Math 302: Abstract Algebra
Sample Exam 1 Solutions

1. To show that $[b] \subseteq [c]$, we must show that for every $x \in [b]$, it is true that $x \in [c]$. Thus, we must show that if $b \sim x$, then $c \sim x$.

   But since $a \in [c]$, we know that $c \sim a$.

   Furthermore, since $a \in [b]$, we know that $b \sim a$. Since $\sim$ is symmetric, this also means that $a \sim b$.

   Again, since $x \in [b]$, we know that $b \sim x$.

   Putting all this facts together gives

   $$c \sim a \sim b \sim x.$$

   By the transitivity of $\sim$, we conclude that $c \sim x$, as desired.

2. Suppose that $a = nq_a + r_a$ and $b = nq_b + r_b$, where $0 \leq r_a, r_b < n$. Note that by definition of the modulus function, $r_a = a \bmod n$ and $r_b = b \bmod n$.

   Without loss of generality, assume that $r_a \geq r_b$. Notice that $0 \leq r_a - r_b < n$.

   We then have

   $$\begin{aligned} a - b &= (nq_a + r_a) - (nq_b - r_b) \\ &= n(q_a - q_b) + (r_a - r_b). \end{aligned}$$

   Since n divides $a - b$, and since $0 \leq r_a - r_b < n$, we conclude that it must be the case that $r_a - r_b = 0$, i.e. $r_a = r_b$, i.e. $a \bmod n = b \bmod n$.

3. Although the identity of G lies in H and H is closed under the binary operation of G (why?), H is not a subgroup of G.

   For example, suppose that $A \in GL(2, \mathbb{R})$ is such that $\det A = 2$.

   We know that since $\det A \neq 0$, the inverse A^{-1} is an element of $GL(2, \mathbb{R})$.

   We also know, however, that $\det A^{-1} = \frac{1}{\det A} = \frac{1}{2}$. Since $\frac{1}{2}$ is not an integer, A^{-1} is not in H, so H is not closed under inverses.

   Thus H is not a subgroup of G.

4. (a) An element a in a group G has infinite order if there is no integer n such that $a^n = e$.

   (b) Suppose that $a \in G$ has order n. Let x be any other element in G.
   Then by one of our homework problems, for any integer m, $(xax^{-1})^m = xa^m x^{-1}$.
   But if $|a| = n$, then $a^n = e$ so

$$(xax^{-1})^n = xa^n x^{-1} = xex^{-1} = xx^{-1} = e.$$

   Thus, since $(xax^{-1})^n = e$, by one of our theorems, the order of xax^{-1} divides n.

5. Let g be any element in G.

   For the base case $n = 2$, we have $\varphi(g^2) = \varphi(gg) = \varphi(g)\varphi(g)$ by the given property of φ. So the base case holds.

   Now, suppose that the property holds for $n = k$, i.e. that $\varphi(g^k) = (\varphi(g))^k$.

   For the induction step, consider $\varphi(g^{k+1})$. Since $g^{k+1} = gg^k$, we have

$$\begin{aligned}
\varphi(g^{k+1}) &= \varphi(gg^k) \\
&= \varphi(g)\varphi(g^k) && \text{(by the given property of } \varphi) \\
&= \varphi(g)(\varphi(g))^k && \text{(by the induction hypothesis)} \\
&= (\varphi(g))^{k+1} && \text{(by properties of exponents).}
\end{aligned}$$

   Thus, we have proven the induction step that $\varphi(g^{k+1}) = (\varphi(g))^{k+1}$ so by induction, $\varphi(g^n) = (\varphi(g))^n$ for all integers $n \geq 2$.

6. (a) By the FTCG, G has exactly one subgroup for each divisor of 12. The divisors of 12 are $1, 2, 3, 4, 6, 12$, so G has 6 subgroups.

   (b) There is one subgroup of order 4 in G, namely $\langle a^3 \rangle = \{e, a^3, a^6, a^9\}$.
   Since there is only one subgroup of order 4 in G, the generators of this subgroup represent all the elements of order 4 in G. An element $(a^3)^k$ generates this subgroup if and only if $\gcd(4, k) = 1$, so the generators (i.e. the elements of order 4 in G) are a^3 and a^9.