HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 1

1.3, Q6. Consider any element $t \in T$. Since $f : S \to T$ is surjective, there exists $s \in S$ with $f(s) = t$. But $g \circ f = h \circ f$, so $g(f(s)) = h(f(s))$, which is to say that $g(t) = h(t)$. Since the latter holds for all $t \in T$, we conclude that $g = h$.

1.3, Q12. (a) No, the map $f : S \to T$ defined by $f(m/n) = 2^m 3^n$ does not define a legitimate function from S to T. The reason is that the set s does not distinguish between $1/2$ and $2/4$, and yet $2^1 3^2 \neq 2^2 3^4$.
(b) Define $f(m/n) = 2^{m_0} 3^{n_0}$, where $m_0 = m/(m,n)$ and $n_0 = n/(m,n)$. Then since $m/n = m_0/n_0$ for all non-negative integers m and n, we find that $f(m/n)$, defined in this way, is a legitimate function (it is well-defined).

1.3, Q16. If f is a bijective self-mapping of S, then for each $x \in S$ one has $(f \circ f^{-1})(x) = f(y)$, where $y = f^{-1}(x)$. But by the definition of an inverse mapping, we then have $f(y) = x$. Thus, for all $x \in S$ we have $(f \circ f^{-1})(x) = x$, and this implies that f acts as the inverse for f^{-1}. Thus $(f^{-1})^{-1} = f$.

1.3, Q23. Observe that if $2^{m_1} 3^{n_1} = 2^{m_2} 3^{n_2}$, for non-negative integers m_i, n_i, then $2^{m_2 - m_1} = 3^{n_1 - n_2}$. Here, without loss of generality, we may suppose that $m_2 \geq m_1$ and $n_1 \geq n_2$. Then by uniqueness of prime factorisations, we see that $m_1 = m_2$ and $n_1 = n_2$. Then these integers $2^m 3^n$, for each distinct ordered pair (m, n) of integers, are uniquely defined. We may therefore arrange these integers in ascending order, say $2^{m_1} 3^{n_1} < 2^{m_2} 3^{n_2} < \ldots$, and relabel these integers as $a_1 < a_2 < \ldots$. We may now write $S = \{a_1, a_2, \ldots\}$. Define the mapping $\varphi : S \to T$ by putting $\varphi(a_n) = n$. Then φ defines a map from S into $\mathbb{N}$ that is self-evidently surjective, since $n = \varphi(a_n)$. Moreover, we have $\varphi(a_n) = \varphi(a_m)$ if and only if $n = m$, and this relation holds if and only if $a_n = a_m$. Hence φ is also injective. Thus φ is a bijection, and so S and T are in bijective correspondence.

1.3, Q30. Write $f^{(k)}$ for the k-fold iteration of f. Since S is finite, say with cardinality m, it follows that given any $a \in S$, one must have a repetition in the values of $f^{(j)}(a)$ among the $m+1$ superscripts $j = 0, 1, 2, \ldots, m$. That is, the $m+1$ elements $f^{(0)}(a), f^{(1)}(a), \ldots, f^{(m)}(a)$ cannot all be distinct. Thus, for some integers k and l with $0 \leq l < l + k \leq m$, one has $f^{(l)}(a) = f^{(l+k)}(a)$. Let l be the smallest non-negative integer for which a relation of the latter type holds. Since we may suppose that the map f is injective, if one were to have $l \geq 1$, we would have also $f^{(l-1)}(a) = f^{(l+k-1)}(a)$, contradicting the minimality of l. Hence $l = 0$, and for some positive integer k with $k \leq m$, we have $f^{(k)}(a) = f^{(0)}(a) = a$. At this point, we have shown that for each $a \in S$, there is an integer $k = k(a)$, with $0 < k \leq m$, having the property that $f^{(k)}$ acts as the identity on the element a. To obtain an integer n for which $f^{(n)}$ acts uniformly as the identity *for every* $a \in S$, just take n to be the least common multiple of all the $k(a)$ for $a \in S$, or even a multiple of this integer. Since S is finite, such an integer exists. Indeed, one can take $n = m!$, for then (since $k(a) \leq m$) one has $k(a) | n$ for each $a \in S$, say $n = r(a)k(a)$. Hence, writing $g_a = f^{(k(a))}$, we have $g_a(a) = a$ and hence

$$f^{(n)}(a) = g_a^{r(a)}(a) = g_a^{(r(a)-1)}(a) = g_a^{(r(a)-2)}(a) = \ldots = g_a(a) = a.$$

Since this relation holds for all $a \in S$, we have $f^{(n)}(a) = a$ for all $a \in S$, as required.

1.4, Q4. When $f, g, h \in A(S)$, the associative property of mapping composition implies that

$$(f^{-1}gf)(f^{-1}hf) = (f^{-1}g)(ff^{-1})(hf) = (f^{-1}g)(\mathrm{id}_S(hf)) = (f^{-1}g)(hf) = f^{-1}(gh)f.$$

One can apply induction to prove that $(f^{-1}gf)^n = f^{-1}g^nf$. To see this, note that the desired conclusion holds for $n = 1$. If we assume that the conclusion holds for all $n < m$ for some $m \geq 2$, then we find that

$$(f^{-1}gf)^m = (f^{-1}gf)^{m-1}(f^{-1}gf) = (f^{-1}g^{m-1}f)(f^{-1}gf),$$

and the first result of this question then shows that

$$(f^{-1}gf)^m = f^{-1}(g^{m-1}g)f = f^{-1}g^mf,$$

confirming the inductive step. The desired conclusion therefore follows.

1.4, Q16. (a) Let $S_f \subset S$ be the set of elements $s \in S$ for which $f(s) \neq s$. Likewise, let $S_g \subset S$ be the set of elements $s \in S$ for which $g(s) \neq s$. We may suppose that both S_f and S_g are finite. One has $g(s) \neq s$ precisely when $s \in S_g$. When $s \notin S_g$, therefore, one has $g(s) = s$, and hence $(fg)(s) = f(g(s)) = f(s)$. But $f(s) \neq s$ precisely when $s \in S_f$. It follows that $(fg)(s) = s$ except, possibly, when $s \in S_g \cup S_f$. Since both S_f and S_g are finite, their union is also finite, and hence $(fg)(s) \neq s$ for at most a finite number of $s \in S$, which shows that $fg \in M$.
(b) If $f \in M$, then $f(s) = s$ for all $s \in S \setminus S_f$. Since $f \in A(S)$, we have $f^{-1} \in A(S)$, and so $f^{-1}(f(s)) = f^{-1}(s)$ for all $s \in S \setminus S_f$. Thus $f^{-1}(s) = s$ except when $s \in S_f$, which shows that $f^{-1}(s) \neq s$ for at most a finite number of $s \in S$, namely for $s \in S_f$. Hence $f^{-1} \in M$.

1.4, Q23. The simplest argument is probably to think of an element σ of S_n in cycle form, where we apply the permutation on the left hand side, say $\sigma = \tau_1\tau_2 \dots \tau_r$, where each τ_i has the shape $(a_1, a_2, \dots, a_{m_i})$, with the elements a_j of each τ_i distinct and disjoint from one another (as one considers distinct τ_i). Now consider a particular one of these cycles, say $\tau = (a_1, a_2, \dots, a_m)$. Remember that this cycle maps a_1 to a_2, and a_2 to a_3, and so on, and a_m to a_1, but leaves the elements besides $a_1 \dots, a_m$ fixed. This may be rewritten in the shape

$$(a_1, a_2, \dots, a_m) = (a_1, a_m)(a_1, a_{m-1}) \dots (a_1, a_3)(a_1, a_2).$$

Here, each term (a_1, a_j) is a transposition. Remember that we are applying this mapping on the left, so a_1 is mapped to a_2 and then left alone. Then a_2 is mapped to a_1, which is then mapped to a_3 and then left alone. And so on. Finally, we see that a_m is mapped to a_1, and that all elements besides $a_1, \dots a_m$ are left alone. Thus τ is a product of transpositions, and hence also so is σ.

1.4, Q27. Suppose that $O(s) \cap O(t)$ is non-empty, say with $c = f^j(s) = f^k(t)$. Then by the injectivity of f, we find that $s = f^0(s) = f^{k-j}(t)$, so that $f^n(s) = f^{n+k-j}(t) \in O(t)$ for all $n \in \mathbb{Z}$. Hence $O(s) \subseteq O(t)$. But similarly, we have $t = f^{j-k}(s)$, and it follows that $O(t) \subseteq O(s)$. We therefore deduce that whenever $O(s) \cap O(t) \neq \emptyset$, then $O(s) = O(t)$, as required.

1.5, Q10. If n is prime, then it is divisible by no integer m with $1 < m < n$, and hence it is divisible by no prime p with $p \leq \sqrt{n}$. Suppose on the other hand that n is not prime, and by way of seeking a contradiction, suppose that n is not divisible by any prime p with $p \leq \sqrt{n}$. Then n must be divisible by some integer m with $1 < m < n$ all of whose prime divisors exceed $\sqrt{n}$, so in particular $\sqrt{n} < m < n$. But if $m|n$ then $d = n/m$ divides n, and $1 < d < \sqrt{n}$. But d is a product of primes, so is divisible by a prime

p no larger than d, and hence smaller than $\sqrt{n}$. But since $p|d$ and $d|n$, we have $p|n$, contradicting our assumption that n is not divisible by any prime p with $p \leq \sqrt{n}$. Then we are forced to conclude that whenever n is not divisible by any prime p with $p \leq \sqrt{n}$, it is necessarily prime.

1.5, Q14. (a) Suppose that there are only finitely many primes of the form $4n+3$, and let these primes be $p_1, \ldots, p_m$. Plainly, there is no loss of generality in supposing that 3 is one of these primes. Consider the integer $P = 4p_1p_2\cdots p_m - 1$. We have $(P, 2p_i) = (4p_1\cdots p_m - 1, 2p_i) = (-1, 2p_i) = 1$ for each i, and hence P is neither divisible by 2 nor any prime of the form $4n+3$. But then P must be divisible only by primes of the form $4n+1$, say $P = (4l_1+1)(4l_2+1)\cdots(4l_k+1)$. Thus $P-1$ is divisible by 4, which is not the case. We therefore contradict our original assumption that there are only finitely many primes of the form $4n+3$, and must conclude that there are in fact infinitely many such.
(b) Suppose that there are only finitely many primes of the form $6n+5$, and let these primes be $p_1, \ldots, p_m$. Plainly, there is no loss of generality in supposing that 5 is one of these primes. Consider the integer $P = 6p_1p_2\cdots p_m - 1$. We have $(P, 6p_i) = (6p_1\cdots p_m - 1, 6p_i) = (-1, 6p_i) = 1$ for each i, and hence P is not divisible by 2, 3 nor any prime of the form $6n+5$. But then P must be divisible only by primes of the form $6n+1$, say $P = (6l_1+1)(6l_2+1)\cdots(6l_k+1)$. Thus $P-1$ is divisible by 6, which is not the case. We therefore contradict our original assumption that there are only finitely many primes of the form $6n+5$, and must conclude that there are in fact infinitely many such.

1.6, Q3. When $n = 2$, there is only one way to choose a subset of two elements, namely as the whole set, and so the claimed result is true for $n = 2$. Suppose then that $n > 2$, and that the claimed assertion has been confirmed for all sets having m elements, where $2 \leq m < n$. Consider a set having n elements, say $\{a_1, \ldots, a_n\}$. A subset of two elements either contains a_n, or it does not. If it does contain a_n, then the second element in the set can be any of $a_1, \ldots, a_{n-1}$, so there are $n-1$ choices here. If the subset does not contain a_n, then it is a subset of the $n-1$ element set $\{a_1, \ldots, a_{n-1}\}$. The inductive hypothesis shows that there are $\frac{1}{2}(n-1)(n-2)$ subsets of this type. Thus the total number of two element subsets is $(n-1) + \frac{1}{2}(n-1)(n-2) = \frac{1}{2}n(n-1)$. This confirms the inductive hypothesis for n-element sets, and hence the desired conclusion holds for all $n \geq 2$.

1.6, Q7. When $n = 0$ and $a \neq 1$, one has $1 + a + a^2 + \ldots + a^n = 1 = (a-1)/(a-1)$. Thus the inductive hypothesis holds for $n = 0$. Suppose then that $n \geq 1$, and that for all non-negative integers m with $m < n$, one has that $1 + a + a^2 + \ldots + a^m = (a^{m+1} - 1)/(a-1)$ whenever $a \neq 0$. From the inductive hypothesis for $m = n-1$, we have

$$1 + a + a^2 + \ldots + a^n = 1 + a(1 + a + \ldots + a^{n-1}) = 1 + a\Big(\frac{a^n - 1}{a-1}\Big)$$
$$= \frac{a - 1 + a(a^n - 1)}{a-1} = \frac{a^{n+1} - 1}{a-1}.$$

This confirms the inductive hypothesis when $m = n$, and hence the desired conclusion holds for all $n \geq 0$.

1.6, Q12. A set having 0 elements has precisely 1 subset, namely the empty set, so the claimed statement holds when $n = 0$. Suppose then that $n \geq 1$, and that it has been shown that whenever $0 \leq m < n$, any set of m elements has precisely 2^m subsets. Consider a

set having n elements, say $S = \{a_1, \ldots, a_n\}$. Any subset T of S either contains a_n, or it does not. If it does not, then it is a subset of the $n-1$ element set $\{a_1, \ldots, a_{n-1}\}$, and by the inductive hypothesis there are 2^{n-1} such subsets. If this subset T does contain a_n, then $T \setminus \{a_n\}$ is a subset of the same $n-1$ element set, and so again there are 2^{n-1} possible choices for T in this case. Thus the total number of subsets is $2^{n-1} + 2^{n-1} = 2^n$, which confirms the inductive hypothesis when $m = n$. Hence the desired conclusion holds for all $n \geq 0$.

1.6, Q15. A set having just 1 element has precisely $1 = 1!$ bijective self-mapping, so that the claim holds when $n = 1$. Suppose then that $n \geq 2$, and that it has been shown that whenever $1 \leq m < n$, any set having m elements has $m!$ bijective self-mappings. By relabelling set elements, it suffices to consider the set $S = \{1, 2, \ldots, n\}$. A bijective self-mapping f of S maps n to an element $b \in S$, and so there are n possible choices for $f(n)$. Now write $T := S \setminus \{b\}$ as $\{a_1, \ldots, a_{n-1}\}$. Since f is a bijective self-mapping, the map $g : \{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n-1\}$ defined via the relation $f(m) = a_{g(m)}$ must be a bijective self-mapping. Since T has $n-1$ elements, the inductive hypothesis tells us that there are $(n-1)!$ such mappings, and so the number of choices for f is n times $(n-1)!$, which is to say $n!$. Thus the total number of bijective self-mappings of S is $n!$, which confirms the inductive hypothesis when $m = n$. Hence the desired conclusion holds for all $n \geq 1$.