1. Prove via inclusion in both directions that for any three sets A, B, and C

$$(A \cup B) \times C = (A \times C) \cup (B \times C)$$

Solution: First, we must show that

$$(A \cup B) \times C \subseteq (A \times C) \cup (B \times C).$$

We know that sets have the distributive property due to Tautology #29, which states that

$$P \vee (Q \wedge R) \iff [(P \vee Q) \wedge (P \vee R)]$$

we know know that

$$C \vee (A \wedge B) \iff [(C \vee A) \wedge (C \vee B)].$$

So

$$(A \cup B) \times C = (A \times C) \cup (B \times C)$$

is proven to be true. Next we must show that

$$(A \times C) \cup (B \times C) \subseteq (A \cup B) \times C.$$

Since Tautology #29 works in reverse as well, this too holds.

Since $(A \times C) \cup (B \times C) \subseteq (A \cup B) \times C$ is true and $(A \cup B) \times C \subseteq (A \times C) \cup (B \times C)$ is true, we have shown that $(A \cup B) \times C = (A \times C) \cup (B \times C)$ is true.

2. Let A be the set of all people who have ever lived. For $x, y, \in A$, xRy if and only if x and y share at least one parent. Determine

   (a) Whether or not the relation R is reflexive;

   (b) Whether or not the relation R is symmetric;

   (c) Whether or not the relation R is anti-symmetric;

   (d) Whether or not the relation R is transitive;

   (e) Whether or not the relation R is an equivalence relation;

   (f) Whether or not the relation R is a partial order.

Solution:

   (a) Yes, R is reflexive. $\forall x$, x shares their parents with themselves. $x \cap x = x$.

   (b) R is symmetric. $\forall x, y \in A$, if x shares one parent with y, then y must share a parent with x. $x \cap y = y \cap x$.

(c) R is not anti-symmetric. R is anti-symmetric iff $xRy \wedge yRx \implies x = y$. In other words, R is anti-symmetric only if one person can have a certain set of parents. We know this is not true as we have already proven A is symmetric, showing that x and y do not need to be equal to share a parent.

(d) R is not transitive. Assume x has parents i and j, y has parents j and k, and z has parents k and l. For transitivity to hold, z must either have i or j as a parent. In this case, xRy and yRz hold, but xRz does not, so R is not transitive.

(e) R is not an equivalence relation. To be an equivalence relation, R must be symmetric, reflexive, and transitive. As R is not transitive, it is not an equivalence relation.

(f) R is not a partial order. To be a partial order, R must be reflexive, transitive, and anti-symmetric. As R is not anti-symmetric or transitive, it is not a partial order.

3. Let $f : [-1, 1] \mapsto [-1, 0]$ be the function defined by $f(x) = x^2 - 1$ for all $x \in [-1, 1]$. Determine whether or not this function is injective and whether or not it is surjective.

Solution:
End points:

$$x = -1 : (-1)^2 - 1 = 1 - 1 = 0$$
$$x = 1 : (1)^2 - 1 = 1 - 1 = 0$$

<u>Injective</u>

$$f'(x^2 - 1) = x = 0$$
$$f''(x^2 - 1) = f'(x) = 1 > 0$$

So there is a local minimum at $x = 0$. Substituting x into $f(x)$ gets us:

$$f(0) = (0)^2 - 1 = -1.$$

So $\exists x \in [0, 1]$ s.t. $f(x) = -1$, as $-1 \in [-1, 0] = [f(0, 1)]$. Let $x^2 - 1 = 0$. Then

$$(x + 1)(x - 1) = 0.$$

Therefore $f(1) = f(-1)$. Since $1 \neq -1$, $f(x)$ is not injective.

<u>Surjective</u>
The local minimum of $f(x)$ is -1 at $x = 0$. The values at the end points were also found to be $f(-1) = 0$ and $f(1) = 0$. Therefore -1 is the global minimum. Let $f(x) = y$. Then

$$y = x^2 - 1$$
$$y + 1 = x^2$$

$$\sqrt{y+1} = x$$

Then $f(x) = f(\sqrt{y+1}) = (\sqrt{y+1}^2 - 1) = y$. Sqauring a square root removes the square, so we are left with $y + 1 - 1 = y$. Since we are left with $y = y$, we know that f is surjective.

4. Prove by mathematical induction that if $k \in \mathbb{N}$ and $k > 2$, then $2^k > 1 + 2k$.
Solution: Fix $k \in N$
Base case: $k = 3$.
Then

$$2^3 > 1 + 2(3) = 8 > 7$$

as required.
Induction step: Assume true for $n = k$.
Prove true for $n = k + 1$.

$$2^k \cdot 2 > 2(2k+1) = 4k + 2$$
$$4k = 2k + 2k > 2k + 1$$
$$= 4k + 2 > 2k + 3$$
$$= 2^{k+1} > 4k + 2 > 2k + 3$$
$$= 2^{k+1} > 2k + 3$$

as required.

5. Let $A = \{z \in \mathbb{C} \mid z^6 = 1\}$ with the operation of multiplication.

   (a) Is $(A, \cdot)$ a semigroup?

   (b) Is $(A, \cdot)$ a monoid?

   (c) Is $(A, \cdot)$ a group?

   (d) Write down an isomorphism between $(A, \cdot)$ and $(\mathbb{Z}_6, \oplus_6)$.

Solution:

(a) Yes, $(A, \cdot)$ is a semigroup. In order to be a semigroup, A must be endowed with an associative binary operation. To prove $\cdot$ is associative, let $x = a+bi, y = c+di$, and $z = e + fi$, where $x, y, z \in \mathbb{C}$ and $x^6 = y^6 = z^6 = 1$. If $\cdot$ is associative, then $x(yz) = (xy)z$. In other words,

$$(a + bi)[(c + di)(e + fi)] = [(a + bi)(c + di)](e + fi).$$

So

$$
\begin{aligned}
&(a+bi)[(c+di)(e+fi) \\
&= (a+bi)[c(e+fi)+di(e+fi)] \\
&= (a+bi)[ce+cfi+dei-df] \\
&= (a+bi)(ce-df+(cf+de)i) \\
&= a(ce-df+(cf+de)i)+bi(ce-df+(cf+de)i) \\
&= ace-adf+acfi+adei+bcei-bdfi-bcf-bde \\
&= ace-adf+bcf+bde+(acf+ade+bce-bdf)i \\
&= [e(ac-bd)+f(ad-bc)]+[e(ad+bc)+f(ac-bd)]i \\
&= (e+fi)[(ac-db)+(ad+bc)i] \\
&= (e+fi)[(a+bi)(c+di)] \\
&= [(a+bi)(c+di)](e+fi).
\end{aligned}
$$

Thus $(a+bi)[(c+di)(e+fi)] = [(a+bi)(c+di)](e+fi)$ as required.

(b) Yes, $(A,\cdot)$ is a monoid. The identity element e under multiplication is 1.
Proof:

$$
\begin{aligned}
1 &= 1+0i \\
(a+bi)(1+0i) &= a+bi \\
&= a(1+0i)+bi(1+0i) \\
&= a(1)+bi(1) \\
&= a+bi
\end{aligned}
$$

Since $1+0i \in \mathbb{C}$ and $(1)^6 = 1, A$ is a monoid.

(c) If A is a group, then it must be a monoid and every element in A must be invertible. Let $z \in \mathbb{C}$, where $z^6 = 1$. Let z^{-1} be the inverse of z, such that $zz^{-1} = z^{-1}z = 1$. z can be written in the form $a+bi$, where $a,b \in \mathbb{R}$. So

$$
\begin{aligned}
z^{-1}(a+bi) &= 1 \\
z^{-1} &= \frac{1}{a+bi} \\
&= \frac{a-bi}{(a+bi)(a-bi)} \\
&= \frac{a-bi}{a^2+b^2}
\end{aligned}
$$

So $z^{-1} = \frac{a-bi}{a^2+b^2}$. To confirm this, we will test if $z^{-1}z = 1$.

$$
zz^{-1} = (a+bi)\frac{a-bi}{a^2+b^2}
$$

$$= \frac{a^2 - abi + abi - b^2i^2}{a^2 + b^2}$$
$$= \frac{a^2 + b^2}{a^2 + b^2}$$
$$= 1$$

So as long as $a^2 + b^2 \neq 0$, there exists an inverse of $z \in \mathbb{C}$. Since $(0)^6 = 0 \neq 1$ and $0 \notin A$, it is a group.

(d) An isomorphism between $(A, \cdot)$ and $(\mathbb{Z}_6, \oplus_6)$ is

$$f(k) = cos\left(\frac{2\pi k}{6}\right) + i \cdot sin\left(\frac{2\pi k}{6}\right)$$

To justify this, take some $z \in \mathbb{C}$ such that $z^6 = 1$. According to De Moivre's theorem, $z^k = r^k(\cos k\theta + i \cdot \sin k\theta) = r^k e^{ki\theta}$, so then $e^{ki\theta} = \cos k\theta + i \cdot \sin k\theta$, for some $k \in \mathbb{Z}$. Let $\theta = 2\pi$. Then

$$e^{2\pi ik} = \cos 2\pi ik + i \cdot \sin 2\pi ik$$

$$= 1$$

Then $e^{2\pi ik} = 1$. According to De Moivre's theorem, $z^6 = r^6e^{6i\theta} = 1$. For any $z,\ z = a + bi,\ a, b \in \mathbb{R}$. Since $r = |\sqrt{a^2 + b^2}|$ is a positive real number and for any $z^n,\ n \in \mathbb{Z},\ z^n = 1,\ r^n = 1$. So $r = 1$ and $e^{6i\theta} = e^{2\pi ik}$. Taking the natural logarithm of of both sides gets us $6i\theta = 2\pi ik$. Solving for θ, we end up with

$$\theta = \frac{2\pi k}{6}$$

Substituting this back into trigonometric form gets us

$$z = cos\left(\frac{2\pi k}{6}\right) + i \cdot sin\left(\frac{2\pi k}{6}\right)$$

for some integer k. So any $z \in \mathbb{C}$ where $z^6 = 1$ can be expressed as this formula given some integer k. Substituting $\{0, 1, 2, \ldots, 5\}$ into k returns each unique root of z. If $k > 5$, the results repeat. In other words, for some integer $k = \{0, 1, 2, \ldots, 5\}$ using a number greater than $n - 1$ still returns a root of z. For example, z when $k = 3$ is the same as z when $k = 9$, or $3 \equiv 9 \pmod 6$. So

$$f(k) = cos\left(\frac{2\pi k}{6}\right) + i \cdot sin\left(\frac{2\pi k}{6}\right)$$

is an isomorphism from $(\mathbb{Z}_6, \oplus_6)$ to $(A, \cdot)$ as any $f(a) \cdot f(b) = f(a \oplus b)$ and each k gives a unique root of z.