$. Then, $hk \in H \cup K$ so $hk \in H$ or $hk \in K$. This implies $k \in H$ or $h \in K$ so $H \subseteq K$ or $K \subseteq H$. □

4. (a) Show that if G has prime order then $G = \left\{g^k | k \in \mathbb{Z}\right\}$ for some $g \neq e \in G$.

   Proof. Let G be a group of prime order p. Let $g \in G$. Notice $\langle g \rangle$ is a subgroup with order $\#g$. Then, by Lagrange's theorem, $\langle g \rangle$ has order 1 or p. The only element that has order 1 is e. Hence, pick $g \neq e \in G$. Then, since $\#\langle g \rangle = p = \#G$, it follows that $G = \langle g \rangle = \left\{g^k | k \in \mathbb{Z}\right\}$ for some $g \neq e \in G$ as required. □

   (b) Let G be a finite group. Show that for $g \in G$, $\#g \mid \#G$ and that $g^{\#G} = e$.

   Proof. Let $g \in G$. $\langle g \rangle$ is a subgroup of G with order $\#g$. Then, by Lagrange's theorem, $\#g \mid \#G$. Then, $\#G = \#g \cdot k$ for some $k \in \mathbb{Z}$ so $g^{\#G} = g^{\#g \cdot k} = (g^{\#g})^k = e^k = e$. □

5. Show that if $\#G$ is even, there exists an element of order 2.

   Proof. Assume for the sake of contradiction that there is not. Consider $G \setminus \{e\}$. Then, for all $g \in G \setminus \{e\}$, g has a distinct inverse g^{-1} so $G \setminus \{e\}$ must have an even cardinality, a contradiction. □

6. Prove that HK is a subgroup if and only if $HK = KH$.

   Proof. We prove each direction in turn.

   - For one direction, let HK be a subgroup. Then, since $h, k \in HK$ for all $h \in H, k \in K$, by closure of a subgroup, $kh \in HK$ so $HK = KH$ and likewise.
   - For the other direction, assume $HK = KH$. Then, let $hk, h'k' \in HK$. It follows that $hk \cdot (h'k')^{-1} = hk(k')^{-1}(h')^{-1} = h(k''(h')^{-1}) = hh''k''' = h'''k''' \in HK$ so by the subgroup test HK is a subgroup.

Hence, the result follows. $\square$

7. Prove that if G is a finite group and H, K are subgroups of G and $\#H, \#K > \sqrt{\#G}$, then $H \cap K \neq \{e\}$.

   Proof. Let H, K be subgroups of G with $\#H, \#K > \sqrt{\#G}$. then, $\#HK = \frac{\#H\#K}{\#H\cap K} > \frac{\#G}{\#H\cap K}$ but $HK \subseteq G$ so $\#H \cap K > 1$ and $H \cap K \neq \{e\}$. $\square$