WORKED SOLUTIONS TO MIDTERM #1

(1) Suppose that \( p_1, p_2, \ldots, p_n \) are primes. Prove that \( p_1 p_2 \cdots p_n + 1 \) is not divisible by any \( p_i \), for \( 1 \leq i \leq n \).

Deduce that there are infinitely many primes. (You may assume that 2 is a prime, if it helps).

**Solution:**

The Division Algorithm states that for any integers \( a, b \) with \( b > 1 \) there are unique integers \( q, r \) with \( 0 \leq r < b - 1 \) so that

\[
a = bq + r.
\]

Then \( a \) divides \( b \) if and only if the \( r \) in this expression is 0.

Now, for any of our primes \( p_i \), note that \( p_i > 1 \), so

\[
p_1 p_2 \cdots p_n + 1 = p_i (p_1 \cdots p_{i-1} p_{i+1} \cdots p_n) + 1
\]

is the expression from the Division algorithm, with

(a) \( a = p_1 \cdots p_n + 1 \);
(b) \( b = p_i \);
(c) \( q = p_1 \cdots p_{i-1} p_{i+1} \cdots p_n \); and
(d) \( r = 1 \).

Therefore, since \( r = 1 \), \( p_i \) does not divide \( p_1 \cdots p_n + 1 \).

Now, suppose that there are only finitely many primes. We are given that 2 is a prime, so there is at least one prime.

Let \( p_1, \ldots, p_n \) be the list of all the prime numbers (with \( n \geq 1 \) since there is at least one prime). We just saw that \( p_1 \cdots p_n + 1 \) is not divisible by any of the \( p_i \).

However, we know that \( p_1 \cdots p_n + 1 \) is either a prime or a product of primes. Let \( p \) be a prime dividing \( p_1 \cdots p_n + 1 \). Since we know \( p \) is not on our list of primes, we arrive at a contradiction. So there must be infinitely many primes.

(2) (a) Give examples of elements \( a, b \in D_3 \) so that \( a^{-1}ba = b^{-1} \).

(b) Let \( G \) be a group, and let \( x, y \in G \) be so that

\[
y \neq y^{-1}, \ \text{and} \quad x^{-1}yx = y^{-1}.
\]
(i) Show that \( x \neq e \).
(ii) Show also that \( x^3 \neq e \).

**Solution:**

(a) There are lots of possible solutions to this. Here are a few (the ones I listed in class);

1. \( b = e, \) and \( a \) any element of \( D_3 \);
2. \( a = b = q, \) for some reflection \( q; \)
3. \( a \) any reflection and \( b \) any rotation.

A simple calculation shows that any of these choices of \( a, b \) give us
\[
 a^{-1}ba = b^{-1}.
\]

(b)

(i) Suppose, in order to obtain a contradiction, that \( x = e \).

Then
\[
y^{-1} = x^{-1}yx
= e^{-1}y
= e^{-1}y
= ey
= y.
\]

However, we are told that \( y \neq y^{-1} \), so we arrive at our contradiction

(ii) Note that inverting both sides of the equation \( x^{-1}yx = y^{-1} \) we get
\[
x^{-1}y^{-1}x = y.
\]

Now, suppose in order to obtain a contradiction that \( x^3 = e \). Then
\[
y = e^{-1}ye
= (x^3)^{-1}yx^3
= x^{-1}x^{-1}(x^{-1}yx)xx
= x^{-1}(x^{-1}y^{-1}x)x
= x^{-1}yx
= y^{-1},
\]

which contradicts the fact that \( y \neq y^{-1} \). Therefore \( x^3 \neq e \).

(3) Let \( C_{20} \) be the cyclic group of order 20 consisting of equivalence classes of integers modulo 20.

(a) How many elements of order 5 are there in \( C_{20} \)? What are they?
(b) What are the possible orders of elements in $C_{20}$?
(c) Name an element in $C_{20}$ of order 20, other than [1].

(No proofs are required in question 3, just the answers are fine).

NOTE: Two versions of the midterm were given out, one with $C_{20}$ as above, and the other with $C_{30}$. The only other difference was that Part (a) asked how many elements of order 6 there are. The solutions for the $C_{30}$ version are the second set.

Solution (1):

(a) The elements of order 5 in $C_{20}$ are [4], [8], [12], [16], so there are 4 of them.
(b) The possible orders are 1, 2, 4, 5, 10, 20.
(c) The following elements are those of order 20 in $C_{20}$ (other than [1]): [3], [7], [9], [11], [13], [17], [19].

Solution (2):

(a) The elements of order 6 in $C_{30}$ are [5] and [25]. There are 2 of them.
(b) The possible orders are 1, 2, 3, 5, 6, 10, 15, 30.
(c) The following elements are those of order 30 in $C_{30}$ (other than [1]): [7], [11], [13], [17], [19], [23], [29].

(4) Let $G$ be a group and $H$ and $K$ subgroups of $G$.

(a) Prove that the intersection $H \cap K$ is a subgroup of $G$.
(b) Give an example of $G, H, K$ where the union $H \cup K$ is not a subgroup.
   (Again, just the answer is fine here, no proof required in part (b)).
   [Hint: For the example in Part (b), you had better not have $H \subseteq K$ or $K \subseteq H$.]

Solution:
Note that a set $A \subseteq G$ is a subgroup if and only if

(i) $e \in A$;
(ii) If $g \in A$ then $g^{-1} \in A$;
(iii) If $g, h \in A$ then $gh \in A$.

We check each of these conditions in turn for $H \cap K$, where $H$ and $K$ are subgroups of $G$.

(i) Since $e \in H$ and $e \in K$ we have $e \in H \cap K$.
(ii) Suppose that $g \in H \cap K$. Then $g^{-1} \in H$, since $H$ is a subgroup, and $g^{-1} \in K$, since $K$ is a subgroup. Therefore $g^{-1} \in H \cap K$. 
(iii) Suppose that \( g, h \in H \cap K \). Then \( gh \in H \), since \( H \) is a subgroup, and \( gh \in K \), since \( K \) is a subgroup. Therefore, \( gh \in H \cap K \).

Thus we have checked all three conditions, and \( H \cap K \) is a subgroup.

For the example, let \( G = C_6 \), the integers modulo 6. Let \( H = \langle [2] \rangle = \{[0], [2], [4]\} \), and \( K = \langle [3] \rangle = \{[0], [3]\} \).

Then \( H \cup K = \{[0], [2], [3], [4]\} \), which is not a subgroup. (No proof was required, but the reason why \( H \cup K \) is not a subgroup is that it fails the third condition. For example, \([2][3] = [2 + 3] = [5] \notin H \cup K\).)

REMARK (aside, that has not much to do with the midterm, and certainly wasn’t required):

In fact, it is not hard to see that in any group \( G \), if \( H \) and \( K \) are subgroups so that \( H \not\subseteq K \) and \( K \not\subseteq H \) then \( H \cup K \) cannot be a subgroup of \( G \).

Here is the proof:

Let \( h \) be an element of \( H \) which is not in \( K \) (there is such an element because \( H \not\subseteq K \)), and let \( k \) be an element of \( K \) which is not in \( H \) (there is such a \( k \) because \( K \not\subseteq H \)).

Now, \( h, k \in H \cup K \). However, I claim that \( hk \not\in H \cup K \), so \( H \cup K \) is not a subgroup of \( G \).

Suppose that \( hk \in H \). Then \( h^{-1} \in H \) since \( H \) is a subgroup (condition (ii) of the definition), and so \( k = h^{-1}(hk) \in H \), by condition (iii) of the definition. But we chose \( k \) so that \( k \notin H \). Therefore, \( hk \notin H \).

Now suppose that \( hk \in K \). By the same argument, we have \( k^{-1} \in K \) and \( h = (hk)k^{-1} \in K \), which contradicts our choice of \( h \).

Therefore \( hk \notin H \) and \( hk \notin K \), so \( hk \notin H \cup K \), as required.

FINAL COMMENT: I have included more details in these solutions than I expected you to in the midterm. I’m hoping to convey some understanding as well as correct solutions. Let me know if you’d like what I consider to be a minimal correct set of solutions.