1. Calculate/determine the following things:

   (a) In words, any even $n > 2$ has a square $m > 1$ dividing n. So $n = 6$ is a counterexample (no square other than 1 divides 6).

   (b) The contrapositive is "if $n^2 = 9$ then $n = 3$" which has $n = -3$ as a counterexample.

   (c) The negation is $\exists x \exists y \forall z,\ x + y + z \leq 5$.

   (d) The negation is $\exists x \in A\, \exists y \in B,\ x \cdot y \notin A \cap B$.

   (e) The negation is ~ there exists an $x \in \mathbb{R}$ such that for all $n \in \mathbb{Z}$, $x \geq n$.

   (f) $A \cap B = \{1\}$ so $A \times (A \cap B) = \{(1,1), (3,1), (5,1), (7,1), (9,1)\}$.

   (g) Take $A = \{1,2\}$ and $B = \{1,3\}$: then $(A \cap B)^c \cup B = \{1,2,3,4\}$ but $(A^c \cup B)^c = \{2\}$.

   (h) (i) False (take $x = y = 1$), (ii) True (take any $y \neq x$), (iii) False (no x has $y \neq x$ for all y), (iv) True (take $x = 1$, $y = 2$).

   (i) (i) False (take $x = 1$, $y = 0$), (ii) True (take any $y^2 > x$), (iii) True (take $x = -1$), (iv) True (take $x = y = 1$).

   (j) Many choices, such as $a = 1$, $b = 2$, $c = 3$: then $a|b$ and $a|c$ but $b \nmid c$.

   (k) Use Euclid: 256,520 have gcd 8 and lcm $256 \cdot 520/8$ while 921,177 have gcd 3 and lcm $921 \cdot 177/3$.

   (l) Gcd has min of exponents so gcd is $2^3 3^2 5^4$ and lcm has max of exponents so lcm is $2^4 3^3 5^4 7^1 11^1$.

   (m) For example $p = 2$ and $q = 3$ are prime and $p + q = 5$ is also prime.

   (n) Any perfect square is a counterexample, such as $n = 4$, since $\sqrt{4} = 2$ is rational.

   (o) The negation is ~ there exist positive integers a and b with $2 = (a/b)^3$.

   (p) $\overline{4} + \overline{8} = \overline{3}$, $\overline{4} - \overline{8} = \overline{5}$, $\overline{4} \cdot \overline{8} = \overline{5}$, $\overline{4}^2 = \overline{7}$, and $\overline{4}^{-1} = \overline{7}$ in $\mathbb{Z}/9\mathbb{Z}$.

   (q) $\overline{10}$ does not (gcd 5). For $\overline{11}$ by Euclid $-9 \cdot 11 + 4 \cdot 25 = 1$ so $\overline{11}^{-1} = \overline{-9}$. For $\overline{12}$ by Euclid $-2 \cdot 12 + 1 \cdot 25 = 1$ so $\overline{12}^{-1} = \overline{-2}$.

   (r) $\overline{30}$ does not (gcd 6). For $\overline{31}$ by Euclid $19 \cdot 31 - 14 \cdot 42 = 1$ so $\overline{31}^{-1} = \overline{19}$. And $\overline{32}$ does not (gcd 2).

   (s) $\{(1,1), (1,2), (1,4), (2,1), (2,2), (2,4), (4,1), (4,2), (4,4), (3,3), (3,5), (5,3), (5,5), (6,6)\}$.

   (t) Solving $y = \frac{6x+5}{2x-7}$ for x yields $y(2x - 7) = 6x + 5$ so $2xy - 7y = 6x + 5$ so $f^{-1}(y) = x = \frac{7y+5}{2y-6}$.

   (u) $\text{im}(f) = \{2,3,4,1\} = \{1,2,3,4\}$. In fact f^{-1} is a function from $\{1,2,3,4\} \to \{1,2,3,4\}$ so f is one-to-one and onto.

   (v) We have $\text{im}(g) = \{\overline{1}, \overline{3}, \overline{5}\}$. g is not one-to-one since $g(\overline{1}) = g(\overline{4})$ and g is not onto since there is no $\overline{n}$ with $g(\overline{n}) = \overline{0}$.

   (w) We have $\text{im}(h) = \mathbb{Z}/6\mathbb{Z}$, and in fact h is both one-to-one and onto.

   (x) Here f has an inverse function $f^{-1} : \mathbb{R} \to \mathbb{R}$ with $f^{-1}(y) = y/2$ so f is a bijection.

   (y) Here g is one-to-one since $g(x_1) = g(x_2)$ implies $x_1 = x_2$, but g is not onto since the image of f is the even integers. We have $g^{-1}(2n) = n$.

   (z) Many choices, such as $f(n) = n^3$ or $f(n) = n$ for $n \leq 0$ and $n + 1$ for $n \geq 1$, and $g(n) = \lfloor n/2 \rfloor$ or $g(n) = n$ for $n \leq 0$ and $n - 1$ for $n \geq 1$.

2.

#	Reflexive	Symmetric	Transitive	Antisymmetric	Irreflexive	Equiv Rel	Partial	Total
(a)	Yes	No	Yes	Yes	No	No	Yes	Yes
(b)	No	Yes	No	No	Yes	No	No	No
(c)	Yes	Yes	Yes	No	No	Yes	No	No
(d)	Yes	No	Yes	Yes	No	No	Yes	No
(e)	Yes	No	Yes	Yes	No	No	Yes	Yes
(f)	Yes	Yes	Yes	No	No	Yes	No	No
(g)	No (0)	Yes	Yes	No	No	No	No	No

---

3. Calculate/determine the following things:

(a) $\mathbb{Q}$ and $\mathbb{Q} \cap \mathbb{R} = \mathbb{Q}$ are countable, while $\mathbb{R}$, $\mathbb{Q} \times \mathbb{R}$, $\mathbb{Q} \cup \mathbb{R} = \mathbb{R}$, and $\mathbb{R} \backslash \mathbb{Q}$ are uncountable.

(b) $\mathcal{P}(\emptyset)$ and $\mathcal{P}(\{1, , \dots, 10000\})$ are finite hence countable, while $\mathcal{P}(\mathbb{Z})$, $\mathcal{P}(\mathbb{Q})$, $\mathcal{P}(\mathbb{R})$, $\mathcal{P}(\mathcal{P}(\mathbb{Q}))$ are uncountable.

(c) It is not a group: the operation is not associative and there is no identity ($n - 0 = n$ but $0 - n = -n$).

(d) It is a group: the operation is associative, there is an identity 0, and $2n$ has an additive inverse $-2n$.

(e) The inverse of $\overline{30}$ in the additive group is simply $\overline{-30} = \overline{29}$.

(f) By Euclid we have $2 \cdot 30 - 59 = 1$ so $\overline{2} \cdot \overline{30} = \overline{1}$ so the inverse of $\overline{30}$ in the multiplicative group is $\overline{2}$.

(g) $(sr)(sr^2) = s(sr^{-1})r^2 = r$ and $s^2r^3s^4r^5 = r^3r^5 = r^8$.

(h) $(r^3)^{-1} = r^9$ and $(sr^2)^{-1} = r^{-2}s^{-1} = r^{-2}s = sr^2$.

(i) This permutation is $(1\,8)(2\,7)(3\,6)(4\,5)$.

(j) This permutation is $(1\,3\,2\,6\,4\,5)(7) = (1\,3\,2\,6\,4\,5)$.

(k) $(3\,1\,4)(1\,5) = (1\,5\,4\,3)$ by tracing right to left.

(l) $(2\,7\,1\,8) \cdot (2\,8) \cdot (1\,8) \cdot (2\,8) = (1\,7)(2\,8)$ by tracing right to left.

(m) $[(1\,4\,2\,8\,5)(6\,7)]^{-1} = (6\,7)^{-1}(1\,4\,2\,8\,5)^{-1} = (7\,6)(5\,8\,2\,4\,1) = (1\,5\,8\,2\,4)(6\,7)$.

(n) $\mathbb{Z}/8\mathbb{Z}$ and $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ all work.

(o) The dihedral group $D_{2 \cdot 10}$ of order 20 is non-abelian.

(p) The groups $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}\backslash\{0\}, \cdot)$ are all countably infinite.

(q) A Cartesian product of a group in (p) with S_3 or $D_{2 \cdot 4}$ is countably infinite and non-abelian.

(r) The groups $(\mathbb{R}, +)$ and $(\mathbb{R}\backslash\{0\}, \cdot)$ are both uncountably infinite.

(s) A Cartesian product of one of the groups in (r) with S_3 or $D_{2 \cdot 4}$ is uncountably infinite and non-abelian.

(t) s has order 2, r has order 10, r^2 has order 5, r^3 has order 10.

(u) $(1\,2\,3)$ has order 3, $(4\,5)$ has order 2, $(1\,2\,3)(4\,5)$ has order 6.

(v) $(2\,4\,5)$ has order 3, $(1\,5)(2\,3)$ has order 2, $(2\,4\,5) \cdot (1\,5)(2\,3) = (1\,2\,3\,4\,5)$ has order 5.

(w) By Lagrange's theorem these are the divisors of 20: 1, 2, 4, 5, 10, 20.

---

4. Prove the following:

(a) Truth table, or $P \wedge \neg[Q \vee (R \Rightarrow P)] = P \wedge \neg[Q \vee \neg R \vee P] = P \wedge \neg Q \wedge R \wedge \neg P$ which is false due to the $P \wedge \neg P$.

(b) When P is true, Q is false, R is true, then $(P \Rightarrow Q) \Leftrightarrow R$ is false while $P \Rightarrow (Q \Leftrightarrow R)$ is true.

(c) Truth table, or $\neg[Q \wedge \neg(P \wedge Q)] \wedge \neg P = [\neg Q \vee (P \wedge Q)] \wedge \neg P = (\neg Q \wedge \neg P) \vee (P \wedge Q \wedge \neg P) = (\neg Q \wedge \neg P) \vee \text{False} = \neg Q \wedge \neg P$.

(d) Let $x \in (A\backslash B) \cup (B\backslash C)$. Then $x \in A\backslash B$ or $x \in B\backslash C$. If $x \in A\backslash B$ then $x \in A$ and $x \notin B$ so $x \in A \cup B$ and $x \notin B \cap C$, meaning $x \in (A \cup B)\backslash(B \cap C)$. If $x \in B\backslash C$ then $x \in B$ and $x \notin C$ so $x \in A \cup B$ and $x \notin B \cap C$, so again $x \in (A \cup B)\backslash(B \cap C)$.

(e) First suppose $A\backslash B = \emptyset$. If $x \in A$ then since $A\backslash B$ is empty, x must be in B (otherwise x would be in $A\backslash B$), so $A \subseteq B$. Conversely, if $A \subseteq B$, then there are no elements of A not in B, so $A\backslash B = \emptyset$.

(f) Note $x \in A\backslash(B \cap C) \iff x \in A$ and $x \notin (B \cap C) \iff x \in A$ and ($x \notin B$ or $x \notin C$) $\iff$ ($x \in A$ and $x \notin B$) or ($x \in A$ and $x \notin C$) $\iff x \in A\backslash B$ or $x \in A\backslash C \iff x \in (A\backslash B) \cup (A\backslash C)$.

(g) Observe $(A \cup B^c)^c = A^c \cap (B^c)^c = A^c \cap B$ by de Morgan's laws, so $A \cup B^c$ and $A^c \cap B$ are complements. Thus, if $A \cup B^c = U$ then $A^c \cap B = U^c = \emptyset$ and conversely if $A^c \cap B = \emptyset$ then $A \cup B^c = \emptyset^c = U$.

(h) First suppose $A \subseteq B \cup C$. If $x \in A\backslash B$ then $x \in A$ and $x \notin B$. Since $A \subseteq B \cup C$, $x \in B \cup C$ so $x \in B$ or $x \in C$ but since $x \notin B$ we must have $x \in C$: thus $A\backslash B \subseteq C$. Conversely suppose $A\backslash B \subseteq C$ and let $x \in A$. If $x \in B$ then clearly $x \in B \cup C$ and otherwise if $x \notin B$ then $x \in A\backslash B$ hence $x \in C$ and once again $x \in B \cup C$: thus $A \subseteq B \cup C$.

(i) Induct on n. Base case $n = 1$ has $F_1 + F_3 = 3 = F_4$. Inductive step: if $F_1 + \cdots + F_{2n+1} = F_{2n+2}$ then $F_1 + \cdots + F_{2n+1} + F_{2n+3} = [F_1 + \cdots + F_{2n+1}] + F_{2n+3} = F_{2n+2} + F_{2n+3} = F_{2n+4}$ as required.

(j) Induct on n. Base cases $n = 1$ and $n = 2$ have $c_1 = 2^{F_1}$ and $c_2 = 2^{F_2}$. Inductive step: if $c_n = 2^{F_n}$ and $c_{n-1} = 2^{F_{n-1}}$ then $c_{n+1} = c_n c_{n-1} = 2^{F_n} 2^{F_{n-1}} = 2^{F_n + F_{n-1}} = 2^{F_{n+1}}$ as required.

(k) Induct on n. Base case $n = 1$ has $a_1 = 3^1 - 2$. Inductive step: if $a_n = 3^n - 2$ then $a_{n+1} = 3(3^n - 2) + 4 = 3^{n+1} - 2$.

(l) Induct on n. Base case $n = 1$ has $b_1 = 2^1 + 1$. Inductive step: if $b_n = 2^n + n$ then $b_{n+1} = 2(2^n + n) - n + 1 = 2^{n+1} + (n+1)$.

(m) Induct on n. Base cases $n = 0$ and $n = 1$ have $c_0 = 6 \cdot 2^0$ and $c_1 = 4 \cdot 2^1$. Inductive step: if $c_n = (6 - 2n)2^n$ and $c_n = (6 - 2(n-1))2^{n-1} = (4 - n)2^n$ then $c_{n+1} = 4(6 - 2n)2^n - 4(4 - n)2^n = (24 - 8n - 16 + 4n)2^n = (8 - 4n)2^n = (6 - 2(n+1))2^{n+1}$ as required.

(n) Induct on n . Base cases $n = 1$ and $n = 2$ have $d_1 = 2^1$ and $d_2 = 2^2$. Inductive step: if $d_n = 2^n$ and $d_{n-1} = 2^{n-1}$ then $d_{n+1} = 2^n + 2(2^{n-1}) = 2^n + 2^n = 2^{n+1}$ as required.

(o) Induct on n. Base case $n = 1$ has $25^1 + 7 = 32$ a multiple of 8. Inductive step: if 8 divides $25^n + 7$, then 8 divides $25 \cdot (25^n + 7) - 24 \cdot 7 = 25^{n+1} + 7$. (Reducing modulo 8 also works.)

(p) Induct on n. Base case $n = 1$ has $1/2 = 2 - 1/2^0 - 1/2^1$. Inductive step: If $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = 2 - \frac{1}{2^n}$, then $1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} + \frac{1}{2^{n+1}} = 2 - \frac{1}{2^n} + \frac{1}{2^{n+1}} = 2 - \frac{1}{2^{n+1}}$ as required.

(q) Induct on n. Base case $n = 1$ has $\frac{1}{1 \cdot 2} = \frac{1}{2}$. Inductive step: if $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1}$ then $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n \cdot (n+1)} + \frac{1}{(n+1) \cdot (n+2)} = \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} = \frac{n+1}{n+2}$ as required.

(r) If n is the sum of $k, k+1, k+2, k+3, k+4, k+5$ then $n = 6k + 15 \equiv 3 \pmod 6$. Conversely if $n \equiv 3$ mod 6 so that $n = 3 + 6a$, then n is the sum of $a - 2, a - 1, a, a + 1, a + 2, a + 3$.

(s) Modulo 6 we have $7^n + 5 \equiv 1^n + 5 \equiv 1 + 5 \equiv 0 \pmod 6$, which means $7^n + 5$ is divisible by 6.

(t) Since $a \equiv b \pmod n$ and $c \equiv d \pmod n$ we see $b + c \equiv a + d \pmod n$. Then $a(b + c) \equiv b(b + c) \equiv b(a + d) \pmod n$ so $a(b + c) \equiv b(a + d) \pmod n$.

(u) Clearly, if $6|n$ then $2|n$ and $3|n$. For the other direction, if $2|n$ then $n = 2k$. Then if $3|2k$ we must have $3|k$ since $3 \nmid 2$ and 3 is prime. So $k = 3a$, and thus $n = 6a$, meaning $6|n$.

(v) First, $A \subseteq B$ because if $n = 4a + 6b$ then $n = 2(2a + 3c) \in B$. Also, $B \subseteq A$ because if $n = 2c$ then we would have $n = 4(2c) + 6(-c) \in A$ via Euclidean algorithm calculation.

(w) Note $\gcd(n, n+p) = \gcd(n, p)$ by gcd properties. Then $\gcd(n, p)$ divides p so is either 1 or p, and it is equal to p if and only if $p|n$ (by definition of gcd).

(x) If $n \in C$, then $n = 6c$ for some c. Then $n = 10(2c) + 14(-c) \in D$ as required.

(y) Note $(2n)(2n + 2) = 4n^2 + 4n$ is 1 less than $(2n + 1)^2 = 4n^2 + 4n + 1$.

(z) Note $n - 1 \equiv -1 \pmod n$ so $(n - 1)^{-1} \equiv (-1)^{-1} \equiv -1 \equiv n - 1 \pmod n$. Or, $(n - 1)^2 = n^2 - 2n + 1 \equiv 1 \pmod n$.

---

5. Prove the following:

(a) Note $(a, b) \in R^{-1} \cap S^{-1} \iff (a, b) \in R^{-1}$ and $(a, b) \in S^{-1} \iff (b, a) \in R$ and $(b, a) \in S \iff (b, a) \in R \cap S \iff (a, b) \in (R \cap S)^{-1}$.

(b) R is reflexive since $|x| = |x|$, R is symmetric since $|x| = |y|$ implies $|y| = |x|$, and R is transitive since $|x| = |y|$ and $|y| = |z|$ imply $|x| = |z|$. Also, $[0] = \{0\}$, $[2] = [-2] = \{2, -2\}$, $[4] = \{4, -4\}$.

(c) $x \, R \, y$ when $6x \equiv y \pmod 5$, or equivalently when $x \equiv y \pmod 5$. So this relation is just congruence modulo 5, which we already know is an equivalence relation, and the equivalence classes are the congruence classes modulo 5: $[n] = \{\ldots, n - 10, n - 5, n, n + 5, n + 10, \ldots\}$.

(d) If R is reflexive and a function, then $R(a) = a$ for all $a \in A$, so the only possibility is to have $R(a) = a$ for all $a \in A$. But clearly the identity function is also an equivalence relation, so it is the only one that works.

(e) Reflexive: For each $a \in A$ we have $(a, a) \in R$ and so $(a, a) \in R^{-1}$ hence $(a, a) \in S$. Symmetric: if $(a, b) \in S$ then $(a, b) \in R$ and $(a, b) \in R^{-1}$ so $(b, a) \in R^{-1}$ and $(b, a) \in R$ so $(b, a) \in S$. Transitive: if $(a, b), (b, c) \in S$ then $(a, b), (b, c) \in R$ so $(a, c) \in R$ and also $(c, b), (b, a) \in R$ so $(c, a) \in R$ so $(a, c) \in R^{-1}$ so $(a, c) \in S$.

(f) Note $f(f(a)) = a$ for all $a \in A \iff f \circ f = i_A \iff f^{-1} = f$ as functions on $A \iff f^{-1}$ exists and $f^{-1}(a) = f(a)$ for all $a \in A$.

(g) Let $x \in A$. Then by hypothesis $(f \circ g)(x) = (f \circ h)(x)$ which means $f(g(x)) = f(h(x))$. But f is one-to-one, so this implies $g(x) = h(x)$. Since g and h agree on all elements in A, that means $g = h$.

(h) Suppose $c \in C$. Then $f(c) \in f(C)$, so by definition we have $c \in f^{-1}(f(C))$.

(i) From above $C \subseteq f^{-1}(f(C))$. For the reverse, suppose $c \in f^{-1}(f(C))$, so that $f(c) \in f(C)$. Since f is one-to-one, $f(a) = f(c)$ implies $a = c$, so $f(a) \in f(C)$ implies $a \in C$.

(j) Suppose $a \in f^{-1}(D)$. Then $f(a) \in D$ by definition. This holds for all $a \in f^{-1}(D)$, so $f(f^{-1}(D)) \subseteq D$.

(k) From above, $f(f^{-1}(D)) \subseteq D$. For the reverse, suppose $d \in D$. Since f is onto, there exists $a \in A$ with $f(a) = d$, so $a \in f^{-1}(D)$. Hence $d \in f(f^{-1}(D))$.

(l) Suppose $x \in f(C_1) \cap f(C_2)$, meaning that $x = f(c_1) = f(c_2)$ for some $c_1 \in C_1$ and $c_2 \in C_2$. But since f is one-to-one this means $c_1 = c_2$, and so $c_1 \in C_1 \cap C_2$: thus $x = f(c_1)$ for some $c_1 \in C_1 \cap C_2$ so $x \in f(C_1 \cap C_2)$.

(m) Note f has an inverse g. Then in fact $\tilde{f}$ has an inverse $\tilde{g} : \mathcal{P}(B) \to \mathcal{P}(A)$ with $\tilde{g}(T) = \{g(t) : t \in T\}$. Explicitly, for $S \subseteq A$, $\tilde{g}(\tilde{f}(S)) = \tilde{g}(\{f(s) : s \in S\} = \{g(f(s)) : s \in S\} = \{s : s \in S\} = S$ and $\tilde{f}(\tilde{g}(T)) = \tilde{f}(\{g(t) : t \in T\}) = \{f(g(t)) : t \in T\} = \{t : t \in T\} = T$.

(n) All equivalence relations contain the identity relation. So f is one-to-one $\iff [a] = [b]$ is equivalent to $a = b \iff a\,R\,b$ is equivalent to $a = b \iff R$ equals the identity relation.

(o) Note that B is a subset of $A \cup (B \backslash A)$. If A and $B \backslash A$ are countable then their union is also countable, hence any subset is countable. If B is uncountable then this is a contradiction, so $B \backslash A$ is uncountable.

(p) Both $\mathbb{Q}$ and $\mathbb{Q} \cap (0,1)$ are countably infinite, so there is a bijection between these sets since they are both in bijection with the positive integers.

(q) The Cartesian product of two countable sets is countable, so $\mathbb{Q} \times \mathbb{Z}$ is countable since both $\mathbb{Q}$ and $\mathbb{Z}$ are countable. But $\mathbb{R} \times \mathbb{Z}$ contains $\mathbb{R} \times \{1\}$ which is in bijection with $\mathbb{R}$, so $\mathbb{R} \times \mathbb{Z}$ has an uncountable subset hence is uncountable itself.

(r) If S_n is the set of n-element subsets of $\mathbb{Z}$ then S_n is countable since it is a subset of $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (with n terms) and this set is countable. Then the set of finite subsets of $\mathbb{Z}$ is $\cup_{n=0}^{\infty} S_n$ which is a countable union of countable sets, hence countable.

(s) The functions $f : [1,7) \to (2,9)$ with $f(x) = 2 + (x/2)$ and $g : (2,9) \to [1,7)$ with $g(x) = 1 + (x/2)$ are both one-to-one, so by Cantor-Schröder-Bernstein there exists a bijection between $[1,7)$ and $(2,9)$.

(t) The functions $f : (0,1) \to [0,1]$ with $f(x) = x$ and $g : [0,1] \to (0,1)$ with $g(x) = (x+1)/3$ are both one-to-one, so by Cantor-Schröder-Bernstein there exists a bijection between $(0,1)$ and $[0,1]$.

(u) Induct on n. Base case $n = 1$ is given. For inductive step suppose $gh^n = h^n g$. Then $gh^{n+1} = (gh)(h^n) = (hg)h^n = h(gh^n) = h(h^n g) = h^{n+1}g$ using $gh = hg$ and $gh^n = h^n g$.

(v) Multiply $g^{-1}h^{-1} = h^{-1}g^{-1}$ on the left by hg and on the right by gh. This yields $hg(g^{-1}h^{-1})gh = hg(h^{-1}g^{-1})gh$. Then $hg(g^{-1}h^{-1})gh = hgg^{-1}h^{-1}gh = hh^{-1}gh = gh$ while $hg(h^{-1}g^{-1})gh = hgh^{-1}g^{-1}gh = hgh^{-1}h = hg$, so $gh = hg$.

(w) By hypothesis $g^n = e$. Multiplying by g^{-1} on both sides yields $g^{-1}g^n = g^{-1}e = g^{-1}$ and since $g^{-1}g^n = g^{-1}g(g^{n-1}) = eg^{n-1} = g^{n-1}$ we see $g^{n-1} = g^{-1}$.

(x) The function f is an element of the symmetric group S_n. By Lagrange's theorem, its order divides $n!$ hence is finite. But if the order is A then this means f^A is the identity, which is to say, $f^A(i) = i$ for each $i \in \{1, 2, 3, \ldots, n\}$.

(y) Reflextive: $e \in H$ and $g_1 = eg_1$ so $g_1\,R\,g_1$. Symmetric: If $g_1\,R\,g_2$ so that $g_1 = hg_2$ with $h \in H$ then $h^{-1}g_1 = g_2$ and $h^{-1} \in H$, so $g_2\,R\,g_1$. Transitive: If $g_1\,R\,g_2$ and $g_2\,R\,g_3$ so that $g_1 = hg_2$ and $g_2 = kg_3$ with $h, k \in H$ then $g_1 = hg_2 = hkg_3$ and $hk \in H$ so $g_1\,R\,g_3$.

(z) First $e \in S$ since $e^2 = e$. Second if $g, h \in S$ then $g^2 = e$ and $h^2 = e$ so $(gh)^2 = ghgh = g^2h^2 = ee = e$ since $gh = hg$ because G is abelian, so $gh \in S$. Finally if $g \in S$ then $g^2 = e$ so $(g^{-1})^2 = (g^2)^{-1} = e$ so $g^{-1} \in S$.