TEST I: SOLUTIONS
Math 403, J. Adams

Question 1.

(a) (15 points) The Euclidean algorithm: $99 = 57+42, 57 = 42+15, 42 = 2 \cdot 15 + 12, 15 = 12 + 3, 12 = 4 \cdot 3 + 0$, so $(99, 57) = 3$.

Unwinding this we get $3 = 15 - 12 = 15 - (42 - 2 \cdot 15) = 3 \cdot 15 - 42 = 3(57 - 42) - 42 = 3 \cdot 57 - 42 = 3 \cdot 57 - 4(99 - 57) = 7 \cdot 57 - 4 \cdot 99$. (b) (10 points) Since $(a, b) = 1$ we can write $ra + sb = 1$ for some r, s. Multiply both sides by m to get $mra + msb = m$, or $r(am) + s(bm) = m$. Now since $b|m$ then $ab|am$, and since $a|m$ we have $ab|bm$. Therefore ab divides both of the terms on the left hand side, and so also the right hand side, i.e. $ab|m$.
Question 2. (a) (10 points) The group U_{18} consists of the cosets of integers $1 \leq k \leq 18$ relatively prime to 18. This is $\{1, 5, 7, 11, 13, 17\}$. We compute the orders. Remember the order of an element divides the order of the group, i.e. 6. So the only possible orders are $1, 2, 3$ and 6.

Obviously the order of $\overline{1}$ is 1. Now $\overline{5}^2 = \overline{25} = \overline{7}$, $\overline{5}^3 = \overline{35} = \overline{17}$. Since the order of $\overline{5}$ is not $1, 2$ or 3 it must be 6. For the next part of the problem we need to know the other powers of $\overline{5}$ anyway, so we compute them. We have $\overline{5}^4 = \overline{85} = \overline{13}$, and $\overline{5}^5 = \overline{65} = \overline{11}$, and finally $\overline{5}^6 = \overline{55} = \overline{1}$, which we know has to be the case. Next $\overline{7}^2 = \overline{49} = \overline{13}$, and $\overline{7}^3 = \overline{91} = \overline{1}$, so the order of $\overline{7}$ is 3.

The rest of the computation proceeds similarly, for variety we give some alternate ways of computing. For example to compute the order of $\overline{11}$ note that $\overline{11} = \overline{-7}$, so $\overline{11}^2 = \overline{7^2} = \overline{13}$, and $\overline{11}^3 = -\overline{7}^3 = -1 = \overline{17}$, $\overline{11}^4 = \overline{7}^4 = \overline{7}$, and $\overline{11}^5 = -\overline{7}^5 = -\overline{13} = \overline{5}$, so $\overline{11}$ has order 6. For 13 note that $\overline{13} = \overline{5}^4$, so $\overline{13}^2 = \overline{5}^8 = \overline{5}^2 = \overline{7}$, and $\overline{13}3 = \overline{5}^{12} = (\overline{5}^6)^2 = \overline{1}$, so $\overline{13}$ has order 3. Finally $\overline{17} = -\overline{1}$, so $\overline{17}^2 = \overline{1}$ and $\overline{17}$ has order 2.

(b) (10 points) To find an isomorphism of U_{18} with the cyclic group $\mathbb{Z}/6\mathbb{Z}$ find a generator g of U_{18}, and then send g^k to $\overline{k}$ $(k = 1, 2, \ldots, 6)$. From part (a) there are two generators: $\overline{5}$ and $\overline{11}$. Choosing the first of these we see ϕ is an isomorphism with $\phi(\overline{5}) = \overline{1}, \phi(\overline{7}) = \overline{2}, \phi(\overline{11}) = \overline{5}, \phi(\overline{13}) = \overline{4}, \phi(\overline{17}) = \overline{3}$ and of course $\phi(\overline{1}) = \overline{0}$.

The choice of $\overline{11}$ as generator gives $\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}$ going to $\overline{0}, \overline{5}.\overline{4}, \overline{1}, \overline{2}, \overline{3}$ respectively. (c) (5 points) The group U_{11} consists of $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$, so is of order 4. All of these elements have order 2: $5^2 = 25, 7^2 = 49$ and $11^2 = 121$ are equivalent to 1 mod 12. But a cyclic group of order 4 must have an element of order 4, a contradiction.

Question 3. (a) (15 points) Suppose g', h' are elements of G'. We need to show $g'h' = h'g'$. Since ϕ is onto, there exist g, h in G with $\phi(g) = g', \phi(h) = h'$.Then

$$
\begin{aligned}
g'h' &= \phi(g)\phi(h) \\
&= \phi(gh) \quad (\phi \text{ is a homomorphism}), \\
&= \phi(hg) \quad (G \text{ abelian}), \\
&= \phi(h)\phi(g)(\phi \text{ a homomorphism again}), \\
&= h'g'.
\end{aligned} \tag{1}
$$

(b) (10 points) The converse is false. There are many examples where G' is abelian, but G is not. The simplest is to take G any non–abelian group, and $G' = \{e\}$ the trivial group, and the trivial homomorphism $\phi(g) = e$ for all g. Obviously G' is not abelian and the map is onto.

Another example is $G = S_3$ and $G' = G/H$ with H the normal subgroup of order 3 consisting of the identity and the two elements of order 3.Then G/H has order $6/3 = 2$ and is therefore the cyclic group of order 2, which is abelian. Question 4. (a) (10 points) Note that the set H_s depends on the element s as the notation indicates; it is the elements f with $f(s) = s$ for this s. To show it is a subgroup, suppose $f, g \in Hs$, i.e. $f(s) = g(s) = s$; we need to show $f \circ g \in H_s$. That is:

$$
\begin{aligned}
(f \circ g)(s) &= f(g(s)) \\
&= f(s) \quad \text{since } g(s) = s \\
&= s \quad \text{since } f(s) = s.
\end{aligned} \tag{2}
$$

This shows $f \circ g \in H_s$.

Similarly we need to show if $f \in H_s$ then $f^{-1} \in H_s$. That is suppose $f(s) = s$. Take f^{-1} of both sides of this: $f^{-1}(f(s)) = f^{-1}(s)$, i.e. $s = f^{-1}(s)$. (b) (15 points) Consider fH_sf^{-1}, i.e. the elements of the form $\psi = fgf^{-1}$ with $g \in H_s$. There is no reason for $\psi(s)$ to equal s: $\psi(s) = f(g(f^{-1}(s)))$, and there is no way to know what $f^{-1}(s)$ is. However we do know what $f^{-1}(t)$ is: $f(s) = t$ so $f^{-1}(t) = s$. Therefore $(fgf^{-1})(t) = f(g(f^{-1}(s))) = f(g(s)) = f(s) = t$. This says that $fgf^{-1} \in H_t$. That is, $fH_sf^{-1} = H_t$. Since H_s does not equal H_t if $s \neq t$, this says that H_s is not a normal subgroup of $A(S)$.