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 \(3 = 15 - 12 = 15 - (42 - 2 \cdot 15) = 3 \cdot (57 - 42) - 42 = 3 \cdot 57 - 4 \cdot 42 = 3 \cdot 57 - 4 \cdot (99 - 57) = 7 \cdot 57 - 4 \cdot 99\). (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 \(b \mid m\) then \(ab \mid am\), and since \(a \mid m\) we have \(ab \mid bm\). Therefore \(ab\) divides both of the terms on the left hand side, and so also the right hand side, i.e. \(ab \mid m\).

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 \(\bar{1}\) is 1. Now \(\bar{5}^2 = 25 = \bar{7}, \bar{5}^3 = 35 = \bar{17}\). Since the order of \(\bar{5}\) 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 \(\bar{5}\) anyway, so we compute them. We have \(\bar{5}^1 = 85 = \bar{13}\), and \(\bar{5}^6 = 65 = \bar{11}\), and finally \(\bar{5}^6 = 55 = \bar{1}\), which we know has to be the case. Next \(\bar{7}^2 = 49 = \bar{13}, \bar{7}^3 = \bar{1} = \bar{1}, \bar{5}^3 = 35 = \bar{17}\), so the order of \(\bar{7}\) 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 \(\bar{11}\) note that \(\bar{11} = -\bar{7}\), so \(\bar{11}^2 = \bar{7}^2 = \bar{13}\), and \(\bar{11}^3 = -\bar{7}^3 = -1 = \bar{17}, \bar{11}^4 = \bar{7}^4 = \bar{7}, \bar{11}^5 = -\bar{7}^5 = -\bar{13} = \bar{5}, \bar{11}\) has order 6. For 13 note that \(\bar{13} = \bar{5}^4\), so \(\bar{13}^2 = \bar{5}^8 = \bar{5}^2 = \bar{7}, \bar{13}^3 = \bar{5}^{12} = (\bar{5}^6)^2 = \bar{1}, \bar{13}\) has order 3. Finally \(\bar{17} = -\bar{1}, \bar{17}^2 = \bar{1}\), so \(\bar{1}^2\) 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 \(k\) \((k = 1, 2, \ldots, 6)\). From part (a) there are two generators: \(\bar{5}\) and \(\bar{11}\). Choosing the first of these we see \(\phi\) is an isomorphism with \(\phi(\bar{5}) = \bar{1}, \phi(\bar{7}) = \bar{2}, \phi(\bar{11}) = \bar{5}, \phi(\bar{13}) = \bar{1}, \phi(\bar{17}) = \bar{3}\) and of course \(\phi(\bar{1}) = \bar{0}\).

The choice of \(\bar{11}\) as generator gives \(\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}\) going to \(0, 5, 4, 1, 2, 3\) respectively. 

(c) (5 points) The group \(U_{11}\) consists of \(\{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}\), so is of order 4. All of these elements have order 2: \(\bar{5}^2 = 25, \bar{7}^2 = 49\) and \(\bar{11}^2 = 121\) 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 \( \phi \) is onto, there exist \( g, h \) in \( G \) with \( \phi(g) = g', \phi(h) = h' \). Then

\[
\begin{align*}
g'h' &= \phi(g)\phi(h) \\
&= \phi(gh) \quad (\phi \text{ is a homomorphism}), \\
&= \phi(hg) \quad (G \text{ abelian}), \\
&= \phi(h)\phi(g) \quad (\phi \text{ a homomorphism again}), \\
&= h'g'.
\end{align*}
\]

(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 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 \( f, g \in H_s \), i.e. \( f(s) = g(s) = s \); we need to show \( f \circ g \in H_s \). That is:

\[
\begin{align*}
(f \circ g)(s) &= f(g(s)) \\
&= f(s) \quad \text{since } g(s) = s \\
&= s \quad \text{since } f(s) = s.
\end{align*}
\]

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 \( \mathcal{A}(S) \).