Shashank Singh
sss1@andrew.cmu.edu
21-373 Algebraic Structures, Fall 2011
Assignment 1
Due: Friday, September 16

Exercise 1:

Suppose G is a group such that, $\forall g \in G$, $g^2 = e$. Then, by definition of the inverse, $\forall g \in G$, $g = g^{-1}$. As shown in class (Remark 3.4), $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$, so that $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Thus, G is Abelian.

Exercise 2:

i. Suppose G is a group with $|G| = 2n$ for some $n \in \mathbb{N}$. Clearly, the only element in G of order less than 2 is e. $\forall g \in G$ of order greater than 2, two sets A and B can be constructed such that $A \cup B = G$, $A \cap B = \emptyset$, $g \in A$ if and only if $g^{-1} \in B$; that is, the elements of order greater than 2 can be "split" into two disjoint sets, such that the elements of each are the inverses of the elements of the other. Since inversion ($^{-1}$) gives a bijection between these two sets, $|A| = |B| = k$ for some $k \in \mathbb{N}$, so that the number of elements of order greater than 2 is $2k$. Thus, for some $k \in \mathbb{N}$, the number of elements of order 2 in G is given by $2n - (2k+1) = 2(n-k-1)+1$, which is odd, since $n-k-1 \in \mathbb{N}$.

ii. Let $n \in \mathbb{N}$ be odd, and let G be an Abelian group of order $2n = 2(2k+1) = 4k+2$, for some $k \in \mathbb{N}$. By the result of part i., G contains at least one element g with $g^2 = e$. Suppose, for sake of contradiction, that $\exists$ distinct $g_1, g_2 \in G$ with $g_1^2 = g_2^2 = e$. Then, since G is Abelian, it is clear that $\{e, g_1, g_2, g_1g_2\}$ is a subgroup of G (since all of its elements are of order 2), and that it has order 4. By Lagrange's Theorem, then, 4 divides the order of G. However, this is impossible, since 4 cannot divide $4k+2$.
Note that this is not necessarily the case if P is non-Abelian. Consider, for instance, the group of permutations on 3 elements, denoted P_3. P_3 is of order $3! = 6 = 2n$, where $n = 3$ is odd. However, the 3 transpositions in P_3 (denoted here by their cycle decomposition), (2 1)(3), (3 1)(2), and (3 2)(1), are all of order 2.

Exercise 3:

i. Let G be a group, and suppose, for sake of contradiction, that $\exists$ proper subgroups $A, B \subset G$ with $G = A \cup B$. Then, $\exists a \in A$ with $a \notin B$, and $\exists b \in B$ with $b \notin A$, since, if either were not the case, then $G = A \cup B = A$ or $G = A \cup B = B$, violating the supposition that A and B are *proper* subgroups. Since G is a group, $ab \in G$, so $ab \in A$ or $ab \in B$. If the former, then, since $a^{-1} \in A$, $b = eb = \left(a^{-1}a\right)b = a^{-1}(ab) \in A$, and, if the latter, then, since $b^{-1} \in B$, $a = ae = a\left(bb^{-1}\right) = (ab)b^{-1} \in B$. In either case, the existence of a and b as chosen above is contradicted, and so no such A and B can exist.

ii. Consider the group $G = \{e, a, b, c\}$, under the operation determined by the following table (with e as the identity element):

$\star$	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

Then, G is the union of the three groups $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, under the same operation.

Exercise 4:

Let S denote the set of infinite groups with a finite number of subgroups. Suppose, for sake of contradiction, that $S \neq \emptyset$. Let $\# : S \to \mathbb{N}$ such that, $\forall G \in S$, $\#(G)$ gives the number of subgroups of G.

The elements of S can be well-ordered by the number of subgroups each has; that is, $\exists G \in S$ such that, $\forall A \in S$, $\#(G) \leq \#(A)$. Then, if $A \subset G$ is a proper subgroup of G, A is finite, since, otherwise, $A \in S$ and $\#(A) < \#(G)$, contradicting the choice of G. Therefore, since G has a finite number of proper subgroups, all of which are finite, the union of the proper subgroups of G is finite, and, since G is infinite, $\exists g \in G$ such that g is not contained in any proper subgroup of G. However, since G is a group, $G_g = \{g^n | n \in \mathbb{Z}\}$ (the cyclic group of g) is a subgroup of G such that $g \in G_g$, contradicting the choice of g. Thus, $S = \emptyset$, so all infinite groups have an infinite number of subgroups; that is, in contrapositive, all groups with a finite number of subgroups are finite.

Exercise 5:

ii. This is not necessarily the case if P is non-Abelian. Consider, for instance, the group of permutations on 3 elements, denoted P_3. Denoting permutations by their cycle decomposition, (2 1)(3) is of order 2, and (1 2 3) is of order 3, but no element of P_3 is of order greater than 3, let alone $6 = \text{lcm}(2, 3)$.

Exercise 6:

i. Let G be an Abelian group, and let $H = \{g \in G | g^n = e$, for some $n \in \mathbb{N}\backslash\{0\} \subseteq G$. Letting e denote the identity on G, $e \in H$, since $e^1 = e$. Suppose $a, b \in H$, with $a^m = b^n = e$. Then, since G is Abelian, $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n (b^n)^m = e^n e^m = e$. Thus, H is closed under the operation on G. Suppose $g \in H$, with $g^k = e$. Then $\left(g^{-1}\right)^k = \left(g^k\right)^{-1} = e^{-1} = e$, so $g^{-1} \in H$. Thus, $H \leq G$.

ii. Calculating A^2, A^3, and A^4 shows that A is of order 4, and calculating B^2 and B^3 shows that B is of order 3. However, a simple proof by induction shows that, $\forall n \in \mathbb{N}$, $((AB)_{1,2})^n = n$ ($(AB)_{1,2}$ denotes the second element of the first row of AB). Thus, since the corresponding entry of the 2×2 identity matrix is 0, AB is of infinite order.

iii. Let $a = (1, 1), b = (0, -1)$. Then, $\forall n \in \mathbb{N}$, $na = (0, n) \neq (0, 0)$ or $na = (1, n) \neq (0, 0)$, and $nb = (0, -n) \neq (0, 0)$, so a and b are both of infinite order. However, $a + b = (1, 0) \neq (0, 0)$, so that $2(a + b) = (0, 0)$, the identity element of $\mathbb{Z}_2 \times \mathbb{Z}$.