Shashank Singh
sss1@andrew.cmu.edu

21-373 Algebraic Structures, Fall 2011
Assignment 1
Due: Wednesday, September 21

I collaborated with the "Morewood B Tower" group in completing this assignment.

Exercise 8: Let G be a group, with some subgroup H of index $[G : H] = 2$. By definision of the index, H has 2 left cosets, one of which must be $eH = H$, and the other of which is gH, for some $g \in G\backslash H$. If for some $g_2 \in G$ $g_2 \notin H$, then $gg_2 \in H$, since otherwise, gg_2H would be another left coset of H (noting that $e \in H$, so $g_2 \neq e$. Suppose $g \in G$. If $g \in H$, then clearly $gH = Hg$. If $g \notin H$, then, for h such that $gh \in gH$, $gh \notin H$, so, since $g^{-1} \notin H$, $ghg^{-1} \in H$. Thus, since $Hg^{-1} = Hg$, $gh \in H$. Similarly, if $hg \in Hg$, then $g^{-1}hg \in H$, so $hg \in gH$. Thus, since g is an arbitrary element of G, since $gH = Hg$, H is a normal subgroup of G.

This is not necessarily true if H has index 3. For instance, let G be the set of permutations on 3 elements, and let H be the subgroup $\{(1\ 2)(3), (1)(2)(3)\}$ (where elements are denoted by their cycle decomposition). Then, since $|G|$ is finite, H has index $|G|/|H| = 3$. However, for $g = (1\ 2\ 3)$, $(1\ 3)(2) \in gH$, but $(1\ 3)(2) \notin Hg$. Thus, $gH \neq Hg$, so G has a subgroup H of index 3 that is not normal.

Exercise 9: Let G be a subgroup, and let H, K be subgroups of G.

Suppose HK is a subgroup of G.

Suppose $g \in HK$. Then, since $g^{-1} \in HK$, $\exists h \in H, k \in K$, such that $g^{-1} = hk$. Since H, K are subgroups, $h^{-1} \in H$, and $k^{-1} \in K$, so, since $g = (g^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1}$, and $k^{-1}h^{-1} \in KH$, $g \in KH$.

Suppose, on the other hand, that $g \in KH$, so that $\exists k \in K, h \in H$ with $g = kh$. Then, $g^{-1} = (kh)^{-1} = h^{-1}k^{-1}$, so $g^{-1} \in HK$, since $h^{-1} \in H$, and $k^{-1} \in K$ (as H,K are subgroups), so, since HK is a subgroup, $g \in HK$. Thus, $HK = KH$.

Suppose, on the other hand, that $HK = KH$. Since $e \in H$ and $e \in K$, $e = ee \in HK$, so $HK \neq \emptyset$. Suppose $g_1, g_2 \in HK$. Then, for some $h_1, h_2 \in H$, $k_1, k_2 \in K$, $g_1 = h_1k_1$, $g_2 = h_2k_2$. (Note, as a necessary aside, that this implies that $HK \subseteq G$, since $H, K \subseteq G$ and G is a group and consequently close under its operation.)

Show $h_1k_1k_2^{-1}h_2^{-1} = g_1g_2^{-1} \in HK$.

Exercise 10: Let G be a finite group, and an let $A \subseteq G$, such that $\frac{|G|}{2} < |A|$. Suppose $g \in G$. let $gA^{-1} = \{ga^{-1}|a \in A\}$. Since, G is a group, for $f : A \to gA^{-1}$, $G : gA^{-1} \to A$, such that $\forall a \in A$, $f(a) = ga$, and, $\forall b \in gA^{-1}$, $g(b) = g^{-1}b$, f and g are inverses and thus bijective, so $|gA^{-1}| = |A| > \frac{|G|}{2}$. If A and gA^{-1} were disjoint, then $|A \cup gA^{-1}| = |A| + |gA^{-1}| > \frac{|G|}{2} + \frac{|G|}{2}$; however, $A \cup gA^{-1} \subseteq G$, so this is not possible, and $\exists a \in A \cap gA^{-1}$. Furthermore, there must exist $b \in A$ with $a = gb^{-1}$, so that $ab = gb^{-1}b = g$. Thus, g is written and the product of two elements, a and b, in A.

Exercise 11: Suppose $d|n$. Then, since $3 \not| n$, $3 \not| d$. Thus, $3|(d-1)$ or $3|(d+1)$, so $d|(d^2-1)$, since $d^2 - 1 = (d+1)(d-1)$. Furthermore, since $2 \not| n$, $2 \not| d$. Thus, $d \equiv 1 \pmod 4$ or $d \equiv 3 \pmod 4$. In either case, $4|(d-1)$ or $(d+1)$, and 2 divides the other, so $8|(d^2-1)$, and thus $24|d^2-1$. Furthermore, since

$$d + \frac{n}{d} = \frac{d^2 - 1 + n + 1}{d},$$

$24|(d^2-1)v$, $24|(n+1)$, and $(24, d) = 1$,

$$24|d + \frac{n}{d}.$$

Since, if $n = k^2$ for some $k \in \mathbb{N}$, $n = 4k^2$ or $n = 4(k^2 + 4k) + 1$

$$\sum_{\{d:d|n\}} d = \sum_{\{d:d|n \text{ and } d<\sqrt{n}\}} d + \frac{n}{d},$$

which is a sum of multiples of 24 and consequently a multiples of 24.

Exercise 12: Suppose, for sake of contradiction, that, for some $n \in \mathbb{N}$ with $n \geq 2$, n divides $2^n - 1$; in particular, let n be the smallest such natural number. Clearly, n is odd, since, otherwise, it could not divide $2^n - 1$, which is necessarily odd. Since $\phi(n) < n$, $|\mathbb{Z}_n| = \phi(n)$, and the order of 2 in $\mathbb{N}$ is at most $|\mathbb{Z}_n|$, the order of 2 in $\mathbb{N}$ is some $k \in \mathbb{N}$ with $k \neq n$ and k divides n. Thus, $2^k \equiv 1 \pmod{n}$. However, since k divides n, $2^k \equiv 1 \pmod{k}$. Since $k \neq n$, this contradicts the choice of n as the smallest natural number with this divisibility property.

Exercise 14: (i) The elements of G which can be expressed in the form c^2, for some $c \in G$, are the 8 values in the set

$$\{e, a^2, b, b^2, b^3, b^4, b^5, b^6\}.$$