1. (18 marks)

(a) Prove that if x is an odd integer then x^2 is an odd integer.

soln: x odd means $x = 2m + 1$ for some $m \in \mathbb{Z}$.
So $x^2 = 2m(2m + 1) + 2m + 1 = 2(m(2m + 1) + m) + 1$.
Since $m(2m + 1) + m$ is an integer
this shows x^2 is odd.

(b) Consider the statement:

if x is an even integer then x^2 is an even integer.

Write down the statement converse to this statement and then prove this converse statement is true.

soln: Converse is:

if x^2 is an even integer then x is an even integer.

Proof: (Setting the universe of discourse to be the integers) this statement is equivalent to the contrapositive statement:

x is a non-even integer then x^2 is an non-even integer.

That is we should show that if x is an odd integer then x^2 is an odd integer. This was done above.

(c) If A, B are sets then prove that

$$B \setminus (B \setminus A) = A \cap B.$$

soln: We prove $a \in B \setminus (B \setminus A) \;\Leftrightarrow\; a \in A \cap B$.
$\Rightarrow$: Suppose $a \in B \setminus (B \setminus A)$. Then $a \in B$ and $a \notin B \setminus A$
Now $B \setminus A = \{b \in B \;:\; b \notin A\}$. So it must be that $a \in A$. Since a is in both B and A we have $a \in A \cap B$.
$\Leftarrow$ Suppose that $a \in A \cap B$ then $a \in A$ and $a \in B$ and so $a \notin B \setminus A$. So we have $a \in B$ and $a \notin B \setminus A$. This means $a \in B \setminus (B \setminus A)$.

2. (18 marks) Let A be a non-empty set and let B be a fixed subset of A. Define a relation $\sim$ on $\mathcal{P}(A)$ by

For $C, D \in \mathcal{P}(A) \quad C \sim D$ if and only if $C \cap B = D \cap B$.

(a) Show that $\sim$ is an equivalence relation on $\mathcal{P}(A)$.

soln:
Reflexive since: for all $C \in \mathcal{P}(A)$, $C \cap B = C \cap B$ (set equality is reflexive!) so $C \sim C$.

Symmetric since: for all $C, D \in \mathcal{P}(A)$, $C \cap B = D \cap B \;\Leftarrow\; D \cap B = C \cap B$ (set equality is symmetric) so $C \sim D \;\Leftarrow\; D \sim C$.

Transitive since: for all $C, D, E \in \mathcal{P}(A)$, since $C \sim D$ and $D \sim E$ means $C \cap B = D \cap B = E \cap B$ and so $C \cap B = E \cap B$ (set equality is transitive), that is $C \sim E$.

(b) For the particular case where $A = \{1, 2, 3, 4, 5\}$, and $B = \{1, 2, 5\}$, find the equivalence class of $C = \{2, 4, 5\}$, under $\sim$.

soln: $[C] = \{\{2, 4, 5\}, \{2, 5\}, \{2, 3, 5\}, \{2, 3, 4, 5\}\}$.

3. (16 marks) Give a carefully presented proof by induction that for all $n \in \mathbb{N}$, 3 divides $2^{2n} - 1$.

soln: For $n \in \mathbb{N}$ let $P(n)$ be the statement that 3 divides $2^{2n} - 1$.

$P(1)$ is true: $2^2 - 1 = 4 - 1 = 3 = 3 \cdot 1$.

Suppose $P(k)$ is true. Then $2^{2k} - 1 = 3\ell$ for some $\ell \in \mathbb{Z}$. Consider $2^{2(k+1)} - 1$.
$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^2 \cdot 2^{2k} - 1 = 4 \cdot 2^{2k} - 1 = 4(2^{2k} - 2) + 4 - 1 = 4 \cdot 3\ell + 3 = 3 \cdot (4\ell + 1)$.
Since $4\ell + 1 \in \mathbb{Z}$ this shows that $3 \mid 2^{2(k+1)} - 1$. That is $P(k)$ imples $P(k + 1)$.

Thus by the priciple of induction we can conclude that $\forall \; \in \mathbb{N}$ $P(n)$ is true.

4. (20 marks)

(a) Show the equation $\overline{7} = \overline{6} \cdot_{12} \overline{x}$ has no solutions in $\mathbb{Z}_{12}$.

soln: If there is a solution $\overline{x} \in \mathbb{Z}_{12}$ to $\overline{7} = \overline{6} \cdot_{12} \overline{x}$ then there are integers x, k such that $7 = 6x + 12k$. This is clearly impossible since since if $x, k \in \mathbb{Z}$ then $6 \mid (6x + 12k)$ but 6 does not divide (the prime number) 7.

(b) Let $a, b, n \in \mathbb{N}$. Suppose there exists an integer c such that $ac \equiv 1 \pmod{n}$. Show that the equation $\overline{a} \cdot_n \overline{x} = \overline{b}$ has a unique solution $\overline{x} \in \mathbb{Z}_n$.

soln: If $ac \equiv 1 \pmod{n}$ then $\overline{a} \cdot_n \overline{c} = \overline{c} \cdot_n \overline{a} = \overline{1}$. Given this $\overline{x} = \overline{c} \cdot_n \overline{b}$ is a solution since
$\overline{a} \cdot_n (\overline{c} \cdot_n \overline{b}) = (\overline{a} \cdot_n \overline{c}) \cdot_n \overline{b} = \overline{1} \cdot_n \overline{b} = \overline{1 \cdot b} = \overline{b}$. On the other hand if $\overline{x} \in \mathbb{Z}_n$ is a solution to $\overline{a} \cdot_n \overline{x} = \overline{b}$, then
$\overline{c} \cdot_n (\overline{a} \cdot_n \overline{x}) = \overline{c} \cdot_n \overline{b}$
$\Leftrightarrow (\overline{c} \cdot_n \overline{a}) \cdot_n \overline{x} = \overline{c} \cdot_n \overline{b}$
$\Leftrightarrow \overline{1} \cdot_n \overline{x} = \overline{c} \cdot_n \overline{b}$
$\Leftrightarrow \overline{x} = \overline{1 \cdot x} = \overline{c} \cdot_n \overline{b}$. So the solution is unique.

5. (8 marks) Let G, H and J be groups, and let $f : G \to H$ and $g : H \to J$ be homomorphisms. Show that $g \circ f$ is a homomorphism.

soln: Let x and y in G be given. then

$$\begin{aligned} g \circ f(xy) &= g(f(xy)) \quad \text{(def of composite)} \\ &= g(f(x)f(y)) \quad \text{(f a hom)} \\ &= g(f(x))g(f(y)) \quad \text{(g a hom)} \\ &= g \circ f(x) g \circ f(y), \quad \text{(def of composite)} \end{aligned}$$

proving $g \circ f$ is a homomorphism.

6. (10 marks) Let G be a group, and let H and K be subgroups. Show that their intersection, $H \cap K$, is a subgroup.

soln: Since it contains the identity, e say, it is nonempty. Suppose $x \in H \cap K$ and $y \in H \cap K$ are given. Then $x^{-1}y \in H$ and $x^{-1}y \in K$ since H and K are subgroups. Then $x^{-1}y \in H \cap K$, and therefore $H \cap K$ is a subgroup.

7. (14 marks) Let G be a group with identity e_G. Let H be a group with identity e_H. Let $f : G \to H$ be a homomorphism. Prove that if $\{x \in G : f(x) = e_H\} = \{e_G\}$, then f is one to one, adding words to this calculation.

$$f(x) = f(y). \quad f(x^{-1}y) = f(x^{-1})f(y) = f(x)^{-1}f(y) = f(y)^{-1}f(y) = e_H. \quad x^{-1}y = e_G. \quad x = y$$

Prove the converse.

soln: Suppose $x \in G$ and $y \in G$ are given, and $f(x) = f(y)$. Then

$$\begin{aligned} f(x^{-1}y) &= f(x^{-1})f(y) \quad \text{f a hom} \\ &= f(x)^{-1}f(y) \quad \text{a theorem on homs} \\ &= f(y)^{-1}f(y) \\ &= e_H. \end{aligned}$$

Hence $x^{-1}y = e_G$. Hence $x = y$. Thus f is one to one.

Conversely, we suppose f is one to one. We want to show $\{x \in G : f(x) = e_H\} = \{e_G\}$. Let $x \in G$ be given, satisfying $f(x) = e_H$. Now $f(e_G) = e_H$. Since f is 1-1, $x = e_G$. Thus $\{x \in G : f(x) = e_H\} = \{e_G\}$.

8. (12 marks) Let A be a nonempty set and let $a \in A$ be given. Let S_A be the group of bijections $f : A \to A$, under composition. Show that $H = \{f \in S_A : f(a) = a\}$ is a subgroup of S_A.

soln: H is nonempty since $e \in H$, e being the identity. Let $f \in H$ and $g \in H$ be given. Claim $fg^{-1} \in H$. Since $g(a) = a$, we have $g^{-1}(a) = a$, and hence $fg^{-1}(a) = a$. Hence the claim is true. Hence H is a subgroup of S_A.

9. (12 marks) Prove $(0, 1)$ has no least element.

soln: Suppose x is the least element. Then 1)$x \in (0, 1)$ and 2) for all $y \in (0, 1)$, $y \geq x$. Now by 1), $x/2 > 0$. Also, $x/2 < x < 1$, giving $x/2 \in (0, 1)$. By 2), $x/2 > x$. This contradicts $x/2 < x$. Hence there is no least element x.

10. (12 marks) Let A and B be subsets of $\mathbb{R}$. Suppose A is nonempty, $A \subset B$, and B is bounded above. Show that the least upper bounds of A and B exist, and satisfy $\operatorname{lub} A \leq \operatorname{lub} B$.

soln: Since $A \subset B$ and B is bounded above, so is A. Since A is nonempty, $l.u.b.A$ exists. Since A is nonempty and $A \subset B$, B is nonempty. Since it is bounded above, $l.u.b.B$ exists. Let $M = l.u.b.B$. For all $a \in A$, $a \in B$, and hence $a \leq M$. Thus M is an upper bound for A, which implies $M \geq l.u.b.A$. Thus $\operatorname{lub} A \leq \operatorname{lub} B$.

11. (12 marks) Suppose $g : \mathbb{R} \to \mathbb{R}$ satisfies $\lim_{x\to\infty} g(x) = \infty$. Show from first principles that $\lim_{x\to\infty} -0.5g(x) = -\infty$.

soln: Let $M \in \mathbb{R}$ be given. We claim there exists N in $\mathbb{R}$, such that for all $x > N$, $-0.5g(x) < M$. Equivalently, $g(x) > -2M$. But $g(x) \to \infty$ as $x \to \infty$, hence there exists $N \in \mathbb{R}$, such that for all $x > N$, $g(x) > -2M$. Thus $\lim_{x\to\infty} -0.5g(x) = -\infty$.

12. (18 marks) Let f and g be functions from $\mathbb{R}$ to $\mathbb{R}$. Let a and M be real numbers. Suppose $\lim_{x\to a} f(x) = 0$, and there exists $\delta_1 > 0$ such that for all $x \in (a - \delta_1, a + \delta_1)$, $|g(x)| \leq M$. Show from first principles that $\lim_{x\to a} f(x)g(x) = 0$.

soln: We want to show that for all $\epsilon > 0$, there exists $\delta > 0$, such that if $x \in (a - \delta, a + \delta)$, then $|f(x)g(x)| \leq \epsilon$. Let $\epsilon > 0$ be given. Since $\lim_{x\to a} f(x) = 0$, take $\delta_2 > 0$ such that if $x \in (a-\delta_2, a+\delta_2)$, then $|f(x)| \leq \epsilon/M$. Let $\delta = \min(\delta_1, \delta_2) > 0$. Let $x \in (a - \delta, a + \delta)$ be given. Then

$$\begin{aligned} |f(x)g(x)| &\leq (\epsilon/M)M \\ &= \epsilon. \end{aligned}$$

13. (10 marks) Suppose $\{a_n\}$ is a sequence of real numbers converging to 0 as $n \to \infty$. Suppose x is a real number, and for all n, $x \leq a_n$. Show $x \leq 0$.

soln: Suppose not, then $x > 0$. Since $a_n \to 0$, there exists $k \in \mathbb{N}$ such that for all $n > k$, $a_n \in (-x, x)$. Take $n > k$. Then $a_n < x$, but $a_n \geq x$ by hypothesis, a contradiction. Hence $x \leq 0$.