Math 403, Jeffrey Adams

Test I, February 12, 2010 Open Book SOLUTIONS

1. (a) Compute the powers. For example $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16 = 5$, etc. Here goes:

$$
\begin{aligned}
2^k &: 2,4,8,5,10,9,7,3,6,1 : |2| = 10 \\
3^k &: 3,9,5,4,1 : |3| = 5 \\
4^k &: 4,5,9,3,1 : |4| = 5 \\
5^k &: 5,3,4,9,1 : |5| = 5 \\
6^k &: 6,3,7,9,10,5,8,4,2,1 : |6| = 10 \\
7^k &: 7,5,2,3,10,4,6,9,8,1 : |7| = 10 \\
8^k &: 8,9,6,4,10,3,2,5,7,1 : |8| = 10 \\
9^k &: 9,4,3,5,1 : |9| = 5 \\
10^2 &: 10^2 = 1 : |10| = 2
\end{aligned}
$$

So the orders are

x	1	2	3	7	4	5	6	7	8	9	10
order	1	10	5	5	5	5	10	10	10	5	2

There are lots of ways to shorten the computation. For example once you see $< 3 >= \{1,3,9,5,4\}$ since 5 is prime all of these elements also have order 5. Also once you see 2 has order 10, then 2^k also has order 10 for $(k, 10) = 1$, i.e. $k = 3, 7, 9$. This gives that

(b) G is cyclic if and only if it has a generator, i.e. an element of order 10. It does: 2, for example.

(c) Take an element of order 2. The only one is 10, so $H = \langle 1, 10\rangle$.

(d) Take an element of order 5, say 3. Then $K = \{1, 3, 9, 5, 4\}$.

(e) Take $x = 1$, and multiply it by the 5 elements of K, to get the elements of K. Then take $x = 10$, and multiply by the 5 elements of K, to get 5 more elements. These are distinct from the preceding ones (if $1 * a = 10 * b$ with $a, b \in H$, then $10 = ab^{-1}$, but 10 is not in H). These must be the other 5 elements of G.

More explicitly:

x	y	g=xy
1	1	1
1	3	3
1	9	9
1	5	5
1	4	4
10	1	10
10	3	30=8
10	9	90=2
10	5	50=6
10	4	40=7

Another proof. It is easy to see $\{xy|x \in H, y \in K\}$ is a group. It contains K, so has order ≥ 5. But it is strictly bigger than K, since it contains 10. So it has order > 5, but this must divide 10, so it has order 10.

2. The possible orders (by Lagrange) are $1, 2, 3, 4, 6, 8, 12$ and 24.

   Looking at a cube, it has rotations of order $1, 2, 3$ and 4. It does *not* have any rotations of order $8, 12$ or 24.

   How many rotations of order 2 does it have? There are 6 pairs of opposite edges, and a 180 degree rotation about these. This gives 3.

   There are 3 pairs of opposite faces, each giving a 180 degree rotation, for 3 more. This gives $6 + 3 = 9$ elements of order 2.

   There are 4 pairs of opposite vertices, each of which has 3 rotations. Two of these have order 3, the third is the identity. This gives $2 \times 4 = 8$ rotations of order 3.

   Each pair of opposite faces has two 90 degree rotations, clockwise and counter-clockwise. This gives $3^2 = 6$ elements of order 4.

   This gives:

order	number
1	1
2	9
3	8
4	6

   Don't like this? Use the fact that $G \simeq S_4$. Here are the types of elements of S_4: id, $(1, 2)$, $(1, 2, 3)$, $(1, 2)(3, 4)$, and $(1, 2, 3, 4)$. These have orders $1, 2, 3, 2$ and 4.

   Let's list them:

order	elements	number
$1:$	id	1
$2:$	$(1,2),(1,3),(1,4),(2,3),(2,4),(3,4),$ $(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)$	9
$3:$	$(1,2,3),(1,3,2),(1,2,4),(1,4,2),$ $(1,3,4),(1,4,3),(2,3,4),(2,4,3)$	8
$4:$	$(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),$ $(1,4,2,3),(1,4,3,2)$	6

Note: These are the *proper* symmetries, not including reflections. The symmetry group including reflections has order 48. A few of you were confused by this - I was generous in my grading; sorry for the confusion.

3. The key point is $f(ab)=(ab)^{-1}=b^{-1}a^{-1}$. On the other hand $f(a)f(b)=a^{-1}b^{-1}$. Suppose f is a homomorphism. So for $a,b\in G$:

$$f(ab)=f(a)f(b)\Leftrightarrow b^{-1}a^{-1}=a^{-1}b^{-1} \tag{1}$$

Now f is a homomorphism if and only if $f(ab)=f(a)f(b)$ for all a,b. Therefore this holds if and only if $b^{-1}a^{-1}=a^{-1}b^{-1}$ for all $a,b\in G$. This holds if and only if $ab=ba$ for all $a,b\in G$ i.e. if and only if G is abelian.

(Note: $a^{-1}b^{-1}=b^{-1}a^{-1}$ for all a,b if and only if $ab=ba$ for all a,b. This is clear: every element is the inverse of something, so if all inverses commute, then so do all elements.)

(Note: If G is not abelian then $ab\neq ba$ for *some* a,b. It is not the case the $ab\neq ba$ for *all* a,b, for example if $a=1$, or $a=b$).

Now assume G is abelian. To show f is an isomorphism, we have to show it is a homomorphism, and it is one-to-one and onto. We just showed it is a homomorphism. It is clearly one-to-one and onto, since for each element the inverse exists (this gives onto) and is unique (this gives one-to-one).

To be long winded about it: f is one-to-one, since $f(a)=f(b)$ implies $a^{-1}=b^{-1}$ implies $a=b$. It is onto: given a, $f(a^{-1})=(a^{-1})^{-1}=a$.

Alternatively, a homomorphism is an isomorphism if it has an inverse: $f \circ f^{-1} = id$, i.e. $f(f^{-1}(a)) = a$ for all a. Well, take $f^{-1} = f$. That is $f(f(a)) = (a^{-1})^{-1} = a$.

4. (a) We have to show $f(gh) = f(g)f(h)$, i.e. $\det(gh) = \det(g)\det(h)$ for all g, h. This is a basic property of the determinant which you can simply use. Or, write

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad h = \begin{pmatrix} x & y \\ x & w \end{pmatrix}$$

Then

$$gh = \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix}$$

Then

$$\begin{aligned} \det(gh) &= (ax + bz)(cy + dw) - (ay + bw)(cx + dz) \\ &= axcy + axdw + bzcy + bzdw - aycx - aydz - bwcx - bwdz \\ &= axdw + bycz - aydz - bwcx \qquad \text{the other terms cancel} \end{aligned}$$

while

$$\det(g)\det(h) = (ad - bc)(xw - yz) = adxw - adyz - bcxw + bcyz$$

(b) We have to show $gHg^{-1} = H$ for all $g \in G$. In fact it is enough to show $gHg^{-1} \subset H$, i.e. $\det(h) = 1$ implies $\det(ghg^{-1}) = 1$ for all g. But

$$\begin{aligned} \det(ghg^{-1}) &= \det(g)\det(h)\det(g^{-1}) \\ &= \det(g)\det(g^{-1})\det(h) \\ &= \det(gg^{-1})\det(h) \\ &= \det(I)\det(h) \\ &= \det(h) = 1. \end{aligned}$$