Test 3

Math 301/601

NAME: Solutions

Problem 1. Let H be a subgroup of a group G. Define the relation $\sim$ on G by $a \sim b$ if and only if $b^{-1}a \in H$. Prove that $\sim$ is an equivalence relation on G.

Solution. We must show that $\sim$ is reflexive, symmetric, and transitive; we will do so in order. As H is a subgroup, it contains the identity. Therefore, for any $a \in G$, we have $a^{-1}a = e \in H$, implying $a \sim a$ and hence that $\sim$ is reflexive.

Next, suppose that $a, b \in G$ and $a \sim b$ so that $b^{-1}a \in H$. As H is a subgroup, it is closed under taking inverses, and hence $a^{-1}b = (b^{-1}a)^{-1} \in H$, impying $a \sim b$ and hence that $\sim$ is symmetric.

Finally, suppose $a, b, c \in G$, $a \sim b$, and $b \sim c$. Then $b^{-1}a, c^{-1}b \in H$. As H is a subgroup, it is closed under the group operation. Therefore, $c^{-1}a = (c^{-1}b)(b^{-1}a) \in H$, implying $a \sim c$ and that $\sim$ is transitive. $\square$

Problem 2. Suppose G is a nontrivial group in which the only two subgroups of G are itself and the trivial subgroup.

(a) Prove that G is cyclic.

(b) Using part (a), prove that G is a finite group. (Hint: Show that an infinite group cannot have the desired property.)

(c) Using parts (a) and (b), prove that G has prime order. (Hint: Show that a finite group of composite order cannot have the desired property.)

Solution. (a) As G is nontrivial, it contains an element g that is not equal to the identity. Therefore, $\langle g \rangle$ is not the trivial subgroup (as it contains g). Now, G only has two subgrups, so $\langle g \rangle$ is either the trivial subgroup or all of G, but we have already concluded that it is not trivial, and hence $G = \langle g \rangle$; in other words, G is cyclic.

(b) We just established that G is cyclic, so let g be a generator for G. Let us consider the subgroup $\langle g^2 \rangle$. There are two possibilities, either g^2 is the identity or not. In the first case, $2 = |g| = |\langle g \rangle| = |G|$, and G is finite. In the second case, $\langle g^2 \rangle = G$, as $\langle g^2 \rangle$ is not the trivial subgroup, as it contains g^2, and G has only two subgroups. Therefore, there exists $k \in \mathbb{N}$ such that $g^{2k} = g$, implying $g^{2k-1} = e$. As $2k - 1 > 0$, we can concludue that $2k - 1 \geq |g| = |\langle g \rangle| = |G|$; in particular, G is finite.

(c) Now, suppose that n is not prime, so that there exists $a, b \in \mathbb{N}$ such that $g = ab$ and $a, b < n$. As $|g| = |G| = ab$, we have that $g^{ab} = e$. Now, $g^a \neq e$ (as otherwise we would have that $|G| \leq a < n$), but $e = g^{ab} = (g^a)^b$. Therefore, $|g^a| \leq b < n$ (in fact, $|g^a| = b$, but we do not need to know this). This tells us that $\langle g^a \rangle$ is neither trivial (as it contains g^a) nor all of G (as $|g^a| < n$), implying that G has at least three subgroups. Thus, we can conclue that n must be prime. $\square$