Basic Algebra
Solutions to Assignment 1

Let S and T be the sets $\{a, b, c\}$ and $\{x, y\}$ respectively.

Question 1 Saying how many functions there are from S to T amounts to counting how many ways we can "send" the elements of S into T. So we have that if $f : S \to T$ then:

$$\begin{array}{rcl} f(a) & = & \text{two choices i.e. } x \text{ or } y \\ f(b) & = & \text{two choices} \\ f(c) & = & \text{two choices} \end{array}$$

which means that there are 8 possible functions from S to T.

Question 2 We try "build" injective functions. Let $f : S \to T$, then $f(a) =$ either x or y. So let's suppose that $f(a) = x$ then because f is injective $f(b) \neq f(a)$ so we must have $f(b) = y$. Now $f(c)$ is either x or y, both choices yield a non injective function. Similarly if $f(a) = y$ we find that it is also impossible to build an injective function. Having exhausted all the possibilities we have that there are no injective functions from S to T.

Question 3 Here it's easier to count how many functions are not surjective. Suppose $f : S \to T$. Then if $f(a) = x$ then both $f(b)$ and $f(c)$ must be also be x, otherwise we have that f is surjective. Similarly if $f(a) = y$, $f(b) = f(c) = y$. There being no other choices, we have that there are only two non-surjective functions from S to T, which means all the other ones must be surjective. So there are $8 - 2 = 6$ surjective functions from S to T.

Question 4 Let f, g and h be function from X to X. **Claim:** $f(gh) = (fg)h$. (By the way, in calculus some may have seen the composition of f and g denoted by $f \circ g$. In that notation $f(gh) = f \circ (g \circ h)$).
proof of claim: We fix an arbitrary $x \in X$, we compute $f(gh)(x)$. First, we find $gh(x)$. Let $h(x) = y$ and $g(y) = z$, then $gh(x) = z$. Now let $f(z) = w$, since $gh(x) = z$ and $f(z) = w$ we get that the composition $f(gh)(x) = w$.

Now we compute $(fg)h(x)$. We already have that $h(x) = y$. To find $fg(y)$, we use $g(y) = z$, $f(z) = w$ from the previous part to get $fg(y) = w$. It follows that the composition $(fg)h(x) = w = f(gh)(x)$.

Since $x \in X$ is arbitrary, we infer that for each $x \in X$ $f(gh)(x) = (fg)h(x)$, which means that $f(gh)$ and $(fg)h$ are equal as functions from X to X.$\Box$

Question 5 Let f and g be functions from $\mathbb{N}$ to $\mathbb{N}$ given by the rules:

$$f(n) = \begin{cases} 43 & \text{if } n > 20 \\ 1 & \text{otherwise} \end{cases} \quad ; \quad g(n) = n + 10$$

These are clearly well defined (but silly) functions. Now for $n = 11$, we compute $gf(11) = g(1) = 11$ and $fg(11) = f(21) = 43$. For $n = 11, gf(n) \neq fg(n)$, so $fg \neq gf$.

Question 6 The binomial theorem states that for all a, b in a commutative ring (e.g $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$) and n, a positive integer we have the identity:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Letting $a = 1, b = 1$ we get $(1+1)^n = 2^n = \sum_{k=0}^{n} \binom{n}{k} * 1^k * 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}$. Similarly setting $a = -1, b = 1$ gives you the other equality.

Question 7 Compute the gcd of 910091 and 3619 using the Euclidian algorithm.

$$\begin{array}{lcll} 910091 & = & 251 * 3619 & +1722 \\ 3619 & = & 2 * 1722 & +175 \\ 1722 & = & 9 * 175 & +147 \\ 175 & = & 1 * 147 & +28 \\ 147 & = & 5 * 28 & +7 \\ 28 & = & 4 * \boxed{7} & +0 \leftarrow \text{zero!} \end{array}$$

So gcd(910091, 3619) $= 7$

Question 8 (i) Using induction (or otherwise) show that 7 divides $8^n - 1$ for all $n \geq 0$.
We give two different proofs.
(Proof by induction) We first verify the statement for $n = 0$:

$$8^0 - 1 = 1 - 1 = 0 = 0 \times 7. \quad \surd$$

We now suppose that $7 \mid 8^n - 1$. It follows from this that $7 \mid 8(8^n - 1)$, and since obviously $7 \mid 7$, we conclude that

$$7 \mid 8(8^n - 1) + 7 = 8^{n+1} - 1,$$

and we are done.

One can also apply the identity

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1})$$

to get the result at one stroke by replacing a with 8 and b with 1:

$$8^n - 1 = 8^n - 1^n = (8-1)(8^{n-1} + \cdots + 1^{n-1}).$$

(ii) Use induction to show that 49 divides $8^n - 7n - 1$ for all $n \geq 0$.
Once again we first verify the statement for $n = 0$:

$$8^0 - 7 \times 0 - 1 = 1 - 1 = 0 = 0 \times 49. \quad \surd$$

Now we assume that the statement to be proved is true for $n \geq 0$ and then prove it for $n + 1$. Quite akin to what we did in previous case, it is enough to notice that

$$8^{n+1} - 7(n+1) - 1 = 8(8^n - 7n - 1) + 49n.$$

Question 9 We must show that for all a, b, n that $a + (b + n) = (a + b) + n$. The proof is by induction on n.

For $n = 0$ we have that $a + (b + 0) = a + b$ and $(a + b) + 0 = a + b$ by the fact that $x + 0 = x$ for all x.

Now suppose that this was true for all $m \leq n$, then for $S(n)$ we have:

$$\begin{aligned}
(a+b)+S(n) &= S((a+b)+n) && \text{(by definition of +)} \\
&= S(a+(b+n)) && \text{(by induction hypothesis)} \\
&= a+S(b+n) && \text{(by definition of +)} \\
&= a+(b+S(n)) && \text{(by definition of +)}
\end{aligned}$$

So associativity also holds for S(n). Thus, by induction, associativity holds for all n.

Question 10 Show that the expression $1^k + \ldots + n^k$ can be written as a polynomial in n of degree at most $k + 1$.

We start by proving this **proposition**: If $F : \mathbb{N} \to \mathbb{N}$ is a function such that $F(n + 1) - F(n)$ is a polynomial of degree k then F itself is a polynomial of degree $k + 1$.

Proof of proposition: This is done by induction on k. If $k = 0$ then we have that $F(n + 1) - F(n) = b$ a constant. Suppose $F(0) = a$ then we have that $F(n) = bn + a$ (check this, it's a straightforward inductive proof.) So the claim is true for $k = 0$

Now suppose that this was not true in general, let $k > 0$ be the smallest positive integer such that there exist $F : \mathbb{N} \to \mathbb{N}$ such that $F(n + 1) - F(n)$ is a polynomial of degree k but $F(n)$ is not itself a polynomial of degree $k + 1$. Let $f(n) = a_k n^k + a_{k-1}n^{k-1} + \ldots a_0 = F(n + 1) - F(n)$. Let $b = \frac{a_k}{k+1}$ and let $G(n) = F(n) + bn^{k+1}$. Consider $g(n) = G(n + 1) - G(n) = F(n + 1) - F(n) - b(n + 1)^{k+1} + bn^{k+1}$ with the binomial theorem this expands to:

$$g(n) = \underbrace{a_k n^k + \ldots + a_0}_{=F(n+1)-F(n)} - b\Big(\sum_{i=0}^{k+1} \tbinom{k+1}{i} n^i\Big) + bn^{k+1}$$

We see that the coefficient for n^{k+1} in $g(n)$ is zero. For n^k we have that the coefficient in $g(n)$ is $a_k - b * \binom{k+1}{k}$ and we have that $\binom{k+1}{k} = k + 1$ and since $b = \frac{a_k}{k+1}$, the coefficient for n^k is also zero. So $G(n + 1) - G(n)$ is a polynomial of degree j for some $j < k$, since k was chosen to be minimal we have that $G(n)$ is a polynomial of degree $j + 1$. But we have that $F(n) = G(n) + bn^{k+1}$ is a sum of polynomials so therefore itself a polynomial, moreover it is of degree $k + 1$, which is a contradiction. So the proposition is true. $\square$

It now suffices to notice that if we set $F(n) = 1^k + \ldots n^k$ then we have that F is a function such that $F(n + 1) - F(n) = (n + 1)^k$ which, by the binomial theorem, is a polynomial of degree k (notice that the coefficients are independent of n). So we may apply our proposition and it follows that $F(n)$ is a polynomial of degree $k + 1$.

As for the "at most" part suppose that $F(n) = 1^k + \ldots + n^k = a_{k+1}n^{k+1} + \ldots a_0 = b_m n^m + \ldots b_0$ with $m > k+1$ and $b_m \neq 0$. Then we have:

$$\begin{array}{rl} & a_{k+1}n^{k+1} + \ldots + a_0 = b_m n^m + b_{m-1}n^{m-1} + \ldots + b_0 \\ \iff & b_m n^m + \ldots + (b_{k+1} - a_{k+1})n^{k+1} + \ldots + (b_0 - a_0) = 0 \\ \text{(dividing through by } n^m\text{)} & b_m + \ldots + \frac{(b_0 - a_0)}{n^m} = 0 \quad (\star) \end{array}$$

for all n. Picking n' sufficiently large, will yield a contradiction. You can also take the limit of $(\star)$ as $n \to \infty$. The left hand side tends to b_m.